Department for
Digital, Culture,
Media & Sport

Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security

October 2018

Contents

Executive summary

This document maps the Code of Practice for Consumer IoT Security against published standards, recommendations and guidance on IoT security and privacy from around the world.[1] Around 100 documents were reviewed from nearly 50 organisations. Whilst not exhaustive, it represents one of the largest collections of guidance available to date in this area.

The purpose of the mapping is to serve as a reference and tool for users of the Code of Practice. Manufacturers and other organisations are already implementing a range of standards, recommendations and guidance and will seek to understand the relationship between the Code of Practice and existing material from industry and other interested parties. The mapping makes that exercise easier and, therefore, implementation of the Code of Practice more straightforward.

The mapping represents a snapshot in time. Security guidance across the IoT is rapidly evolving. Whilst gathering the information, it was observed that some organisations have merged and others are developing their work further, issuing updated versions regularly.

The intention was not to map the entire global technical standards and recommendations space. The mapping was limited in scope to the documentation that claims to be IoT security and privacy related. This means that the mapping does not include those standards and regulations which might be classified as foundational or which underpin the IoT standards, such as the General Data Protection Regulation (GDPR). Also, due to the variance in styles between recommendations, functional equivalence is not possible and so the mappings should be read as indicative only.

A separate mapping also identifies the relationships between organisations and material based on common external references that have been used in their documentation. This also gives an indication of references in specifications and guidance which may not be specific to IoT.

The raw data of both the Code of Practice and the reference material mappings are also available as open data in JavaScript Object Notation (JSON) format.[2] This enables organisations to use it within their own development processes.

---

[1] DCMS, October 2018, 'Code of Practice for Consumer IoT Security', https://www.gov.uk/government/publications/secure-by-design
[2] Available via the above link and on https://iotsecuritymapping.uk

Mapping the landscape of IoT security and privacy recommendations

The IoT industry, associated recommendations and security/privacy standards are continually developing. The mapping within this document is correct as at July 2018 and represents a snapshot of retrieved material at that time.[3]

The scope of the exercise was primarily contained to consumer-focused IoT, but there is a large amount of crossover with other IoT domains such as automotive and medical recommendations. This demonstrates that there is significant alignment for security and privacy across different IoT domains of interest. Guidance, such as 'I Am The Cavalry's' Hippocratic Oath for Connected Medical Devices, contain many recommendations which would be regarded as relevant to consumer devices and services too.[4] Where these recommendations do not directly refer to medical devices, they have been included in the mapping.

During the course of this mapping exercise, it was noted that some organisations had already merged and some standards or recommendations were not accessible due to them not being public documents. For example, the Online Trust Alliance (OTA) has merged with the Internet Society (ISOC) and the AllSeen Alliance has merged with the Open Connectivity Foundation (OCF). Some of the lists and documents that were investigated contained broken links and older versions of material.

[3] Material published after this date was not included, notably the 'IoT Cybersecurity Certification Program' which was announced by CTIA, a US wireless industry association, in August 2018, https://www.ctia.org/news/wireless-industry-announces-internet-of-things-cybersecurity-certification-program

[4] I Am The Cavalry, 2016, 'Hippocratic Oath for Connected Medial Devices', https://www.iamthecavalry.org/domains/medical/oath/

Summary and methodology of mapping

The mapping of the recommendations and guidance was based on online searches as well as public listings of IoT security and privacy guidance. Sources included:

- The living list of IoT Security and Privacy resources, maintained by David Rogers and Copper Horse Solutions Ltd,[5]
- Bruce Schneier's Security and Privacy Guidelines for the Internet of Things,[6]
- NTIA's IoT security standards catalogue,[7]
- W3C's Web of Things project's reference to existing best practices in related fields.[8]

Some of the documentation and guidance was judged to be out-of-scope, for example recommendations that focused on the automotive sector. This data is retained for reference in the mapping JSON file. The material that is referenced is largely at the same 'level' as the Code of Practice - that is, requirements and guidance rather than bit-level specifications. This avoided creating dependencies on other aspects as well as technology specific references. Also included are other commonly referenced documents such as the US Senate Bill: S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 and industry whitepapers.[9]

It is important to note that the mapping is intended to signpost organisations to recommendations where there is broad equivalence to the intent of the guideline. In some cases external recommendations may exceed the guideline. It is not a compliance document. Implementation of all guidance mapped to a Code of Practice guideline does not guarantee compliance with the guideline. Conversely it may not be necessary to implement all mapped guidance to be considered compliant. Whether a device or service can be considered compliant depends on the implementation specifics.

Recommendations were mapped against the 13 guidelines in the Code of Practice. This means that recommendations outside of that are deemed beyond the scope of this mapping. Implementing a secure development lifecycle is seen as fundamental to meeting the Code of Practice. Examples of documentation that can assist in this domain include the Fundamental Practices for Secure Software Development developed by the SAFECode Forum,[10] and ISO/IEC 29147 for Coordinated Vulnerability Disclosure which is referenced in the Code of Practice.

Also fundamental to meeting the Code of Practice are the already existing laws and regulation related to data protection, security and consumer safety.

---

[5] David Rogers, 2018, 'IoT Security Resources', https://blog.mobilephonesecurity.org/2016/11/iot-security-resources.html
[6] Bruce Schneier, 2017, 'Security and Privacy Guidelines for the Internet of Things', https://www.schneier.com/blog/archives/2017/02/security_and_pr.html
[7] NTIA, 2017, 'Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching', https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security
[8] W3C, 2017, 'Web of Things (WoT) Security and Privacy Considerations', https://www.w3.org/TR/wot-security/#existing-security-best-practices-in-related-fields
[9] US Congress, 2017, 'Internet of Things (IoT) Cybersecurity Improvement Act of 2017', https://www.congress.gov/bill/115th-congress/senate-bill/1691
[10] SAFECode Forum, 2011, 'Fundamental Practices for Secure Software Development', http://safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf

Mapping statistics

Across the entire Code of Practice, the following organisations and standards map to the CoP guidance. The consolidated mapping data is available within the open data JSON file.

The most closely mapped recommendation across the Code of Practice was the IoT Security Foundation's IoT Security Compliance Framework 1.1. Also, a wide-range of recommendations were mapped from the European Union Agency for Network and Information Security (ENISA), GSMA, the Industrial Internet Consortium (IIC) and the Open Web Application Security Project (OWASP). Some organisations split their recommendations across a number of documents, which are also listed below.

Summary Table of recommendations that map to the Code of Practice

Total number of recommendations mapped	Organisation	Standard / recommendation name
159	IoT Security Foundation	IoT Security Compliance Framework 1.1
66	European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT
55	Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0
39	GSMA	IoT Security Guidelines Endpoint Ecosystem
37	Open Web Application Security Project (OWASP)	IoT Security Guidance
33	IoT Security Initiative	Security Design Best Practices
32	Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5
29	GSMA	IoT Security Guidelines for Service Ecosystems
20	Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations
19	Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)
19	Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices
19	oneM2M	TR-0008-V2.0.1 Security (Technical Report)
17	US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering
16	European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments
14	US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)
13	IoT Security Initiative	CyberSecurity Principles of IoT

Total number of recommendations mapped	Organisation	Standard / recommendation name
13	US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching
12	Microsoft	IoT Security Best Practices
12	U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)
11	CableLabs	A Vision for Secure IoT
11	Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1
10	Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT
10	IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines
9	Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security
8	AT&T	The CEO's Guide to Securing the Internet of Things
8	IEEE	IoT Security Principles and Best Practices
6	Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World
6	International Electrotechnical Commission (IEC)	IoT 2020: Smart and secure IoT platform
6	Object Management Group (OMG) Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT
5	City of New York (NYC) Guidelines for the Internet of Things	Privacy + Transparency
5	GSMA	GSMA IoT Security Assessment
5	I am the Cavalry	Hippocratic Oath for Connected Medical Devices
5	Internet Society (ISOC)	The Internet of Things: An Internet Society Public Policy Briefing
5	Symantec	An Internet of Things Security Reference Architecture
4	Atlantic Council Scowcroft Center for Strategy and Security	Smart Homes and the Internet of Things
4	City of New York (NYC) Guidelines for the Internet of Things	Security
4	European Commission and AIOTI	Report on Workshop on Security & Privacy in IoT
4	Intel	Policy Framework for the Internet of Things (IoT)

Total number of recommendations mapped	Organisation	Standard / recommendation name
4	Open Web Application Security Project (OWASP)	OWASP Secure Coding Practices Quick Reference Guide
3	IERC-European Research Cluster on the Internet of Things (IERC)	IoT Governance, Privacy and Security Issues - IERC Position Paper
3	MIT Laboratory for Computer Science	Dos and Don'ts of Client Authentication on the Web
2	Alliance for Internet of Things Innovation (AIOTI)	AIOTI Digitisation of Industry Policy Recommendations
2	Alliance for Internet of Things Innovation (AIOTI)	Digitisation of Industry Policy Recommendations
2	GSMA	IoT Security Guidelines for Network Operators
2	Software and Information Industry Association (SIIA)	Empowering the Internet of Things: Benefits
2	W3C	Web of Things (WoT) Security and Privacy Considerations
1	Atlantic Council Scowcroft Center for Strategy and Security	Smart Homes and the Internet of Things (issue brief)
1	Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT
1	GSMA	Analytics-based Security
1	GSMA	GSMA Coordinated Vulnerability Disclosure Programme (CVD)
1	IoT Security Foundation	Connected Consumer Secure Design Best Practice Guidelines
1	Telecommunications Industry Association (TIA)	Realizing the Potential of the Internet of Things: Recommendations to Policy Makers
1	Web of Things (WoT) Security and Privacy Considerations	Minimize Network Interface Functionality

Mapping of external references within recommendations, guidelines and standards

The mapping has identified the relationships between organisations and material within the IoT security and privacy space. This is solely based on the external references provided within documents covered by the mapping. This also gives an indication of references in specifications and guidance which may not be specific to IoT.

The data of this reference mapping is available in an open data JSON file which can be used for further study. It is available on https://iotsecuritymapping.uk, which also hosts a visualisation of this mapping.

Mapping of Code of Practice guidelines

The recommendations set out in the following tables map to the thirteen guidelines of the Code of Practice. This is not considered to be holistic, but represents the output of a review of nearly 4000 pages of material from a large array of organisations and parties interested in the topic. This data is also available in the open data JSON files and viewable at https://iotsecuritymapping.uk.

Code of Practice: 1 - No default passwords

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
AT&T	The CEO's Guide to Securing the Internet of Things	No default password	Rather than permitting an easy-to-hack default password, each device should require the user to define a unique and reasonably secure password for access from a network interface.	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	IoT products can lend their computing power to launch DDoS Attacks - 2	Never ship IoT products without password protections	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.3.2 first bullet point	If your organization is writing your own applications, use appropriate authentication and authorization mechanisms. Scan for any passwords left in the clear in the application code (e.g. hardcoded telnet logins or passwords that were left behind during testing).	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-23	Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information	Baseline Security Recommendations for IoT	GP-TM-26	Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Security (ENISA)				
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-49	Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	5.2, fifth bullet point	Identification, authentication, authorization: strong authentication methods must be used, as well as access control mechanisms. Passwords and sessions should be managed accordingly.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.11	Enforce Strong Password Policy. It is imperative that all authentication systems enforce strong passwords where passwords are required for user authentication.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.12-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.9	Endpoint Password Management	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.12	Where passwords are used, enforce the use of passwords that conform to best practices regarding password complexity and length	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
IEEE	IoT Security Principles and Best Practices	5	IoT devices should not use easy-to-guess username/password credentials, such as admin/admin. Devices should not use default credentials that are invariant across multiple devices and should not include back doors and debug-mode settings (secret credentials established by the device's programmer) because, once guessed, they can be used to hack many devices. Each device should have a unique default username/password, perhaps printed on its casing, and preferably resettable by the user. Passwords should be sophisticated enough to resist educated guessing and so-called brute force methods.	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.2	The vast majority of Internet-connected devices will require authentication for some purposes, whether to protect the device from unauthorized use or reconfiguration, and to protect information stored within the device from disclosure or modification. This section details authentication requirements for devices that require authentication.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.2.4	A device that supports authentication SHOULD NOT be shipped in a condition that allows an unauthenticated client to use any function of the device that requires authentication, or to change that device's authentication credentials. Explanation: Most devices that can be used in an unauthenticated state will never be configured to require authentication. These devices are attractive targets for attack and compromise, especially by botnets. This is very similar to the problems caused by shipping devices with default passwords.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.2.5	Many devices that require authentication will be shipped with default authentication credentials, so that the customer can authenticate to the device using those credentials until they are changed. Each device that requires authentication SHOULD be instantiated either prior to shipping, or on initial configuration by the user, with credentials unique to that device. If a device is not instantiated with device-unique credentials, that device MUST NOT permit normal operation until those credentials have been changed to something other than the default credentials. Explanation: devices that were shipped with default passwords have been implicated in several serious denial-of-service attacks on widely-used Internet services.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.11	Flaws in the design and implementation of IoT devices and networks can lead to security vulnerabilities. A common flaw is the use of well-known or easy-to-guess passwords for configuration of IoT devices.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.7	If a connection requires a password or passcode or passkey for connection authentication, the factory issued or reset password is unique to each device and is not derived e.g. from serial numbers. Examples are WiFi access passwords and Bluetooth PINS	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.9	Where a wireless interface has an initial pairing process, the passkeys are changed from the factory issued or reset password prior to providing normal service.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.11	Where WPA2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is unique to each device in the product family.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.4	The product does not accept the use of null or blank passwords.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.6	The product/system enforces passwords to be compliant as NIST SP800-63b [Section 5.1.1.2] or similar recommendations on: password length; characters from the groupings and special characters.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.12	The product allows the factory issued or OEM login accounts to be disabled, erased or renamed. This is to avoid the type of attacks where factory default logins and passwords are published on the web, which allows attackers to mount very simple scanning and dictionary attacks on devices.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.13	The product supports having any or all of the factory default user login passwords, altered prior to normal service. This is to avoid the type of attacks where factory default logins and passwords are published on the web, which allows attackers to mount very simple scanning and dictionary attacks on devices.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.10.4	Where a web user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.11.1	Where an application's user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Initiative	Security Design Best Practices		Do not code in "secret" login bypasses/access methods – even if just for seemingly temporary Dev/Test purposes.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		If creating default credentials, create quality randomized and unique passwords/symmetric-keys.	https://www.iotsi.org/security-best-practices
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	13	Include strong authentication by default, including providing unique, system-generated or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	14	Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential reset using multi-factor verification and authentication (email and phone, etc.) where no user password exists.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	15	Take steps to protect against 'brute force' and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid login attempts	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Open Web Application Security Project (OWASP)	IoT Security Guidance	I1: Insecure Web Interface	Ensure that any web interface in the product disallows weak passwords	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I6: Insecure Cloud Interface	Ensure that any cloud-based web interface disallows weak passwords	https://www.owasp.org/index.php/IoT_Security_Guidance

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Web Application Security Project (OWASP)	IoT Security Guidance	I6: Insecure Cloud Interface	Ensure that users have the option to require strong passwords	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I7: Insecure Mobile Interface	Ensure that any mobile application disallows weak passwords	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I7: Insecure Mobile Interface	Ensure that users have the option to require strong passwords	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I8: Insufficient Security Configurability	Ensure password security options are made available (e.g. Enabling 20 character passwords or enabling two-factor authentication)	https://www.owasp.org/index.php/IoT_Security_Guidance
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Enable security by default through unique, hard to crack default user names and passwords. User names and passwords for IoT devices supplied by the manufacturer are often never changed by the user and are easily cracked. Botnets operate by continuously scanning for IoT devices that are protected by known factory default user names and passwords. Strong security controls should be something the industrial consumer has to deliberately disable rather than deliberately enable.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (A) (i) (IV)	IN GENERAL.—A clause that requires the contractor providing the Internet-connected device to provide written certification that the device (IV) does not include any fixed or hard-coded credentials used for remote administration, the delivery of updates, or communication.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

Code of Practice: 2 - Implement a vulnerability disclosure policy

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Report on Workshop on Security and Privacy in the Hyper connected World	Accountability & Risk Impact Assessment by Design	Any data controller and processor to be accountable for regulatory, contractual and ethical compliance. If data is compromised, disclosed, accessed or lost, clear statement by vendors, data controllers and data processors on impact is another prerequisite.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
Alliance for Internet of Things Innovation (AIOTI)	Report on Workshop on Security and Privacy in the Hyper connected World	Basic Requirements on IoT HARDWARE AND COMPONENTS	Sharing information about incidents/potential vulnerabilities between manufacturers	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
Alliance for Internet of Things Innovation (AIOTI)	Report on Workshop on Security and Privacy in the Hyper connected World	Basic Requirements on APPLICATIONS	Data should be encrypted on the application layer. End-to-End Security, cryptographic principles and key management are extremely important and should be carefully described.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Atlantic Council Scowcroft Center for Strategy and Security	Smart Homes and the Internet of Things		A published policy accepting help from willing allies acting in good faith, such as customers and security researchers, who find and report flaws.	http://www.atlanticcouncil.org/images/publications/Smart_Homes_0317_web.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.1	**Bug reporting system.** Manufacturers should provide a bug reporting system with a well-defined bug submission mechanisms and documented response policy.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.10	**Report discovery and remediation of software vulnerabilities.** Manufacturers should report discovery and remediation of software vulnerabilities that pose security or privacy threats to consumers.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.10	**Vulnerability reporting process.** Manufacturers should provide a vulnerability reporting process with a welldefined, easy-to-locate, and secure vulnerability reporting form, as well as a documented response policy. Manufacturers should consider compliance with ISO 30111 [108], a standard for vulnerability report handling.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
CableLabs	A Vision for Secure IoT	Detection and Identification Systems	Cable operators have widely deployed and continue to improve systems that are designed to detect compromised customer-owned devices controlled by botnets. These systems rely on (i) high-quality, third-party data feeds that identify sources of malicious traffic on the operator's network, (ii) DNS based anomaly detection systems, (iii) NetFlow detection systems that seek to identify devices communicating with known command and control servers, and (iv) email metadata to identify compromised customer devices originating SPAM	https://www.cablelabs.com/insights/vision-secure-iot/
CableLabs	A Vision for Secure IoT	Vulnerability Management	An IoT provider should have a well-defined procedure for receiving reports of security issues for their devices. The procedure should include status reporting and a timeline to address the problem that is provided to the individual or entity that submitted the security vulnerability. At a minimum, the IoT provider should publicly and prominently disclose an email address, a telephone number, and a website where security issues can be submitted to the company. Once there is a remedy to the vulnerability, the IoT provider should have a mechanism to publicly disclose the vulnerability and associated remedy.	https://www.cablelabs.com/insights/vision-secure-iot/
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-05	Establish procedures for analysing and handling security incidents. For any incident there should be a response to: a) confirm the nature and extent of the incident; b) take control of the situation; c) contain the incident; and d) communicate with stakeholders Establish management procedures in order to ensure a quick, effective and orderly response to information security incidents	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-06	Coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT).	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-07	Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-08	Create a publicly disclosed mechanism for vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	8.3	Vendors' awareness IoT vendors shall keep track of vulnerabilities in other IoT products, especially in the context of Smart Home Environments. For that purpose, vendors can hire or train security experts to understand security vulnerabilities in IoT, as they can only get worse with a wider adoption of the products. It is also important to consider early warnings on security issues provided by users and researchers, as they contribute to reducing the attack surface on devices and services. By raising the awareness level of IoT companies to security, product security will be improved and vendors will reduce the	https://www.ENISA.europa.eu/publications/security-resilience-good-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			threats they face and associated reputation issues. It is particularly true for vendors with limited experience in security.	
GSMA	GSMA Coordinated Vulnerability Disclosure Programme (CVD)		See GSMA Coordinated Vulnerability Disclosure Programme	https://www.gsma.com/security
I am the Cavalry	Hippocratic Oath for Connected Medical Devices	Third-Party Collaboration	I acknowledge that vulnerabilities will persist, despite best efforts. I will invite disclosure of potential safety or security issues, reported in good faith. Software flaws identified before they become safety issues give defenders an advantage. Manufacturers with the capability to receive and investigate flaws quickly increase this advantage. Those who encourage and act on reporting from independent sources can also reduce cost and exposure beyond what is possible with internal review alone. Value from researcher-manufacturer collaborations has led to manufacturers incentivizing research via recognition and reward programs.	https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
I am the Cavalry	Hippocratic Oath for Connected Medical Devices	Stakeholder communication	Communication to stakeholders should be prompt, transparent, and forthright. Manufacturers should notify relevant stakeholders when and where flaws exist, their severity, contents of the update, and instructions for each role. Updates may be exclusively communication about workarounds, warnings, unsafe conditions, labeling, instructions for use, or other relevant information.	https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf
IEEE	IoT Security Principles and Best Practices	10	Recently a bill was drafted for the Senate of the State of Michigan which would punish automobile hacking with a sentence of life in prison. One of the authors contacted one of the senators proposing the legislation and that senator agreed to modify the bill to allow hacking for beneficial research purposes. Researchers who discover serious vulnerabilities and report them responsibly provide a service to the industry similar to people who discover safety flaws in automobiles and other safety-critical machinery. Legitimate security research may be hindered by excessive legislation. One way to differentiate between research and unethical hacking is to mandate responsible disclosure of discovered vulnerabilities. Responsible disclosure requires the researcher to first notify the manufacturer or governing authorities and allow reasonable time for the vulnerability to be independently verified and fixed before going public with a system hack. Another, less desirable, approach might be to require researchers to first register with a government office or the manufacturer before attempting to break into a device.	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	5.2	Vendors MUST provide an easy to find way for reporting of security bugs, which is free of charge.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.5	A policy has been established for dealing with both internal and third party security researcher(s) on the products or services	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.6	A security policy has been established for addressing changes, such as vulnerabilities, that could impact security and affect or involve technology or components incorporated into the product or service provided.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.7	Processes and plans are in place based upon the IoTSF "Vulnerability Disclosure Guidelines" or a similar recognised process to deal with the identification of a security vulnerability or compromise when they occur.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.8	A process is in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those who may deal with the media or make public announcements. In particular, that any public statements made in the event of a security breach should give as full and accurate an account of the facts as possible.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.9	There is a secure notification process based upon the IoTSF "Vulnerability Disclosure Guidelines" or a similar recognised process, for notifying partners/users of any security updates.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.11	As part of the Security Policy develop specific contact web pages for Vulnerability Disclosure reporting.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.12	As part of the Security Policy provide a dedicated security email address and/or secure webform for Vulnerability Disclosure communications.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.13	As part of the Security Policy develop a conflict resolution process for Vulnerability Disclosures.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.13	As part of the Security Policy publish the organisation's conflict resolution process for Vulnerability Disclosures.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.14	As part of the Security Policy develop response steps and performance targets for Vulnerability Disclosures.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.15	As part of the Security Policy develop security advisory notification steps.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.16	The Security Policy shall be compliant with ISO 30111 or similar standard.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.2	The following is some proposed text for inclusion on a Vulnerability Disclosure page on a company website, to be approved by the company's legal team. Some companies also choose to specify what they consider to be unacceptable security research (such as that which would lead to the disclosure of customer data): *"[Company Name] takes security issues extremely seriously and welcomes feedback from security researchers in order to improve the security of its products and services. We operate a policy of coordinated disclosure for dealing with reports of security vulnerabilities and issues.* *To privately report a suspected security issue to us, please send an email to security alert@<companydomain>, giving as much detail as you can. We will respond to you as soon as possible. If the suspected security issue is confirmed, we will then come back to you with an estimate of how long the issue will take to fix. Once the fix is available, we will notify you and recognise your efforts on this page.* ***Thank You*** *Thanks to the following people who have helped make our products and services more secure by making a coordinated disclosure with us:* *[Name/alias, Twitter handle]"*	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.3	The email address securityalert@<companydomain> or security@<companydomain> is a de facto standard for researchers who disclose vulnerabilities to organisations. We recommend that organisations create and monitor both of these email addresses where possible. It is important to provide a secure mechanism for communication about security issues, to avoid any risk of the communication being intercepted and the information being used maliciously. It is recommended that organisations provide a secured web form for the initial contact message, as this does not require the reporting party to install email encryption software and the necessary encryption keys, which can be prone to error. Nevertheless, organisations should consider also publishing a public key with which emails can be encrypted for confidentiality.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.4	Security researchers may have a wide variety of backgrounds and expectations; they may be, for example, hobbyists unused to business processes, academics who desire the freedom to publish research, or professional consultants building a reputation for expertise in finding security problems. It is important, in communication with researchers, that due consideration and recognition is given to the effort that they have made into researching the particular security problem. Their motivation and expectations may well differ from yours, so it is imperative that they are given enough room to work with you and that a constructive, understanding tone is adopted at all times even if their actions may seem inappropriate in your business context.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.5	It is likely that at some point, there are going to be issues where both parties disagree. The Organisation for Internet Safety guidelines [OIS] included recommendations on how to resolve such conflicts in the context of an organisation's published vulnerability disclosure process. In summary: • Leave the process only after exhausting reasonable efforts to resolve the disagreement; • Leave the process only after providing notice to the other party; • Resume the process once the disagreement is resolved.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.6	The text on your security contact web page should state in what time frame the security researcher can expect a response; this will typically be a few days, perhaps up to a week. It is good practice to send an automatic acknowledgement for email sent to the contact email address including the same details on the expected response time. The following response should then further clarify expectations regarding the timing of further communications and, once a problem has been confirmed, in what time frame a patch, fix or other remediation is expected to be made available.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.7	The organisation should have a mechanism via which security advisories can be issued, so that users can be informed once a problem is fixed. This should be done via a secure webpage to authenticate the information. Some organisations also use security announcement mailing lists; it is good practice to digitally sign the advisory email text so that it can be authenticated.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.8	It is standard practice as a gesture of goodwill and recognition of security researchers' efforts to name security researchers who have cooperated in a vulnerability disclosure, although it is important to confirm their consent to this before publicly identifying them. The acknowledgement is often done on the same web page as the vulnerability disclosure policy. It is generally expected that a researcher's Twitter handle (if available) will also be included.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.9	Crediting a security researcher does not necessarily indicate that they are financially compensated and such compensation is not generally expected. Companies may wish to introduce “bug bounty” programmes or work with intermediaries who manage such programmes on behalf of companies, but this topic is out of the scope of these recommendations.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	2.10	It can be argued that, by publishing a Vulnerability Disclosure policy, organisations could be encouraging hackers in the name of security research. This is a misleading argument as, without a published policy, the organisation is turning a blind eye to research that would otherwise go on without its knowledge.Companies can fall into the trap of “shooting the messenger” when it comes to the disclosure of a vulnerability. This is why some people are suspicious of approaching a company when they discover a security issue. A company should, however, not encourage damaging activity. Some security pages explicitly exclude certain types of research – for example Denial of Service attacks on a site or the hacking into systems in order to expose customer data. An example of this can be found in the IoT Security Foundation’s own vulnerability disclosure policy: http://www.iotsecurityfoundation.org/security.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines	3	Successful vulnerability disclosure management must involve a nominated responsible person. It is suggested that this should be the CISO, or a Head of Security Response if one is appointed. In addition to this, it is recommended that confirmed disclosure emails sent to the disclosure email address are distributed to a list of senior staff that should be aware of disclosures that are underway. The remaining steps should continue as per the standard internal security incident handling processes of the organisation, with the added aspects of communicating with the security researcher on a regular basis to update and possibly asking for additional information or assistance. The final step is the creation of the security advisory and agreeing the “go public” date with the researcher.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/Vulnerability-Disclosure_WG4_2017.pdf
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 8	The public vulnerability disclosure contact details are clearly identified on both the manufacturers Device Security Level Agreement (DSLA) page and any solution web sites.	https://www.iotsi.org/iot-cybersecurity-principles
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	5	Establish coordinated vulnerability disclosure including processes and systems to receive, track and promptly respond to external vulnerability reports from third parties, including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications or other effective mechanism(s). Developers should consider “bug bounty” programs and crowdsourcing methods to help identify vulnerabilities.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Develop a policy regarding the coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT). The US Computer Emergency Readiness Team (US-CERT), Industrial	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			Control Systems (ICS)-CERT, and other CSIRTs provide regular technical alerts, including after major incidents, which provide information about vulnerabilities and mitigation.	
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Consider creating a publicly disclosed mechanism for using vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (A) (ii) (I)	(I) APPLICATION FOR WAIVER.—At the time of submitting a proposal to an executive agency, a contractor may submit a written application for a waiver from the requirement under clause (i)(I) for the purpose of disclosing a known vulnerability to the executive agency.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (A) (ii) (II)	(II) CONTENTS.—An application submitted under subclause (I) shall— (aa) identify the specific known vulnerability; (bb) include any mitigation actions that may limit or eliminate the ability for an adversary to exploit the vulnerability; and	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			(cc) include a justification for secure use of the device notwithstanding the persisting vulnerability.	
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (A) (ii) (III)	(III) APPROVAL.—If the head of the purchasing executive agency approves the waiver, the head of the purchasing executive agency shall provide the contractor a written statement that the executive agency accepts such risks resulting from use of the device with the known vulnerability as represented by the contractor.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (B)	B) NOTIFICATION REQUIRED.—A clause that requires the contractor providing the Internet-connected device software or firmware component to notify the purchasing agency of any known security vulnerabilities or defects subsequently disclosed to the vendor by a security researcher or of which the vendor otherwise becomes aware for the duration of the contract.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (b) (1)	(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the National Protection and Programs Directorate, in consultation with cybersecurity researchers and private-sector industry experts, shall issue guidelines for each agency with respect to any Internet-connected device in use by the United States Government regarding cybersecurity coordinated disclosure requirements that shall be required of contractors providing such software devices to the United States Government.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (b) (2) (A)	(2) CONTENTS.—The guidelines required to be issued under paragraph (1) shall— (A) include policies and procedures for conducting research on the cybersecurity of an Internet-connected device, which shall be based, in part, on Standard 29147 of the International Standards Organization, or any successor standard, relating to the processing and resolving of potential vulnerability information in a product or online service, such as— (i) procedures for a contractor providing an Internet-connected device to the United States Government on how to— (I) receive information about potential vulnerabilities in the product or online service of the contractor; and (II) disseminate resolution information about vulnerabilities in the product or online service of the contractor; and (ii) guidance, including example content, on the information items that should be produced through the implementation of the vulnerability disclosure process of the contractor; and	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (b) (2) (B)	(B) require that research on the cybersecurity of an Internet-connected device provided by a contractor to the United States Government shall be conducted on the same class, model, or type of the device provided to the United States Government and not on the actual device provided to the United States Government.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.4	The Director of NIST shall ensure that NIST establishes, maintains, and uses best practices in the identification and tracking of vulnerabilities for purposes of the National Vulnerability Database of NIST.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

Code of Practice: 3 - Keep software updated

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Digitisation of Industry Policy Recommendations	3.32 (i) Third bullet point	Promote that over the life cycle of any products and services there is regular updating of security measures, including to address emerging threats.	https://aioti.eu/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf
AT&T	The CEO's Guide to Securing the Internet of Things	Software/firmware update capability	Every network-connected device should have a means for authorized operators to update the device's software and firmware (e.g. softwareover- the-air/SOTA and firmware-over-the air/FOTA). Ideally, the updating process will be highly automated while still providing cryptographic checks to allow updates from an authorized source.	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
Atlantic Council Scowcroft Center for Strategy and Security	Smart Homes and the Internet of Things		A secure, prompt, and agile response to security or other flaws greatly reduces support costs, increases consistency of experience, and allows feature improvements over time.	http://www.atlanticcouncil.org/images/publications/Smart_Homes_0317_web.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations		**IoT Devices Should Ship with Reasonably Current Software.** BITAG recommends that IoT devices should ship to customers or retail outlets with reasonably current software that does not contain severe, known vulnerabilities. However, software bugs are somewhat of a "fact of life" and it is not uncommon for new vulnerabilities to be discovered while devices are on the shelf. Hence it is critical for an IoT device to have a mechanism by which devices receive automatic, secure software updates	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.1	**IoT Devices Should Have a Mechanism for Automated, Secure Software Updates.** BITAG recommends that manufacturers of IoT devices or IoT service providers should therefore design their devices and systems based on the assumption that new bugs and vulnerabilities will be discovered over time. They should design systems and processes to ensure the automatic update of IoT device software, without requiring or expecting any type of user action or even user opt-in.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.2	**Use Libraries That Are Actively Maintained and Supported.** Many of the recommendations in this report require implementing secure communications channels. Yet, home-grown implementations of cryptographic protocols and secure communications channels can themselves introduce vulnerabilities. BITAG recommends that, when implementing the recommendations in this report, device manufacturers use libraries and frameworks that are actively supported and maintained whenever possible.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
CableLabs	A Vision for Secure IoT	Lifecycle Management	IoT security requires vigilance throughout the life of the device – vulnerabilities will be discovered and new threats will emerge after the consumer purchases the device. IoT providers must make lifecycle management a central consideration in the design of every connected device and clearly disclose the key considerations to consumers prior to sale. Specifically, IoT providers must, with limited exception for ephemeral devices, provide secure, automated, software updates during the disclosed security support period. In addition, IoT providers must publicly disclose vulnerability remedies and changes to functionality at end-of-life (EOL)/end-of-support (EOS).	https://www.cablelabs.com/insights/vision-secure-iot/
CableLabs	A Vision for Secure IoT	Software Updates	IoT providers must provide secure, automated software updates throughout a clearly defined and disclosed security support period. By default, the software update mechanism should not require or rely on any consumer action. IoT providers incorporating a secure, automated software update mechanism into their devices recognize	https://www.cablelabs.com/insights/vision-secure-iot/

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			the reality that vulnerabilities are discovered in devices after they are deployed and that software updates can mitigate the risks associated with these vulnerabilities	
CableLabs	A Vision for Secure IoT	End-of-Life (EOL) / End-of-Support (EOS) Functionality	To protect end-users and third-parties, IoT providers should consider limiting device functionality after the security support period ends. Prior to sale, IoT providers should clearly disclose whether and to what extent device functionality will be limited due to an increased risk of vulnerability after the security support period ends To set consumer expectations, the disclosure should describe exactly what, if any, functionality will be limited at the end of the support period – whether only the “smart” functions and features (e.g., connectivity and control remotely through an app) will become inoperable, or whether core device functionality will be lost as well.	https://www.cablelabs.com/insights/vision-secure-iot/
CableLabs	A Vision for Secure IoT	Future (Upgradable) Security	IoT providers should consider and design into their products the ability to have strong security controls including secure cryptographic algorithms/cipher suites for the entire intended and expected life of the device. A device with a short lifespan (e.g., less than one year) may not require the capability to upgrade. In comparison, providers of connected, durable home appliances (e.g., expected service life of 10 or more years) should consider how the security controls will need to evolve over the life of the device.	https://www.cablelabs.com/insights/vision-secure-iot/
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	Medical Devices and Medical Standard Protocols are Vulnerable to Attack - 4	Provide an ability for customers to easily keep software components (e.g., web servers on the device patched)	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	IoT products may be deployed in insecure or physically exposed environments - 1	Apply policy based security to force IoT products to update latest security critical fw/sw	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.5	Life cycle controls for IoT edge devices require the management and monitoring of assets to ensure that they are authorized, and secure and regularly updated with the latest firmware, software and patches. In addition, organization's must have a documented method for securely disposing of IoT assets at the end of the life-cycle. Define a life-cycle management approach for IoT devices.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.5.3.1	Making sure that these updates are legitimate and haven't been tampered with is just as important as with traditional computing technology. System Administrators should outline a process for validating the authenticity and integrity of all updates, and ensure that the end-to-end process for retrieving, storing and then updating IoT devices is secured.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.3.2 first bullet point	If the organization is using any third party or open source libraries, then it is recommended to maintain an inventory of those libraries and keep them updated. Also, check the version and the corresponding vulnerabilities in those versions so that you can avoid using those vulnerable versions. This will ensure that security patches can be applied to the third party or open source libraries used.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.3.3 first bullet point	Take care regarding the sources of the update files and how they were transported. Make sure you scan the files or check for its integrity prior to installing them into your device. Check the "reputation" of a file, which can be done in a number of ways. Every computer file has a unique checksum—a relatively short mathematical value for the file. Another reputational characteristic of a file is how widely it has been used. Such assessments create a context for the file, indicating whether it is known to be good or bad or whether it is an unknown risk that should be monitored closely.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
European Commission and AIOTI	Report on Workshop on Security & Privacy in IoT	1) 5)	Life Time Protection – give security, safety and privacy protection over the full life time	http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf
European Commission and AIOTI	Report on Workshop on Security & Privacy in IoT	1) 6)	Updatability – trusted and transparent updates only by authorised parties, not by malicious actors	http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-05	Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow unauthenticated software, such software should only be run with limited permissions and/or sandbox.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-06	GP-TM-06: Restore Secure State - Enable a system to return to a state that was known to be secure, after a security breach has occured or if an upgrade has not been successful.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-18	Ensure the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), and that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins. Failing to build in OTA update capabilities will leave devices exposed to threats and vulnerabilities for the entirety of their lifetimes	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-19	Offer an automatic firmware update mechanism. Devices should be configured to check for the existence of firmware updates at frequent intervals. Automatic firmware updates should be enabled by default. A device may offer an option to disable automatic firmware updates and require authentication for it.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-20	Backward compatibility of firmware updates. Automatic firmware updates should not change network protocol interfaces in any way that is incompatible with previous versions. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. Users should have the ability to approve, authorise or reject updates.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-01	Develop an end-of-life strategy for IoT products. Security patches and updates will eventually be discontinued for some IoT devices. Therefore, developers should prepare and communicate a product sunset plan from the initial stages to ensure that manufacturers and consumers are aware of the risks posed to a device beyond its expected expiry date	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-02	Disclose the duration and end-of-life security and patch support (beyond product warranty). Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-03	Monitor the performance and patch known vulnerabilities up until the “end-of-support|” period of of a product’s lifecycle. Due to the limited life cycle of many IoT devices, critical, publicly known security or privacy bugs will pose a risk to consumers using outdated devices.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	7.2.2	Security updates provide protection against vulnerabilities found during the life of a device or application. However this comes at a cost, since support of this functionality also provides an entry point for an attacker. In particular vendors should: • Provide automatic and timely security updates. • Protect the updates (typically via encryption and digital signature). The update files must not contain sensitive data. The signature must be verified before the update is applied. • Protect the application of an update on the device. An attacker should not be able to trigger a firmware installation without an authorization. • Protect the security update interface against attacks.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.4	Over The Air Application Updates	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_5.10	Every system that is deployed by an organization, and every tier used, has a lifetime. Even if the same product or service is deployed by the organization for decades, the technologies used to drive that product or service will change. Thus, there must not only be a plan for designing and implementing the product or service, there must be a plan to sunset that product or service.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.12-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.6	Updating an execution environment, application image, or TCB is a challenging process. Consider the following example model that simplifies the overall process: • For each layer of the execution platform, define a network resource such as a unique URL for the new application image • Generate a signing key for each specific layer • For all new, authorized versions of each layer, generate an image of that layer • Include metadata describing the image (version, timestamp, identity, etc.) in the layer image • Sign the layer image with the signing key • Make the image, the signature, and the public key available, possibly via the unique network resource, or through a update service When a new system is deployed it should: • For each layer: o Retrieve the version(s) to be deployed o Cryptographically verify the image o Deploy the image layer on the system	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.12-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.5	This recommendation implies that a Patch Management process should be implemented by the organization to identify vulnerable services, deploy patches, and monitor the success of implementing those patches.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.12-v2.0.pdf
I am the Cavalry	Hippocratic Oath for Connected Medical Devices	Cyber Safety Updates	I understand that cyber safety will always change. I will support prompt, agile, and secure updates. Once an issue is known that could affect patient care, a faster response improves care delivery. Software updates are faster and less expensive than hardware replacement; and automated, remote software updates are most efficient. Increases in exposure are compensated for by the speed and scale of addressing flaws or weaknesses that could lead to negative outcomes.	https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
I am the Cavalry	Hippocratic Oath for Connected Medical Devices	Automation and documentation.	Update processes that are more automated and better controlled are less prone to error, delay, malice, misinterpretation, or other issues. Process documentation should outline clear roles and responsibilities for relevant stakeholders and allow development of corresponding processes inside stakeholder groups.	https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf
I am the Cavalry	Hippocratic Oath for Connected Medical Devices	Secure update process.	Processes should verify the authenticity and integrity of software updates to prevent adversarial, malicious, or accidental tampering. Remote update capability can give cost, reputational, and speed advantages if implemented in KNOWN good ways.	https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf
IEEE	IoT Security Principles and Best Practices	2	Inevitably vulnerabilities will be discovered after devices have been deployed. Devices must be patchable or upgradable. Naturally, device firmware should only be modifiable with the proper digital signature. As it stands, device vendors and manufacturers have little financial incentive in ensuring ongoing IoT patch upgrades since revenue comes from the sale of the device, not the maintenance. Upkeep of IoT devices may detract from revenue. In addition, vendors are not legally held accountable to ongoing maintenance of devices beyond initial sales and competition drives vendors to cut corners, negating on quality for efficiency and speed of release into the market. While these factors may not have been critical previous to IoT, the interconnected nature of IoT devices raises the bar to a new level in terms of functionality and accountability.	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
Industrial Internet	Industrial Internet of Things	7.3	**ENDPOINT PROTECTION.** Endpoint Secure Configuration and management controls updates of security policy and configuration	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Consortium (IIC)	Volume G4: Security Framework v1.0		at the endpoint, including upgrades and patches of known vulnerabilities.	
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.4	**COMMUNICATIONS AND CONNECTIVITY PROTECTION.** Network Configuration and Management controls updates to all network elements and provides enforcement of security policy and configuration for the communications, including network segmentation, cryptographically protected communications settings, and configuration of gateways and firewalls.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS.** Vulnerabilities in Configuration & Management, ⑬: Vulnerability of the Configuration & Management system may result from improper access control to the configuration management system, insertion of unauthorized changes in the system or corruption of update payloads. Updates to the endpoints should be planned and managed so as to limit the number of different operational configurations and reduce fragmentation of the fleet.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**ENDPOINT CONFIGURATION AND MANAGEMENT.** The endpoint must provide secure and controlled changes to the endpoint components, though in some rare cases no security is desired. All updates and changes should be signed, their payload encrypted and actions logged for subsequent auditing and recovery of the endpoint. These services should be provided non-intrusively to the operational functionality and have a separate logical connectivity to system-level configuration management and control.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	11.5.1	**SECURE SOFTWARE PATCHING AND FIRMWARE UPDATE.** As the amount and complexity of software increases, so does the number of defects, some of which will be exploitable vulnerabilities. Others may cause unpredictable system failures, timing issues, reduction in system performance, reliability or other unknown problems. Once discovered, these defects can often be fixed by patching. If over-the-air updates are implemented, network-related	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			vulnerabilities that affect the integrity of the over-the-air process should be addressed first.	
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.4.1	Vendors MUST offer an automatic firmware update mechanism. A discussion about the firmware update mechanisms can be found in [I-D.iab-iotsu-workshop].Devices SHOULD be configured to check for the existence of firmware updates at frequent but irregular intervals.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.4.2	Automatic firmware updates SHOULD be enabled by default. A device MAY offer an option to disable automatic firmware updates. Especially for any device for which a firmware update would disrupt operation, the device SHOULD be configurable to allow the operator to control the timing of firmware updates. If enabling or disabling or changing the timing of the automatic update feature is controlled by a network protocol, the device MUST require authentication of any request to control those features.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.4.3	Automatic firmware updates SHOULD NOT change network protocol interfaces in any way that is incompatible with previous versions. A vendor MAY offer firmware updates which add new features as long as those updates are not automatically initiated.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.4.4	To prevent widespread simultaneous failure of all instances of a particular kind of device due to a bug in a new firmware release, automatic firmware updates SHOULD be phased-in over a short time interval rather than updating all devices at once	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.4.5	Firmware updates MUST be authenticated and the integrity of such updates assured before the update is installed. Unauthenticated updates or updates where the authentication or integrity checking fails MUST be rejected. Firmware updates SHOULD be authenticated using digital signature items that use public key cryptography to verify the authenticity of the signer. Ordinary checksums or hash algorithms are insufficient by themselves, and keyed hashes that use shared secrets are generally discoverable by a determined attacker.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	5.1	Vendors MUST be transparent about their commitment to supply devices with updates before selling products to their customers and what happens with those devices after the support period finishes. Within the support period, vendors SHOULD provide firmware updates whenever new security risks associated with their products are identified. Such firmware updates SHOULD NOT change the protocol interfaces to those products, except as necessary to address security issues, so that they can be deployed without disruption to customers' networks. Firmware updates MAY introduce new features which change protocol interfaces if those features are optional and disabled by default.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.4	IoT devices are often expected to stay functional for several years and decades even though they might operate unattended with direct Internet connectivity. Software updates for IoT devices are therefore not only required for new functionality, but also to eliminate security vulnerabilities due to software bugs, design flaws, or deprecated algorithms.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.5	Like all commercial devices, IoT devices have a given useful lifetime. The term end-of-life (EOL) is used by vendors or network operators to indicate the point of time in which they limit or end support for the IoT device. This may be planned or unplanned (for example when the manufacturer goes bankrupt, when the vendor just decides to abandon a product, or when a network operator moves to a different type of networking technology). A user should still be able to use and perhaps even update the device. This requires for some form of authorization handover.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.3.25	Where remote software upgrade can be supported by the device, there should be a published /transparent and auditable policy and schedule of actions to fix any vulnerabilities found.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.2	Where remote software upgrade can be supported by the device, the software images are digitally signed by the organisation's approved signing authority.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.3	A software update package has its digital signature, signing certificate and signing certificate chain verified by the device before the update process begins.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.4	If remote software upgrade is supported by a device, software images shall be encrypted whilst being transferred to it.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.8	The product has protection against reverting the software to an earlier and potentially less secure version.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.9	The cryptographic key chain used for signing production software is different from that used for any other test, development or other software images, to prevent the installation of non-production software onto production devices.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.10	Production software images should be assessed on release to remove all unnecessary debug and symbolic information “Know what is being released, and have checks in place to prevent accidental release of superfluous data	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.11	Development software versions have any debug functionality switched off if the software is operated on the product outside of the product vendors’ trusted environment.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.2	Where remote update is supported, there is an established process/plan for validating and delivering updates on an on-going or remedial basis.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	Security Design Best Practices		Implement reliable and securely managed software/firmware update mechanisms throughout the solution that are link authenticated, encrypted as needed, and verified for authenticity and integrity before implementation on system.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Ship with, and maintain, security updated open source libraries used in products and services created.	https://www.iotsi.org/security-best-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 10	The software update support timespan and frequency are clearly identified in the manufacturers Device Security Level Agreement (DSLA) page.	https://www.iotsi.org/iot-cybersecurity-principles
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 11	All device Industry use classifications, with the allowed exception of "Consumer," provide a software patch update support timespan of not less than 6 years from manufacture date.	https://www.iotsi.org/iot-cybersecurity-principles
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 12	The Device Security Level Agreement (DSLA) for a device identifies the software update mechanism as either Direct-Physical, Remote-Network-Automatic, or Remote-Network-Manual facilitated.	https://www.iotsi.org/iot-cybersecurity-principles
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 14	A device with inbound network services running is supported with remote-network firmware updates by the manufacturer in order to remain in an operational state.	https://www.iotsi.org/iot-cybersecurity-principles
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 15	A device without a User Interface notification system and without an owner/operator patch notification system implements Remote-Network-Automatic firmware updates.	https://www.iotsi.org/iot-cybersecurity-principles
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 16	A device with a system classification of "Gateway" implements Remote-Network-Automatic firmware updates.	https://www.iotsi.org/iot-cybersecurity-principles
Microsoft	IoT Security Best Practices	Make upgrades secure	Firmware upgrades during the lifetime of the device are inevitable. Building devices with secure paths for upgrades and cryptographic assurance of firmware versions will allow the device to be secure during and after upgrades.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Microsoft	IoT Security Best Practices	Keep the system up-to-date	Ensure that device operating systems and all device drivers are upgraded to the latest versions. If you turn on automatic updates in Windows 10 (IoT or other SKUs), Microsoft keeps it up-to-date, providing a secure operating system for IoT devices. Keeping other operating systems (such as Linux) up-to-date helps ensure that they are also protected against malicious attacks.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	1	Disclose whether the device is capable of receiving security related updates, and if yes, disclose if the device can receive security updates automatically and what user action is required to ensure the device is updated correctly and in a timely fashion.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	6	Ensure a mechanism is in place for automated safe and secure methods to provide software and/or firmware updates, patches and revisions. Such updates must either be signed and/or otherwise verified as coming from a trusted source, including but not limited to signing and integrity checking	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	7	Updates and patches must not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where the device firmware or software is overwritten, on first use the user must be provided the ability to review and select privacy settings.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	8	Security update process must disclose if they are Automated (vs automatic). Automated updates provide users the ability to approve, authorize or reject updates. In certain cases a user may want the ability to decide how and when the updates are made, including but not limited to data consumption and connection through their mobile carrier or ISP connection. Conversely, automatic updates are pushed to the device seamlessly without user interaction and may or may not provide user notice	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	9	Ensure all IoT devices and associated software have been subjected to rigorous, standardized software development lifecycle testing including unit, system, acceptance, and regression testing and threat modeling, along with maintaining an inventory of the source for any third-party/open source code and/or components. Employ generally accepted code and system hardening techniques across a range of typical use case scenarios, including prevention of any data leaks between the device, apps and cloud services. Developing secure software requires thinking about security from a project's inception through implementation, testing, and	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			deployment. Devices should ship with current software and/or on first boot push automatic updates to address any known critical vulnerabilities.	
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	19	Disclose the duration and end-of-life security and patch support (beyond product warranty). Support may end on a sunset date, such as January 1, 2025, or for a specific duration from time of purchase, not unlike a traditional warranty. Ideally such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase. (It is recognized that IoT devices cannot be indefinitely secure and patchable. Consider communicating the risks of using a device beyond its usability date, and impact and risk to others if warnings are ignored or the device is not retired). If users must pay any fees or subscribe to an annual support agreement this should be disclosed prior to purchase.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.1.3	Secure download and boot – To prevent the loading and execution of malicious software, where it is practical, it is recommended that Secure Download and Secure Boot methods that authenticate a binary's source as well as its contents be used.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf
Open Web Application Security Project (OWASP)	IoT Security Guidance	I9: Insecure Software/Firmware	Ensure all system devices have update capability and can be updated quickly when vulnerabilities are discovered	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security	IoT Security Guidance	I9: Insecure Software/Firmware	Ensure update files are encrypted and that the files are also transmitted using encryption	https://www.owasp.org/index.php/IoT_Security_Guidance

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Project (OWASP)				
Open Web Application Security Project (OWASP)	IoT Security Guidance	I9: Insecure Software/Firmware	Ensure that update files are signed and then validated by the device before installing	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I9: Insecure Software/Firmware	Ensure update servers are secure	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I9: Insecure Software/Firmware	Ensure the product has the ability to implement scheduled updates	https://www.owasp.org/index.php/IoT_Security_Guidance
Symantec	An Internet of Things Security Reference Architecture		IoT systems must have update capabilities built into them from the beginning. Failing to build in OTA update capabilities will leave devices exposed to threats and vulnerabilities for the entirety of their lifetimes. Of course, such update capabilities can be used to manage device configurations, security content, credentials and much more. Similarly, such update capabilities can be used to push functionality and collect telemetry in addition to collecting software inventory information and pushing security patches. However, with or without such additional functionality, basic update capabilities and the ability to manage the security posture of each device must be built into the device from the beginning.	https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Consider ways in which to secure the device over network connections or through automated means. Ideally, patches would be applied automatically and leverage cryptographic integrity and authenticity protections to more quickly address vulnerabilities.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Consider coordinating software updates among third-party vendors to address vulnerabilities and security improvements to ensure consumer devices have the complete set of current protections.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Develop an end-of-life strategy for IoT products. Not all IoT devices will be indefinitely patchable and updateable. Developers should consider product sunset issues ahead of time and communicate to manufacturers and consumers expectations regarding the device and the risks of using a device beyond its usability date.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.3.3	**Secure System Modification.**The principle of secure system modification states that system modification must maintain system security with respect to the security requirements and risk tolerance of stakeholders. Upgrades or modifications to systems can transform a secure system into an insecure one. The procedures for system modification must ensure that, if the system is to maintain its trustworthiness, the same rigor that was applied to its initial development is applied to any changes.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Mitigations: Signing the update payload cryptographically protects the integrity of the payload, including from undetected intentional modification by a bad actor. It also provides authenticity in the provenance of the payload. This is different from a more traditional approach of using noncryptographic hash such as a cyclic redundancy check (CRC) or a checksum. These noncryptographic hashes can validate the integrity against naturally occurring corruption of the payload, but can be easily subverted by bad actors. Similarly, failure to use a strong enough cryptographic signature or hash function also fails to completely mitigate these risks. For older, weaker hash functions, an attacker with sufficient motivation and resources could generate a malicious update that generated the same hash as the legitimate update.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Mitigation: Encryption of the update before transmission and decryption of the update on the device can reduce the risk of exposure during transmission regardless of the communications path(s) of the update deliverable.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Basic Implementation: Transport-layer encryption, such as TLS or BLE 4.2+, can provide widely-accepted levels of security between the endpoints. Using features such as pinning of certificates in TLS can authenticate the source, and user-pairing of devices in BLE can authenticate endpoints. VPNs also offer confidentiality and integrity of data in motion.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		The device receives the update. No design risks are specifically associated with the required step. However normal good security hygiene practices should be followed, such as mitigations against buffer overflow	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Basic implementation: In addition to the signature and encryption features above, a monotonic versioning system can prevent a downgrade attack. Further security considerations: A system capable of disallowing previous versions requires an additional step for a manufacturer-driven rollback update, and can make user-driven rollbacks more complex. Alternatively, the device can securely validate the path and source of the update to ensure that the older version is not coming from an untrustworthy source	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Basic Implementation: Manufacturer should consider the use and installation of a device to determine the optimal approach to automatic updates, user control, and uptime criticality. Depending on the context and use case, there will likely be a need for a balance between giving a user a choice in the updating of devices and pushing an update after a period of time for the good of the user and everyone else on the internet. For more on the question of end user approval of updates, see “Communicating IoT Device Security Update Capability to Improve Transparency for Consumers” by the Working Group on Communicating Upgradability. Further Security Considerations: If the user does not take action to update the device, the manufacturer or device administrator may wish to take further actions at a future date. How to address a non-updated device is outside the scope of this document.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Basic Implementation: Update image remains encrypted and integrity protected while in motion if traveling across exposed transport media. Support is provided for multiple of layers of systems, devices, or CPUs to be targeted. Further Security Considerations: The adversary might still be able to try to compromise nonexposed internal communication channels. To address this residual risk, the update image should remain encrypted while in motion.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Similar to the “Check” step above, however this may be performed on a target in a lower “child” relationship, if a hierarchical relationship between update targets is implemented. Basic Implementation: Each target validates the integrity of the plain text update image using a cryptographic hash signature. Each target decrypts its specific update image, if encrypted.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		During this step, any activities necessary to performing the update on the device can occur, including functions such as erasing flash memory, placing the device in a “safe mode” of operation, ensuring sufficient battery life to complete the operation, etc. Basic Implementation: No security features are assumed; manufacturer may define them in specific contexts.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		The actual update process occurs. This includes writing to a file structure, updating the binary program space in flash memory, etc. Basic Security Implementation: No special processing is assumed Further Security Considerations: When updating multiple internal targets coordination of timing should be considered. If needed, conversion of persistent data on each target should occur during this step. Update is placed into a separate flash region from existing image for reliability purposes (in case a failed update requires a rollback to the previous working version)	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Mitigation: A redundant test of update integrity would confirm that the process of writing the update image to the intended target was performed correctly and that no malicious actor or device / memory failure altered the intended update image. Basic Implementation: Each target vets the integrity of the installed update. Further Security Considerations: Potentially use cryptographic hashing.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Once the code has been verified, it is actually enabled, and execution path switches to the new, updated code. No additional risks are incurred during this step. Basic Implementation: No special processing is assumed Further Security Considerations: If multiple flash images are stored (redundant duplicate copies, or previous and current), then activation may entail pointing to the new image for subsequent boot cycles.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US National Telecommunications and Information Administration (NTIA)	Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching		Basic Implementation: No special processing is assumed Further Security Considerations: If one is concerned about accidental or intentional communication failure, several mitigations exist. One approach is to allow remote querying by a central server. However, this can introduce further risks of attack by confusion or denial of 11 service. Discerning legitimate requests may require further validity checks. It is left up to the implementer to identify the appropriate solution. For robustness of the system, one concern is coordination of versions between targets on a multi-target system. One solution is notification of successful update across the system by each target.	https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (A) (i) (II)	IN GENERAL.—A clause that requires the contractor providing the Internet-connected device to provide written certification that the device— (II) relies on software or firmware components capable of accepting properly authenticated and trusted updates from the vendor;	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (C)	(C) UPDATES.—A clause that requires such Internet-connected device software or firmware component to be updated or replaced, consistent with other provisions in the contract governing the term of support, in a manner that allows for any future security vulnerability or defect in any part of the software or firmware to be patched in order to fix or remove a vulnerability or defect in the software or firmware component in a properly authenticated and secure manner.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (D)	(D) TIMELY REPAIR.—A clause that requires the contractor to provide a repair or replacement in a timely manner in respect to any new security vulnerability discovered through any of the databases described in subparagraph (A)(i)(I) or from the coordinated disclosure program described in subsection (b) in the event the vulnerability cannot be remediated through an update described in subparagraph (C).	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (E)	(E) CONTINUATION OF SERVICES.—A clause that requires the contractor to provide the purchasing agency with general information on the ability of the device to be updated, such as— (i) the manner in which the device receives security updates; (ii) the anticipated timeline for ending security support associated with the Internet-connected device; (iii) formal notification when security support has ceased; and (iv) any additional information recommended by the National Telecommunications and Information Administration.	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

Code of Practice: 4 - Securely store credentials and security-sensitive data

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Preset Certified Security Structures	Encryption requirement for identities, access, communication channels and secure storage of keys and to store data at rest – also for secure boot process.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.2	**Encrypt Local Storage of Sensitive Data.** BITAG recommends that any sensitive or confidential data (e.g., private key, pre-shared key, user or facility information) reside in encrypted storage.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.2	**Use Unique Credentials for Each Device.** BITAG recommends that each device have unique credentials. If a device uses public-key cryptography (e.g., to sign messages, exchange a session key, or authenticate itself) each device should have a unique, verifiable certificate. If a device is using symmetric key cryptography, pairs of endpoints should never share the symmetric key with other parties.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.2	**Use Credentials That Can Be Updated.** BITAG recommends that device manufacturers support a secure mechanism by which the credentials used by a device can be updated. However, implementing this recommendation securely requires particular care, since an incorrect implementation may itself introduce a new attack vector.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
CableLabs	A Vision for Secure IoT	Confidentiality	Strong confidentially protections ensure sensitive information remains private and inaccessible to unauthorized parties. Ensuring the confidentiality of sensitive information goes beyond just encryption. IoT devices should protect sensitive data at rest, in use, and in transit and limit the information disclosed in response to anonymous or untrusted requests. The IoT device manufacturer must first identify the sensitive information a device handles. This may include personally identifiable information (PII), protected health information (PHI), credentials, and private keys, to name just a few categories.	https://www.cablelabs.com/insights/vision-secure-iot/
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	IoT products may be deployed in insecure or physically exposed environments - 3	Encrypt indentify/key material within mobile applications when used to establish trust relationships with IoT products	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	Resource constraints in embedded systems limit security options - 1	When possible, use hardware-based security controls to safeguard sensitive information	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.4	Identifying the cryptographic algorithms and key sizes to support within an IoT device is only one aspect of the cryptographic puzzle. These algorithms must be able to operate within a trusted environment and keys must be stored within secure containers. Within larger systems, designers often employ Hardware Security Modules (HSM) for key storage and operations, however HSMs are often not viable for the IoT. Instead designers must explore other options, such as the Trusted Execution Environment (TEE) and Trusted Platform Module (TPM).	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.4.1.1	Depending on the complexity of the IoT device, many application-specific data elements may need to be encrypted when not actively used in executable processes. The device should encrypt these parameters using a DAR encryption key securely stored in a physically hardened, locked down cryptographic module resident in the device. In addition to sensitive application data, all secret and private keys, authentication, access control and other security configurations should be stored encrypted if possible. DAR security is designed to protect private information (e.g., medical data) in the event of device theft or loss.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-01	Employ a hardware-based immutable root of trust. The Hardware Root of Trust is a trusted hardware component which receives control at power-on. It then extends the chain of trust to other hardware, firmware, and software components. The Root of Trust should then be attestable by software agents running within and throughout the infrastructure.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information	Baseline Security Recommendations for IoT	GP-TM-34	Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Security (ENISA)				
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-35	Cryptographic keys must be securely managed. Encryption is only as robust as the ability for any encryption based system to keep the encryption key hidden. Cryptographic key management includes key generation, distribution, storage, and maintenance.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-36	Build devices to be compatible with lightweight encryption and security techniques (including entities secure identification, secure configuration, etc.) that can, on the one hand, be usable on resource-constrained devices, and, on the other hand, be scalable so to minimise the management effort and maximise their usability	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-38	Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud, using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information	Baseline Security Recommendations for IoT	GP-TM-40	Ensure credentials are not exposed in internal or external network traffic.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Security (ENISA)				
GSMA	GSMA IoT Security Assessment	CLP13_6.2	Utilise a Trust Anchor	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.6	Endpoint devices must be enabled with cryptographically unique identities to ensure that adversaries, competitors, and hobbyists can't impersonate other users or devices in production environments. To accomplish this adequately, the personalization process must be performed at fabrication. This can be done either through the manufacturer of the particular TCB solution, or during the Printed Circuit Board Assembly (PCB/A) process.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.1	Where possible, processors should use internal CPU memory for the processing of core secrets and cryptographic keys not contained within a trust anchor. This will ensure that if an adversary is monitoring, or capable of manipulating, the memory bus, they will not obtain core secrets, but will only see the effects of the use of these secrets on a running application.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.12	Do not place private cryptographic components in insecure storage on Endpoints, such as SSH private keys, TLS private keys, or passwords Screen reader support enabled.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_9.4	A cold boot attack is a physical attack strategy against computer systems that extracts secrets from a running computer by removing the physical memory from the computer, and placing the memory in a secondary system controlled by the adversary. The benefit of this attack is that the Attacker can run a custom operating system that dumps the contents of RAM to permanent storage. This will allow the Attacker to comb through the retrieved data and determine if there are security related tokens that can be used.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_5.2	An Organizational Root of Trust is a certificate or public-key based system for authenticating computing platform entities in an organization. Each computing platform in a Service Ecosystem must be cryptographically authenticated during network communications. This diminishes the ability for an insider, or someone within a privileged network position, to impersonate or otherwise abuse the trust of a privileged system. To build an Organizational Root of Trust, simply perform the following actions: • Build or acquire, for example, a Hardware Security Module (HSM) to store the organizational root secret • Generate a root secret and/or certificate • Ensure the private facet of the secret is stored securely • Generate a set of one or more signing keys to be used for Tier TCB signing key • Sign the public facet of the signing key with the organizational root • Ensure these keys cannot be used without authentication and authorization from the business and engineering leads	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	11.7.2	**CREDENTIAL MANAGEMENT PHASE.** After the enrollment phase, the credential management phase comprises a number of steps broken down into two categories. The first category comprises the steps required to generate credentials, bind them to an entity, and issue them to the entity to which the credential should be issued. The second category comprises the steps for storing credentials, and end-of-life as well as extending the useful life of the credential. The first category of steps for credential management brings the entity into the state where the credentials are in place and ready to use. Credential generation includes any steps required to create the credential itself, or to enable or direct the entity to create the credential. Then, during credential binding, the credential, or the means to create it, is associated to the identity assigned to the entity. Finally, during credential issuance, the credential, or the means or directive to create it, is delivered to the entity using a secured and auditable process. The specific process depends on the organizational policy for the environment.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.2.2	A device MUST be designed to protect any secrets used to authenticate to the device (such as passwords or private keys) from disclosure via monitoring of network traffic to or from the device. For example, if a password is used to authenticate a client to the device, that password must not appear "in the clear", or in any form via which extraction of the password from network traffic is computationally feasible.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.10	ne existing solution to prevent such data leaks is the use of asecure element, a tamper-resistant device that is capable of securely hosting applications and their confidential data. Another potential solution is the usage of of Physical Unclonable Function (PUFs) that serves as unique digital fingerprint of a hardware device. PUFs can also enable other functionalities such as secure key storage. Protection against such data leakage patterns is non-trivial since devices are inherently resource-constrained. An open question is whether there are any viable techniques to protect IoT devices and the data in the devices in such an adversarial model.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.7	The product's software signing root of trust is stored in tamper resistant memory.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.19	The production software signing keys are under access control.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.4	Files and directories are set to appropriate access privileges on a need to access basis.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.5	Passwords file(s) are owned by and are only accessible to and writable by the Devices' OS's most privileged account.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.8	The product's OS kernel and its functions are prevented from being called by external product level interfaces and unauthorised applications.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.9	Applications are operated at the lowest privilege level possible.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.10	All the applicable security features supported by the OS are enabled.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.11	The OS is separated from the application(s) and is only accessible via defined secure interfaces.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.12	All network communications keys are stored securely, in accordance with industry standards such as FIPS 140 [5] or similar.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.1	The product contains a unique and tamper-resistant device identifier (e.g. such as the chip serial number or other unique silicon identifier) which is used for binding code and data to a specific device hardware.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.2	Where the product has a secure source of time there is a method of validating its integrity, such as Secure NTP. https://www.ntpsec.org/.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.8	The product securely stores any passwords using an industry standard cryptographic algorithm, compliant with an industry standard such as NIST SP800-63b [26] or similar.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.9	The product supports access control measures to the root account to restrict access to sensitive information or system processes.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism cannot readily be abused by an unauthorised party.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.16	The product allows an authorised factory reset of the device's authorisation information.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.4	There is a secure method of key insertion that protects keys against copying.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.7	The product stores all sensitive unencrypted parameters, (e.g. keys), in a secure, tamper-resistant location.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.9	In device manufacture all asymmetric encryption private keys that are unique to each device are secured in accordance with FIPS 140 [ref 5] and truly randomly internally generated or securely programmed into each device.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.11.5	The product securely stores any passwords using an industry standard cryptographic algorithm, for example see FIPS 140 [5].	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.16	All the related servers and network elements store any passwords using a cryptographic implementation using industry standard cryptographic algorithms, for example see FIPS 140 [5].	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	Security Design Best Practices		Make use of chip-level security and virtualization capabilities, and utilize crypto coprocessors for key creation and storage.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		All stored secrets are vulnerable to compromise with enough time and/or resources – ALL. Design and mitigate weakness per risk tolerance.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Utilize trusted platform modules (TPM), secure elements (SE), and other hardware security modules (HSM) for storing and processing cryptographic secrets.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Use high-iteration, heavy-salt, key derivation functions such as scrypt/jane, bcrypt and PBKDF2 for storing account passwords.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Use sufficiently large, as well as high quality, entropy for encryption routines.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		When in question over possible data sensitivity or privacy, just encrypt.	https://www.iotsi.org/security-best-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Microsoft	IoT Security Best Practices	Keep authentication keys safe	During deployment, each device requires device IDs and associated authentication keys generated by the cloud service. Keep these keys physically safe even after the deployment. Any compromised key can be used by a malicious device to masquerade as an existing device.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Microsoft	IoT Security Best Practices	Build around secure hardware	If COGS permits, build security features such as secure and encrypted storage, or boot functionality based on Trusted Platform Module (TPM). These features make devices more secure and help protect the overall IoT infrastructure.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
MIT Laboratory for Computer Science	Dos and Don'ts of Client Authentication on the Web	3.2 Protect passwords	Passwords are the primary means of authenticating users on the Web today. It is important that any Web site guard the passwords of its users carefully. This is especially important since users, when faced with many Web sites requiring passwords, tend to reuse passwords across sites.	http://pdos.csail.mit.edu/papers/webauth:sec10.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	6.1	Sensitive data comprises key material/credentials, privacy related data such as identifiers and other data as identified by the M2M Solution Provider for the purpose of its use case. In order to prevent misuse of sensitive data, it requires protected and secure storage within the termination points of the M2M System. Secure storage capability can be implemented by several means within the network infrastructure nodes and network applications by the M2M Service Provider. In addition it needs to be ensured that secure storage capabilities are present in the termination node residing at the consumer, i.e. in the M2M Device and/or the M2M Gateway, depending on the requirements of the use case. It is highly recommended that M2M Devices/Gateways support a secure and tamper resistant storage capability for sensitive data, in particular when they are physically exposed to potential attackers.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.1	M2M long-term service-layer keys are stored in a HSM (whose tamper-resistance may be certified) residing within the M2M Device/Gateway which renders it infeasible for the attacker to discover the value of keys by logical or physical means.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.2	M2M long-term service-layer keys (other than public keys) are securely stored in a server-HSM residing in infrastructure equipment which renders it infeasible for the attacker to discover the value of keys by logical or physical means	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.3	HSM/server-HSM do not reveal the value of the stored secret keys (other than public keys), even to a management system or to an authorized representative of the M2M System Operator, such as a System Administrator.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.4	The execution of Sensitive Functions never causes long-term service-layer keys to be exposed outside of the HSM in which they are stored. Sensitive functions may be executed within the HSM.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.6	Access to and/or modification of stored Sensitive Data and in particular of the long-term service-layer keys requires strong (i.e. cryptographic) authentication of the accessing/modifying entity, followed by authorization.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	17	Authentication credentials, including but not limited to user passwords, shall be salted, hashed and/or encrypted. Applies to all stored credentials to help prevent unauthorized access and brute force attacks.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.1	Secure storage refers to the physical method of housing sensitive or confidential data (“Sensitive Data”). Such data could include but not be limited to symmetric or asymmetric private keys, certificate data, network access credentials, or personal user information. Sensitive Data requires that its integrity be maintained, whereas Critical Sensitive Data requires that both its integrity and confidentiality be maintained.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.1.1	Hardware secure storage is recommended for use with critical Sensitive Data such as symmetric and asymmetric private keys, access credentials, personal private data. Hardware secure storage most often involves semiconductor-based non-volatile memory (“NVRAM”) and includes countermeasures for protecting against unauthorized access to Critical Sensitive Data.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.1.2	It is generally NOT recommended to rely solely on software and unsecured memory to store Sensitive Data even if it is encrypted. Critical Sensitive Data such as authentication and encryption keys should be housed in hardware secure storage whenever possible. Sensitive Data stored in volatile and non-volatile memory shall be encrypted using acceptable algorithms to prevent access by unauthorized parties through methods described in section 15.1.1.1.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.1.2	Isolation of execution of sensitive processes from unauthorized parties/ processes. This 2502 includes isolation of CPU caches, and all of execution elements that needed to be 2503 considered as part of trusted (crypto) boundary.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1	**Execution environment elements.** Execution environment within a computing device has many components. To perform security functions in a robustness manner, each of these components has to be secured as a separate dimension. For instance, an execution environment performing AES cannot be considered secure if the input path entering keys into the execution engine is not secured, even though the partitions of the CPU, performing the AES encryption, operate in isolation from other processes. Different dimensions referred to as elements of the execution environment are listed below. To qualify as a secure execution environment (SEE), the corresponding SEE element must qualify as secure. • (secure) Storage • (Secure) Execution engine • (trusted) Input/output paths • (Secure) Time Source/clock • (random) number generator • (approved) cryptographic algorithms • Hardware Tamper (protection)	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf

Code of Practice: 5 - Communicate securely

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Basic Requirements on IoT HARDWARE AND COMPONENTS	Interoperability of components and communication protocols.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Basic Requirements on INTERFACES, COMMUNICATION, CLOUD	Security and data Management process and clarification of ownership required; easy to adopt; data should also be encrypted on the application layer; all aspects of cryptographic principles and key management are extremely important and should be carefully described.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.1	**IoT Devices Should Use Strong Authentication by Default.** BITAG recommends that IoT devices be secured by default (e.g. password protected) and not use common or easily guessable user names and passwords (e.g., “admin”, “password”). Finally, authentication for remote access should be secured, as it potentially allows others who are not physically present in the home to monitor and control aspects within the home (e.g., changing climate controls, monitoring user activity). Authentication credentials should be unique to each device.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.2	**IoT Devices Should Follow Security & Cryptography Best Practices.** BITAG recommends that IoT device manufacturers secure communications using Transport Layer Security (TLS) or Lightweight Cryptography (LWC) [96,97,98]. Some devices can perform symmetric key encryption in near-real time. In addition, Lightweight Cryptography (LWC) provides additional options for securing traffic to and from resourceconstrained devices. If devices rely on a public key infrastructure (PKI), then an authorized entity must be able to revoke certificates when they become compromised, as web browsers and PC operating systems do [99,100,101,102,103,104,105]. Cloud services can strengthen the integrity of certificates issued by certificate authorities through, for example, participating in Certificate Transparency [106]. Finally, manufacturers should take care to avoid encryption methods, protocols, and key sizes with known weaknesses. Vendors who rely on cloud-hosted support for IoT devices should configure their servers to follow best practices, such as configuring the TLS implementation to only accept the latest TLS protocol versions.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.2	**Encrypt Configuration (Command & Control) Communications By Default.** BITAG recommends that all communication for device management take place over an authenticated and secured channel.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.2	**Secure Communications To and From IoT Controllers.** If IoT devices use a centralized controller to facilitate over-the-Internet communication with a cloud service, then BITAG recommends this communications channel be secured in both directions.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
CableLabs	A Vision for Secure IoT	Authentication, Authorization, and Accountability - Onboarding	Secure authentication, authorization, and accountability minimize the potential for compromising a device or other devices in the local IoT ecosystem during the onboarding process. “Onboarding” is the process by which a new device is connected and added to the network and the local IoT ecosystem. Onboarding includes the processes for authentication, authorization, and accountability (AAA) of that new device. Authentication is the process by which the device identity is verified and confirmed. Authorization determines what network resources the device will have access to. And, accountability is the process that tracks what the device does	https://www.cablelabs.com/insights/vision-secure-iot/
City of New York (NYC) Guidelines for the Internet of Things	Security	4.2	IoT systems should utilize established security frameworks, where possible, and ensure communication between components is tightly constrained.	https://iot.cityofnewyork.us/security/
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	IoT Products Can Compromise Privacy - 1	Encrypt all account registration using Transport Layer Security (TLS)	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	Drones Are Approaching Mainstream Status and Being Used as a Platform for Reconnaissance - 1	Carefully evaluate the chosen IoT communication protocols for your product and configure in modes that limit the amount of information shared	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	Critical national infrastructure can rely on the IoT ecosystem - 3	Implement secure interface connectivity within your IoT products	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.3.2 eighth bullet point	The encryption of data during transport must be able to take into consideration the resource constrained devices and hence must have a small footprint be lightweight instead of the traditional ones to avoid performance bottlenecks.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.4.1.2	Data-in-Transit refers to the sending or receiving of data (application, management commands, status, etc.) over a link or network. Whenever possible, DIT protections should include cryptographic confidentiality (encryption), integrity and authentication algorithms executed by a properly integrated cryptographic module. Well-validated network and/or application security protocols should be utilized to provide end-to-end DIT security whenever possible.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.7.3	Ensure that security data from edge devices and aggregators is encrypted and authenticated during transport.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	1	All stakeholders should reach a consensus on security requirements	https://www.ENISA.europa.eu/publications/security-resilience-good-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	2	Industry actors should support security-driven business models	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-04	Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided. Purely proprietary approaches and standards limit interoperability and can severely hamper the potential of the Digital Single Market. Common open standards will help users access new innovative services, especially for SMEs, the public sector and the scientific community. In particular, the portability of applications and data between different providers is essential to avoid lock-in.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-07	Use protocols and mechanisms able to represent and manage trust and trust relationships. Each communication channel must be trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions).	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-34	Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-37	Support scalable key management schemes. It has to be considered that tiny sensor nodes cannot provide all security features because they have lots of system limitations. Thus, the sensed data carried over infrastructure networks may not have strong encryption or security protection.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-38	Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud, using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-39	Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-40	Ensure credentials are not exposed in internal or external network traffic.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-41	Guarantee data authenticity to enable trustable exchanges (from data emission to data reception - both ways). Data is often stored, cached, and processed by several nodes; not just sent from point A to point B. For these reasons, data should always be signed whenever and wherever the data is captured and stored.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-52	Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	5.2, second bullet point	Communication protection: communication should be protected against disclosure, modification, replay and denial of service.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	5.2, third bullet point	Cryptography: Confidentiality, integrity and authenticity must be protected by using strong and standard cryptography. Keys must be managed securely, and the use of a trust infrastructure (such as PKI) is encouraged.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	A.1.3	The usage of dedicated security mechanisms varies depending on the solution used. Several approaches are taken, from the transport to the applicative layer: • User authentication/authorization protocols such as Oauth / OpenID, XACML/SAML Single sign-on etc. • Communication protection protocols such as SSL/TLS over TCP/IP, or DTLS over UDP. • Usage of cryptographic algorithms to secure transport layer is found amongst many of the communication protocols.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	6.2	Using a trust infrastructure give assurance in heterogeneous environments where devices may enter or quit a given networks, and cannot necessarily be trusted by default. Smart Home is a good example of environments where trust is needed: • between the devices; and • between the devices and remote services.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.19	Endpoint Communication Security	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Network Operators	CLP14_5.2	This section contains recommendations and best practices for network authentication and link encryption for different wide area networks.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.14-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.4	Once a root of trust has been established within the TCB, a protocol must be used that incorporates the TCB's capabilities and the root of trust effectively.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.12	Enforce confidentiality and integrity on the administrative communications channel	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.12	Diminish the potential for replay of administrative commands by ensuring the communications protocol has adequate entropy by using an industry standard communications protocol	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.4	All communications to and from the trust anchor should be authenticated and should enforce confidentiality and integrity. The only exception to this model is if the trust anchor is internal to the core of the processor. Any external trust anchor, such as a UICC, can only be trusted if the messages received and sent can be trusted. To do this, choose trust anchors that are capable of authentication and encryption and validate that all messages containing answers to challenges are sent confidentially and, where possible, with verifiable integrity.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.6.1	All environments are vulnerable to spoofing. For example, any Cellular radio can signal that it is the owner of any given International Mobile Subscriber Identity (IMSI), whether it is true or not. Any laptop can change its Ethernet address, impersonating other computers on the Local Area Network (LAN). Regardless of whether the topology traverses a physical or an airwave space, a communication Endpoint's identity can be impersonated.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.6.2	In the 3GPP model, only Endpoints (called User Equipment in 3GPP) are authenticated. Endpoints do not authenticate the base stations they connect to. Thus, any base station can claim to serve on behalf of any Cellular carrier. Individuals capable of manipulating or building a Cellular base station may then impersonate any Cellular carrier of their choosing. A custom Cellular base station currently costs under 1,000 USD to build, but the resultant power only allows the interception of messages in the local area. Once the fake tower is built, the base station can impersonate a local Cellular carrier, and intercept phone calls, text messages, and even data, from Endpoints in the local area Newer 3GPP network protocols, such as UMTS and LTE, enforce mutual authentication of both entities. This allows Endpoints to cryptographically verify that the base station is serving on behalf of the Cellular carrier it claims to serve. An adversary must now break the Cellular carrier's cryptography to impersonate a base station, significantly increasing the complexity, difficulty, and cost of an attack.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.6.4	Bringing up Cellular interrogators helps summarize this section quite adequately by touching on the idea that communications security is not absolute. It only protects the communication channel between two entities. These entities, however, act as gates allowing data to pass in and out of the ecosystems these entities are connected to. For example, a particular SIM card may be provisioned for use in an industrial control system such as an oil well monitoring device. A SIM card, by design, is a removable component. Anyone with physical access to the oil well monitoring device can extract the SIM card and place it in a laptop. If the laptop has software on it that can simulate the functionality of the oil device, the back-end server will be unable to differentiate between the actual oil device and the laptop. Yet, the laptop will be authenticated to the Cellular network because of the SIM card! Thus, the Cellular network has authenticated the SIM card, but not the laptop.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.6.5	Each peer in an IoT ecosystem must authenticate all other peers that participate in that ecosystem. To accomplish this, a TCB must be used to ensure that proper cryptographic architecture is driving the communications technology. Mutual authentication can't occur if keys are easily exposed to adversaries. Review the TCB section of this document for more information.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_8.9	Endpoints, especially Gateways, or Endpoints acting as Gateways, must be capable of enforcing communications security even in environments where connectivity to the back-end network is unavailable. Regardless of whether this lack of connectivity is temporary or not, the Gateway or Endpoint must be capable of enforcing security as if the back-end system were available. To achieve this, the TCB must be used to authenticate all peers that the Endpoint must communicate privacy-centric, configuration, or command data to. The TCB can be used to ensure that messages sent and received from peers are being sent and received from an entity that has been provisioned by the same organization. This reduces the likelihood that an adversarial device is being communicated with.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.2	All technology deployed in an IoT environment must use cryptography, regardless of whether the technology is a rudimentary low-power endpoint, or a robust Cloud service. To properly implement security in an IoT product or service, the cryptography used must be well architected, managed, and adjusted to meet changing specifications over time.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.3	Each system in the Service Ecosystem must be capable of mutual authentication. No computing platforms within this ecosystem should be accessible to anonymous public users. Each Endpoint, Partner, or User will communicate with the Service Ecosystem through technologies that require mutual authentication. Since the services that make up the user interface are typically deployed and managed in a separate environment, the publicly accessible interface must be confined to that space. The Service Ecosystem, however, comprises the set of all system used to deploy service to all authenticated resources.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.4	Network Operators, when used as partners, allow users to be authenticated using tokens specific to the network operator. While these tokens, present in the Network Operator's UICC, authenticate a user to the network layer, they don't necessarily authenticate the user at the application layer.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.8	A user interface should never authenticate a user directly. The system must always be able to authenticate the user by using the centrally available service. The only exception to this rule is if an application running on a mobile device is guarded by a local passcode. This passcode may be used to access the local application. However, access to remote services and resources should be verified by a separate authentication token.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.14	Communications privacy is a slightly different topic than application privacy (described above) or communications information security. While privacy is largely evaluated from the ability for third parties to effectively read or intercept data, confidentiality and integrity do not represent the full scope of communications privacy. Other issues that affect communications privacy include: • Cryptographic uniqueness of each message • Transmission patterns • Plaintext metadata • Hardware addresses or attributable serial numbers	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IEEE	IoT Security Principles and Best Practices	6	Even if device passwords are secure, communications between devices may be hackable. In the IoT there are many protocols, including Bluetooth, Zigbee, Z-Wave, 6LoWPAN, Thread, Wi-Fi, cellular, NFC, Sigfox, Neul, and LoRaWAN. Depending on the protocol and on available computing resources, a device may be more or less able to use strong encryption. Manufacturers should examine their situation on a case-by-case basis and use the strongest encryption possible, preferably IPsec and/or TLS/SSL.	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.4	**COMMUNICATIONS AND CONNECTIVITY PROTECTION.** Communicating Endpoints Protection provides some of the functional security building blocks, such as cryptographic keys, to secure communication between endpoints.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.4	**COMMUNICATIONS AND CONNECTIVITY PROTECTION.** Cryptographic Protection uses cryptographic technologies to protect authenticity of communicating parties and integrity and confidentiality of exchanged data and metadata.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.4	**COMMUNICATIONS AND CONNECTIVITY PROTECTION.** Data-in-Motion Protection provides controls to preserve the integrity, confidentiality and availability of its data.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.7	**DATA PROTECTION.** Data, whether in-motion, in-use, or at-rest, must be protected against unauthorized access and uncontrolled changes by applying functions such as confidentiality controls, integrity controls, access control, isolation and replication. The level of protection should be commensurate with the impact of data loss or falsification, and the retention period should be defined.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.8	**SECURITY MODEL AND POLICY.** The Security Policy includes policies for the system and sub-policies for the endpoint protection, communications and connectivity protection, security monitoring and analysis, security configuration and management and data protection (see individual sections 7.3 to 7.7). The system threat analysis enables the creation of the security objectives for the system, derived from regulations and standards. From these objectives, the applicable security policies are selected based on the industry vertical, customer base, geographic location and other considerations. The security policy describes the overall business-risk considerations and defines the guidelines for securing the day-to-day proper functioning of the system. This policy is then transformed into a security model, and determines and drives requirements to the functionality of the building blocks of the security framework. For example, each machine-level security policy specifically covers the security policies associated with the endpoint and the devices it may be connected to or in control of.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0		**ENDPOINT AUTHENTICATION.** The process of establishing trust through endpoint authentication, or identity assertion of the remote endpoint, has several steps. First, an attestation must be made that the credentials are of the proper level of strength, and that they are in the possession of the appropriate entity. Then, the actual value of data in the credential is evaluated for correctness. Finally, validity of the credential must be tested to ensure that the credential is not suspended, revoked or expired. All successful authentication attempts do not result in the same level of trust in the identity of the remote endpoint. There are different levels of entity identity assurance based on what type of credential is applied to that authentication, how the credential is stored, and what actual authentication technique is implemented. Strong cryptographic credentials are recommended for most endpoints. In addition, credentials should be stored in the strongest storage available, ideally in trusted hardware.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.8	**ENDPOINT DATA PROTECTION.** Securing data in endpoints involves data-at-rest (DAR) and data-in-use (DIU). The protection strategy for data-in-motion (DIM) differs at the edge, the cloud, and in the communications. Cryptography enforces data confidentiality and ensures integrity of the data. It may be used on all the data, only the sensitive portions or the entire storage medium. In practice, multiple data protection techniques may be applied simultaneously, providing protection from different types of attacks.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.11	**CRYPTOGRAPHY TECHNIQUES FOR ENDPOINT PROTECTION.** Endpoints must always use standard cryptographic algorithms. These algorithms should be implemented utilizing safe-coding practices, and whenever possible, with libraries that are updated and maintained regularly. Creating cryptographic algorithms without a public evaluation should be avoided.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	9.1	**CRYPTOGRAPHIC PROTECTION OF COMMUNICATIONS & CONNECTIVITY.** Most IIoT applications should use standardized protocols whose functionality, including security and cryptography, have been evaluated and tested. IIC's 'Industrial Internet Reference Architecture'1 identifies and discusses requirements for IIoT core connectivity protocols.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	9.1.2	**BUILDING BLOCKS FOR PROTECTING EXCHANGED CONTENT.** Where possible, information exchange security among communicating endpoints for sensitive networks and equipment should employ: • explicit endpoint communication policies, • cryptographically strong mutual authentication between endpoints, • authorization mechanisms that enforce access control rules derived from the policy and • cryptographically backed mechanisms to ensure confidentiality, integrity and freshness of exchanged information	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	9.1.3	**CONNECTIVITY STANDARDS AND SECURITY.** A core connectivity technology, as defined in 'Industrial Internet of Things, Volume G5: Connectivity Framework'1, should: • be an open standard with strong independent, international governance, such as IEEE, IETF, OASIS, OMG, or W3C, • be horizontal and neutral in its applicability across industries, • be applicable, stable and proven across multiple industries and • have standard-defined gateways to all other connectivity standards.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Intel	Policy Framework for the Internet of Things (IoT)	Privacy and Security	For trusted data exchange in an IoT ecosystem, data generated by devices and existing infrastructure must be able to be shared between the cloud, the network, and intelligent devices for analysis – enabling users to aggregate, filter, and share data from the edge to the cloud with robust protection.	https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-framework.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
International Electrotechnical Commission (IEC)	IoT 2020: Smart and secure IoT platform	5.2.1	Remote access capabilities as well as secure connectivity need to be implemented end-to-end, with particular implications at the device and edge levels. Hence, reliable, secure and trustworthy connectivity is integral from device to platform, as are authentication and access control.	http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf
International Electrotechnical Commission (IEC)	IoT 2020: Smart and secure IoT platform	5.2.6.1.1	Technologies are required to ensure data integrity and data authenticity as well as data delivery and processing without interferences and manipulations. This mainly requires scalable and efficient technologies beyond heavy-weight public key infrastructures (PKIs) to identify devices and smart objects in future IoT systems.	http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf
International Electrotechnical Commission (IEC)	IoT 2020: Smart and secure IoT platform	5.2.6.1.2	Once communication is introduced, even at a low level (such as in wireless sensor networks), the potential surfaces for privacy breaches increase. Because sensors usually have extremely limited computational and storage capabilities (if any at all), novel methods of securing the contents of a data stream, such as embedded and light-weight encryption, are required.	http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.1.2	Standard or well-established, mature algorithms for cryptographic functions (such as symmetric encryption, public-key encryption, digital signatures, cryptographic hash / message integrity check) MUST be used. Explanation: A tremendous amount of subtlety must be understood in order to construct cryptographic algorithms that are resistant to attack. A very few people in the world have the knowledge required to construct or analyze robust new cryptographic algorithms, and even then, many knowledgeable people have constructed algorithms that were	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			found to be flawed within a short time.	
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.1.3	Standard protocols for authentication, encryption, and other means of assuring security SHOULD be used whenever apparently-robust, applicable protocols exist. Explanation: The amount of expertise required to design robust security protocols is comparable to that required to design robust cryptographic algorithms. However, there are sometimes use cases for which no existing standard protocol may be suitable. In these cases it may be necessary to adapt an existing protocol for a new use case, or even to design a new security protocol.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.3.1	Internet-connected devices SHOULD support the capability to encrypt traffic sent to or from the device. Any information transmitted over a network is potentially sensitive to some customers. For example, even a home temperature monitoring sensor may reveal information about when occupants are away from home, when they wake up and when they go to bed, when and how often they cook meals - all of which are useful to, say, a thief.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.3.2	If a device supports encryption and use of encryption is optional, the device SHOULD be configurable to require encryption, and this SHOULD be the default.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.5	If public key cryptography is used by the device to authenticate itself to other devices or parties, each device MUST be instantiated with its own unique private key or keys. In many cases it will be necessary for the vendor to sign such keys or arrange for them to be signed by a trusted party, prior to shipping the device. Per-device private keys SHOULD be generated on the device and never exposed outside the device.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.1.3	Services such as confidentiality and integrity protection on packet data, message authentication codes or encryption are typically used to provide end-to-end security. These protection methods render the protected parts of the packets immutable as rewriting is either not possible because a) the relevant information is encrypted and inaccessible to the gateway or b) rewriting integrity-protected parts of the packet would invalidate the end-to-end integrity protection.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/
Internet Society (ISOC)	The Internet of Things: An Internet Society Public Policy Briefing	Interoperability and standards	The Internet Society believes that greater interoperability and the use of generic, open, voluntary, and widely available standards as technical building blocks for IoT devices and services (such as the Internet Protocol, or IP) will support greater user benefits, innovation, and economic opportunity.	https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-IoT.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Society (ISOC)	The Internet of Things: An Internet Society Public Policy Briefing	Encourage a collaborative approach to IoT security	The Internet Society believes that IoT security is the collective responsibility of all who develop and use IoT devices. Participants in the IoT space should adopt a collaborative approach to security among its broad, multistakeholder community by assuming responsibility, sharing best practices and lessons learned, encouraging security dialog, and emphasizing the development of flexible, shared security solutions that can adapt and evolve as threats change over time. IoT security policy should focus on empowering players to address security issues close to where they occur, rather than centralizing IoT security among a few, while also preserving the fundamental properties of the Internet and user rights.	https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-IoT.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.15	The software must be architected to identify and ring fence sensitive software components, including cryptographic processes, to aid inspection, review and test. The access from other software components must be controlled and restricted to known and acceptable operations. For example security related processes should be executed at higher privilege levels in the application processor hardware.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.21	Where the device software communicates with a product related webserver or application over TCP/IP or UDP/IP, the device software uses certificate pinning or public/private key equivalent, where appropriate.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.22	The device remains secure and maintains state during a side channel attack.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.1	The product prevents unauthorised connections to it or other devices the product is connected to. For example is there a firewall on each interface and internet layer protocol.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.2	The network component and firewall (if applicable) configuration has been reviewed and documented for the required/defined secure behaviour	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.4	Devices support only the latest versions of application layer protocols with no publically known vulnerabilities and it should not be possible to downgrade a connection to an older, less secure version.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.5	Insecure and unauthenticated application layer protocols (such as TELNET, FTP, HTTP, SMTP and NTP < v4) are not used.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.7	If a connection requires a password or passcode or passkey for connection authentication, the factory issued or reset password is unique to each device and is not derived e.g. from serial numbers.. Examples are WiFi access passwords and Bluetooth PINS.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.8	Where a wireless communications interface requires an initial pairing process, a Strong Authentication shall be used, requiring physical interaction with the device or possession of a shared secret. For example, Bluetooth Numeric Comparison.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.10	For any WiFi connection, WPA2 with AES or a similar strength encryption has been used and insecure protocols such as WPA and TKIP are disabled.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.11	Where WPA2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.12	All network communications keys are stored securely, in accordance with industry standards such as FIPS 140 [5] or similar.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.13	Where the MQTT protocol is used, it is protected by a TLS connection with no known cipher vulnerabilities.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.14	Where the CoAP protocol is used, it is protected by a DTLS connection with no known cipher vulnerabilities.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.15	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A 2] or OWASP. Where insecure ciphers suites are identified they shall be removed from the product.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.17	Where there is a loss of communications it shall not compromise the integrity of the device.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.18	The product only enables the communications interfaces, network protocols, application protocols and network services necessary for the products' operation.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.19	Communications protocols should be at the most secure versions available and/or appropriate for the product. For example, Bluetooth 4.2 rather than 4.0.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.20	Post product launch communications protocols should be maintained to the most secure versions available and/or appropriate for the product.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.1	A true random number generator source is exclusively used for all relevant cryptographic operations including nonce, initialisation vector and key generation algorithms. NIST SP 800-90A [3]	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.2	The true random number generator source has been validated for true randomness using an NIST SP800-22 [4], FIPS 140-2 [5] or similar compliance process.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.3	There is a process for secure provisioning of keys that includes generation, distribution, revocation and destruction. For example in compliance with FIPS140-2 [5] or similar process.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.4	There is a secure method of key insertion that protects keys against copying	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.5	All the product related cryptographic functions have no publicly known unmitigated weaknesses, for example MD5 and SHA-1 are not used, e.g. those stipulated in NIST SP800-131A [2].	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.6	All the product related cryptographic functions are sufficiently secure for the lifecycle of the product, e.g. those stipulated in NIST SP800- 131A [2].].	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.7	The product stores all sensitive unencrypted parameters, (e.g. keys), in a secure, tamper-resistant location.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.9.9	In device manufacture all asymmetric encryption private keys that are unique to each device are secured in accordance with FIPS 140 [5] and truly randomly internally generated or securely programmed into each device.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.11.4	Where the application communicates with a product related remote server(s) or device it does so over a secure connection such as a TLS connection using certificate pinning.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.2	The product/service ensures that all Personal Information is encrypted at rest and in transit.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.4	All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities; are within their validity period; and processes are in place for their renewal.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.5	The Product Manufacturer or Service Provider has a process to monitor the relevant security advisories to ensure all the product related web servers use protocols with no publicly known weaknesses.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.6	The product related web servers support appropriately secure TLS/DTLS ciphers and disable / remove support for deprecated ciphers. For example those published at ENISA [27] SSL Labs [29], IETF RFC7525 [28]:	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.7	The product related web servers have repeated renegotiation of TLS connections disabled.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.9	Where a product related to a webserver encrypts communications using TLS and requests a client certificate, the server(s) only establishes a connection if the client certificate and its chain of trust are valid.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.10	Where a product related to a webserver encrypts communications using TLS, certificate pinning is implemented. For example using OWASP, https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning or similar organisations' certificate and public key pinning guidance.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	Security Design Best Practices		Implement end-to-end security and privacy of system data and operations; from fielded devices, to the server, to the end-user on a management web portal.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Restrict system and network communications to only known, authorized system components where able.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Utilize two-factor authenticated and encrypted remote management services.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Do not build your own encryption functions – and have encryption implementations security-reviewed.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Whitelist and control both ingress and egress of device/system communications where able.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Use whitelisting methods over blacklisting when feasible.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Implement application data layer encryption in addition to communications link layer encryption for higher risk data communications.	https://www.iotsi.org/security-best-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Initiative	Security Design Best Practices		Utilize mutually authenticated and encrypted RF communications.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Ensure the identity, authenticity, and integrity of communicated data by authenticating both the communication link and the data communicated.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		When in question over possible data sensitivity or privacy, just encrypt.	https://www.iotsi.org/security-best-practices
MIT Laboratory for Computer Science	Dos and Don'ts of Client Authentication on the Web	3.1 Use cryptography appropriately	Use of cryptography is critical to providing authentication. Without the use of cryptography, it is not possible to protect a system from the weakest of adversaries.	http://pdos.csail.mit.edu/papers/webauth:sec10.pdf
MIT Laboratory for Computer Science	Dos and Don'ts of Client Authentication on the Web	3.3 Handle authenticators carefully	Authenticators are the workhorse of any authentication scheme. These are the tokens presented by the client to gain access to the system. As discussed above, authenticators protect passwords by being a short-term secret; the authenticator can be changed at any time whereas passwords are much less convenient to change.	http://pdos.csail.mit.edu/papers/webauth:sec10.pdf
Object Management Group (OMG) Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	Data Protection	Data in the device, in flight throughout the public network, provider cloud, and enterprise network, as well as at rest in a variety of locations and formats must be protected from inappropriate access and use. Multiple methods can be utilized, and indeed, in many cases, multiple methods are applied simultaneously to provide different levels of protection of data against different types of threats or isolation from different entities supporting the system.	https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	6.3	As many M2M Applications generate and exchange sensitive data, and essential M2M Services deal with the routing and exploitation of such information, the M2M System needs to be able to support security services such as ensuring availability, mutual authentication between communicating parties, confidentiality (e.g. protection against eavesdropping by unauthorized parties), integrity (i.e. protection against manipulation) and access control.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.7	A security association is established between the communicating entities, which provides mutual authentication, integrity and confidentiality.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.8	The security association between communicating entities uses protocols which are proven to resist man-in-the-middle attacks.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.9	Communications whose security is anchored in M2M Service Layer keys use session keys, i.e. keys with a limited lifetime which can be set by security policy. Session keys can be derived from M2M Service-layer keys.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.10	The protocol includes functionality to detect if all or part of a message is an unauthorized repeat of an earlier message or part of a message	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.19	Establish Secure Communications Link/security association between relevant entities/nodes using modern cryptographic algorithms	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.24	Ensure appropriate strong standard algorithms and strong keys are used, and key management is in place.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	2	Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This includes but is not limited to wired, Wi-Fi, and Bluetooth connections	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	3	All IoT support websites must fully encrypt the user session from the device to the backend services. Current best practices include HTTPS and HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications. 1	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	34	End-user communications, including but not limited to email and SMS, must adopt authentication protocols to help prevent spearphishing and spoofing. Domains should implement SPF, DKIM and DMARC for all security and privacy-related communications and notices as well as for parked domains and those that never send email.5	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	36	IoT vendors using email communication should adopt transport-level confidentiality, including generally accepted security techniques to aid in securing communications and enhancing the privacy and integrity of the message (also referred to as “Opportunistic TLS for email”). 7	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.5	An important aspect of security of the entire ecosystem is the robustness of publicly vetted and peer-reviewed (e.g. NIST-approved) cryptographic algorithms. Security is not achieved by obscurity of the cryptographic algorithm. To ensure both interoperability and security, not only widely accepted cryptographic algorithms must be used, but also a list of approved cryptographic functions must be specified explicitly. As new algorithms are NIST approved or old algorithms are deprecated, the list of approved algorithms must be maintained by OIC. All other algorithms (even if they deemed stronger by some parties) must be considered non-approved.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.1.3, 1)	FIPS Random Number Generator (“RNG”) – Insufficient randomness or entropy in the RNG used for authentication challenges can substantially degrade security strength. For this reason, it is recommended that a FIPS 800-90A-compliant RNG with a certified noise source be used for all authentication challenges.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf
Open Web Application Security Project (OWASP)	OWASP Secure Coding Practices Quick Reference Guide	Cryptographic Practices	All cryptographic functions used to protect secrets from the application user must be implemented on a trusted system (e.g., The server) Protect master secrets from unauthorized access Cryptographic modules should fail securely All random numbers, random file names, random GUIDs, and random strings should be generated using the cryptographic module’s approved random number generator when these random values are intended to be un-guessable Cryptographic modules used by the application should be compliant to FIPS 140-2 or an equivalent standard. (See http://csrc.nist.gov/groups/STM/cmvp/validation.html) Establish and utilize a policy and process for how cryptographic keys will be managed	https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Web Application Security Project (OWASP)	IoT Security Guidance	I1: Insecure Web Interface	Ensure that any web interface has the ability to use HTTPS to protect transmitted information	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I4: Lack of Transport Encryption	Ensure all communication between system components is encrypted as well as encrypting traffic between the system or device and the internet	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I4: Lack of Transport Encryption	Use recommended and accepted encryption practices and avoid proprietary protocols	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I4: Lack of Transport Encryption	Ensure SSL/TLS implementations are up to date and properly configured	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I4: Lack of Transport Encryption	Consider making a firewall option available for the product	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I6: Insecure Cloud Interface	Ensure that all cloud interfaces use transport encryption	https://www.owasp.org/index.php/IoT_Security_Guidance

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Web Application Security Project (OWASP)	IoT Security Guidance	I7: Insecure Mobile Interface	Ensure that any mobile application uses transport encryption	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I8: Insufficient Security Configurability	Ensure encryption options are made available (e.g. Enabling AES-256 where AES-128 is the default setting)	https://www.owasp.org/index.php/IoT_Security_Guidance
Symantec	An Internet of Things Security Reference Architecture		Security rests on fundamentals. Encryption, authentication, and "key management" are invariably the foundation of meaningfully resilient security. Fortunately, some great open source libraries perform encryption really well, even in resource constrained IoT devices. Unfortunately, most companies still take dangerous risks attempting to do the key management for IoT entirely on their own. In contrast, roughly $4 billion per day of e-commerce transactions are protected by a simple but strong trust model serving billions of users, and serving over a million companies worldwide. This "trust model" helps their systems safely authenticate systems of other companies and safely start encrypted communications with those systems.	https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F1.17	**Secure Distributed Composition.** The principle of secure distributed composition states that the composition of distributed components that enforce the same security policy should result in a system that enforces that policy at least as well as the individual components do. Many of the design principles for secure systems deal with how components can or should interact.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.1.18	**Trusted Communication Channels.** The principle of trusted communication channels states that when composing a system where there is a potential threat to communications between components (i.e., the interconnections between components), each communication channel must be trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions).	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
US Senate	S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill)	SEC.3 (a) (1) (A) (i) (III)	IN GENERAL.—A clause that requires the contractor providing the Internet-connected device to provide written certification that the device—(III) uses only non-deprecated industry-standard protocols and technologies for functions such as— (aa) communications, such as standard ports for network traffic; (bb) encryption; and (cc) interconnection with other devices or peripherals; and	https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt
W3C	Web of Things (WoT) Security and Privacy Considerations	4.1.2	**Use Secure Transports.** When defining protocols for APIs exposed by a TD, it is often important to use secure protocols guaranteeing data authenticity and confidentiality.	https://www.w3.org/TR/wot-security/#recommended-security-practices

Code of Practice: 6 - Minimise exposed attack surfaces

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Basic Requirements on IoT HARDWARE AND COMPONENTS	IoT devices should only be able to perform documented functions, making sense for device/service.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
AT&T	The CEO's Guide to Securing the Internet of Things		No ancillary services. A device should not offer any services to the network that it does not require to support its core functions	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
AT&T	The CEO's Guide to Securing the Internet of Things		No backdoors. A device should not have hidden or known entry points that can be easily exploited by the device vendor or others.	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Atlantic Council Scowcroft Center for Strategy and Security	Smart Homes and the Internet of Things (issue brief)		A published commitment to integrating security throughout the development, manufacturing, and deployment life cycle. Key elements, such as adversarial threat modeling,32 resilience testing, and reduced elective complexity, lower costs and shorten the timeline of securing IoT devices.	http://www.atlanticcouncil.org/images/publications/Smart_Homes_0317_web.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.2	Close Unnecessary Ports and Disable Unnecessary Services. BITAG recommends that device manufacturers close unnecessary ports, such as telnet, as unnecessary ports may be unsecured or can otherwise become compromised [107]. Devices should close or disable administrative interfaces and functions that are not being used. Devices should also not ship with drivers that the device is not using.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.3	IoT Devices Should Be Restrictive Rather Than Permissive in Communicating. BITAG recommends that IoT devices communicate only with trusted endpoints. When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not necessarily traverse the firewall. Note that a BITAG recommendation to restrict the configuration of IoT device communications should not come at the cost of an open ecosystem. A user should be able to configure communications between arbitrary IoT devices, and devices that trust one another should be allowed to communicate. Secure communications can bootstrap restricted trust lists that reflect the set of devices with which any given device expects to communicate. These inter-device communications should only be permitted through trusted mechanisms and secure communication channels.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
City of New York (NYC) Guidelines for the Internet of Things	Security	4.1	IoT systems should be designed with an explicit focus on minimizing security risks (e.g. unauthorized operation or hacking, system faults, tampering, and environmental risks), limiting the potential impact from a security breach (e.g. the release of personally identifiable information), and ensuring that any compromises can be quickly detected and managed.	https://iot.cityofnewyork.us/security/
City of New York (NYC) Guidelines for the Internet of Things	Security	4.4	All data should be protected in transit and at rest, and systems should be secured against unauthorized access or operation. Data storage mechanisms must not be easily removed from devices and systems must not have vulnerable external interfaces (e.g. unsecured USB ports).	https://iot.cityofnewyork.us/security/
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	The low price point increases the potential adversary pool - 1	Consider physical safeguards such as tamper detection to guard against physical access to sensitive internals	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	The low price point increases the potential adversary pool - 2	Lock-down physical ports (including test ports) on the product using passwords	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf
Cloud Security Alliance (CSA)	Future-proofing the connected world: 13 steps to Developing Secure IoT	Medical Devices and Medical Standard Protocols are Vulnerable to Attack - 2	Authenticate access to all ports	https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-02	Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-08	Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-27	Limit permissions of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users). Implement fine-grained authorisation mechanisms - such as Attribute-Based Access Control (ABAC) or Role-Based Access Control (RBAC)- for executing privileged actions, access to files and directories, applications, etc. Use the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-28	Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them, and device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code. in order to minimise the potential for compromised code to access those code and/or data.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-32	Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed. There should be mechanisms to control device security settings, such as remotely locking or erasing contents of a device if the device has been stolen.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-33	Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-50	Ensure only necessary ports are exposed and available.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-47	Risk Segmentation - Splitting network elements into separate components to help isolate security breaches and minimise overall risk. Networks can be divided into isolated subnetworks to boost performance and improve security.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-45	Disable specific ports and/or network connections for selective connectivity. If necessary, provide users with guidelines to perform this process in the final implementation.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-44	Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-31	Since some devices, gateways, etc. are required to be managed remotely rather than operated manually in the field, measures for tamper protection and detection are needed. Detection and reaction to hardware tampering should not rely on network connectivity. Hardware tampering means that an attacker has physical control of the device for some period of time. Broadly speaking, hardware tampering might occur at any of the different periods in the life cycle of a device.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	7.2.3	Protection of remote monitoring interfaces is crucial since they often provide a highly-privileged entry point into a device. This protection includes access control and authentication mechanisms, as described in good practices on Identification, authentication, authorisation.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines for Network Operators	CLP.14_5.1.1.2	Non-Removable UICC. The Network Operator should provide non-removable UICCs (i.e. Machine Form Factor) for IoT Services where the service threat model suggests that the IoT Endpoint device may be vulnerable to physical tampering.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.14-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_5.6	Each system must be accessible by administration to troubleshoot and diagnose application faults. This can be challenging in environments where services or servers are short-lived, if an administrative model is not sufficiently designed.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_7.3	Use a Private APN for Cellular Connectivity. By restricting access to the APN, an organization can ensure that only authenticated endpoints are allowed to connect to the service infrastructure made available through the APN. This diminishes the potential for rogue or random wireless clients to connect to the APN and access restricted services.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.3	The physical device should not only be tamper resistant at the chip level, it should also be tamper resistant at the product level. The case used in the product should provide protection from adversarial or curious users.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.9	Applications running on an Endpoint typically do not require super-user privileges. Most often, applications require access to device drivers or a network port. While some of these devices, ports, or other objects may require super-user privileges to initially access them, the super-user privileges are not required to perform subsequent operations. Thus, it is best practice to only use super-user privileges at the start of the application to gain access to these resources. Then, super-user privileges should be dropped. Dropping super-user privileges is a common process that is well documented, and has been implemented exceptionally well in applications such as the Secure Shell (SSH), apache2, and other well engineered servers.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.10	Applications running on an Endpoint should have different user identities associated with each unique process. This ensures that if one application is compromised, a separate application on the same Endpoint cannot be compromised without a successful second attack. This extra step required on behalf of an Attacker is often a critical hindrance to the overall exploit development process and increases the cost and complexity of an attack against an Endpoint.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.11	Programming languages have varying degrees of security, depending on the purpose of the language and how high level it is. Some languages provide constructs for limiting access to raw memory, and enforce constraints around how memory is used. The engineering team should identify a language that is capable of providing security to the application run-time or resultant binary. The compiler or run-time should be security hardened, where possible, to restrict the potential for a vulnerability to be abused by an adversary. In a well defined run-time environment, even an easy-to-trigger programming flaw can be extremely difficult to fully exploit. This presumes that security enhancements are used to protect the way the application executes, accesses memory, and is supported by the operating system's security enhancements.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_8.1	Applications running on an Operating System should be designed to use (either transparently, or intentionally) the security enhancements of the underlying Operating System and Kernel. This includes technologies such as:Applications running on an Operating System should be designed to use (either transparently, or intentionally) the security enhancements of the underlying Operating System and Kernel. This includes technologies such as: ASLR" User-Pointer Dereference Protection (UDEREF) Structure Leakage (information disclosure) Protection Each operating system used in an embedded system will provide different variations and combinations of these technologies, sometimes under different names. Determine what the operating system and kernel are capable of providing, and enable these technologies, where possible, to enhance the security of applications."	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_8.2	When a product is being developed it is often enabled with debugging and testing technologies to facilitate the engineering process. This is entirely normal. However, when a device is ready for production deployment, these technologies should be stripped from the production environment prior to the definition of the Approved Configuration.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_9.3	Components on the physical circuit typically do not use any semblance of confidentiality and integrity when communicating with each other or the central processing unit. As a result, any adversary can read or write data transmitted on these buses. The effect of this gap in communications security is the ability for an adversary to impersonate legitimate devices on the physical circuit. If the adversary chooses, they can impersonate a critical component such as NVRAM, RAM, or even a trust anchor.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.12	While the Organizational Root of Trust and its services will define authentication technologies that secure the network communication layer, the user, administration, and partner authorization technologies must be configured separately. While these entities' communications channels are secured with the Organizational Root of Trust, their actions and identities must be authenticated using a separate system.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.13	In some service infrastructure environments, ingress and egress protection mechanisms are not configured by default. This means that engineers must employ firewall or network traffic rulesets themselves. These rules must be set in infrastructure before any service is deployed to the public. Note that software firewalls carry an additional risk, in that they can be manipulated by a savvy attacker. If a software firewall is used, any server infrastructure that is improperly hardened may be manipulated by an attacker. In other words, if a public service running on a server carries unnecessary privileges (such as super-user privileges) and is compromised, the attacker will likely be capable of disabling the software firewall. Thus, the engineering team must evaluate whether a software firewall is too high of a risk for the chosen architecture.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.5	Accepting dynamically generated data, such as advertisements, from a Partner requires a certain level of presumption regarding the quality and security of the data. Instead of making presumptions and applying the data to the presentation layer, the engineering team must take steps to ensure that the data distributed from the service application to or from a partner is well formed and does not contain potentially malicious content.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_8.1	Some implementations of modern RAM technology such as Dynamic Random Access Memory (DRAM) and Static Random Access Memory (SRAM) are vulnerable to errors that can be provably induced by certain memory access sequences. Abusing this type of error can result in the alteration of a specific bit, or bits, in predictable areas of memory. A successful exploit of this condition can alter bits in memory that represent types of privilege denoted by software. In other words, if exploited correctly, an adversary can elevate their privileges from one user to another user by manipulating a hardware flaw in modern implementations of DRAM or SRAM. Many modern implementations of DRAM and SRAM have been found provably exploitable through this vulnerability. However, it requires the ability to execute code on the local system in order to create the memory access sequences capable of triggering this bug.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_8.2	Modern service infrastructure often utilizes virtual machines to deploy services on demand. While this model has proved extremely convenient and easy to deploy with, the problem with this methodology is the security of the overall infrastructure. While the engineering team may succeed in deploying a well thought-out architecture, the organization that manages and deploys the virtual infrastructure may not be as successful. One major concern of deploying in virtual server environments is the ability for hosts to be compromised, or for servers (virtual guests) to intercept the data of other guests running on the same infrastructure.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IEEE	IoT Security Principles and Best Practices	1	Some IoT devices may operate continuously unattended and not subject to the security implied by this frequent, direct human observation. While it is best to keep devices relatively isolated so that only a few designated persons have physical access, especially for completely unattended devices, making them tamper-proof or tamper-evident may be advantageous. This form of endpoint hardening can help block potential intruders from reaching data. It may also defend against a hacker buying and then weaponizing devices.	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
IEEE	IoT Security Principles and Best Practices	7	Recently DDoS attacks have been conducted in large measure by armies of poorly protected IoT devices that have become zombie systems in massive global campaigns. Most IoT devices are made of commodity components that have vastly overpowered network capabilities for the function they are supposed to perform causing congestion on home networks and potentially contributing to huge costs for the targets of IoT-borne DDoS attacks.	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.3	ENDPOINT PROTECTION. Endpoint Physical Security provides physical protection of the endpoint with anti-tampering and theft prevention mechanisms to prevent uncontrolled changes or removal of the endpoint.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.3	ENDPOINT PROTECTION. Endpoint Root of Trust provides a foundation to secure other functions at the endpoint, from the hardware to applications including firmware, virtualization layer, operating system, execution environment and application. It also provides confidence on the endpoint identity.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things	7.9	FROM FUNCTIONAL TO IMPLEMENTATION VIEWPOINT. Principle of economy of mechanism: keep the design as simple and small as possible.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
	Volume G4: Security Framework v1.0			
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.9	FROM FUNCTIONAL TO IMPLEMENTATION VIEWPOINT. Principle of complete mediation: every access to every object must be checked for authority.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.9	FROM FUNCTIONAL TO IMPLEMENTATION VIEWPOINT. Principle of open design: a design should not be secret. The mechanisms should not depend on the ignorance of potential attackers, but rather on the possession of specific, more easily protected, keys or passwords.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.9	FROM FUNCTIONAL TO IMPLEMENTATION VIEWPOINT. Principle of least privilege: every program and every user of the system should operate using the least set of privileges necessary to complete the job.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.9	FROM FUNCTIONAL TO IMPLEMENTATION VIEWPOINT. Principle of least common mechanism: minimize the amount of mechanism common to more than one user and depended on by all users.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS. Changes in hardware components and configuration, ①: Hardware integrity must be assured throughout the endpoint lifecycle to deter uncontrolled changes to the hardware components. A potential vulnerability of the hardware is the usurpation of some part of the hardware resources. The endpoint must be able to protect itself against unauthorized access and the monopolizing of key resources such as memory, processing cycles and privileged processing modes.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	9.2.5	NETWORK FIREWALLS. Network firewalls are message-oriented filtering gateways used extensively to segment IIoT systems. Most firewalls are Layer 2, 3 or 4 IP routers/message forwarders with sophisticated message filters. Firewalls may be deployed as either physical or virtual network devices. A firewall's filtering function examines every message received by the firewall. If the filter determines that the message agrees with the firewall's configured traffic policy, the message is passed to the firewall's router component to be forwarded.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.12.2	CONTAINER ISOLATION. The container isolation model implements either hardware-or software-enforced boundaries Software containers rely on the OS to enforce the resource isolation boundaries; hardware containers use a physically different compute element on the same platform. Hybrid containers combine both approaches.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.6.1	Device firmware SHOULD be designed to use hardware and operating systems that implement memory compartmentalization techniques, in order to prevent read, write, and/or execute access to areas of memory by processes not authorized to use those areas for those purposes. Vendors that do not make use of such features MUST document their design rationale. Explanation: Such mechanisms, when properly used, reduce the impact of a firmware bug, such as a buffer overflow vulnerability. Operating systems, or even firmware running on "bare metal", that do not provide such a separation allow an attacker to gain access to the complete address space. While these concepts have been available in hardware for a long time already, they often are not utilized by real-time operating systems.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.6.2	Device firmware SHOULD be designed to isolate privileged code and data from portions of the firmware that do not need to access them, in order to minimize the potential for compromised code to access those code and/or data.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.4.5	Any debug interface (for example, I/O ports such as JTAG) only communicate with authorised and authenticated entities on the production devices.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.4.9	All communications port(s), such as USB, RS232 etc., which are not used as part of the product's normal operation are not physically accessible or only communicate with authorised and authenticated entities.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.4.10	After manufacture, all the product's test points are securely disabled or removed wherever possible.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.1	The product has measures to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or sandbox.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.5	If the product has any port(s) that are not required for normal operation, they are only allowed to communicate with authorised and authenticated entities or securely disabled when shipped. Where a port is used for field diagnostics, the port input is deactivated and the output provides no information which could compromise the device	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.10	Production software images should be assessed on release to remove all unnecessary debug and symbolic information “Know what is being released, and have checks in place to prevent accidental release of superfluous data	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.11	Development software versions have any debug functionality switched off if the software is operated on the product outside of the product vendors’ trusted environment.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.15	The software must be architected to identify and ring fence sensitive software components, including cryptographic processes, to aid inspection, review and test. The access from other software components must be controlled and restricted to known and acceptable operations. For example security related processes should be executed at higher privilege levels in the application processor hardware.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.19	The production software signing keys are under access control.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.3	All interactive OS accounts or logins have been disabled or eliminated from the software at the end of the software development process.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.4	Files and directories are set to appropriate access privileges on a need to access basis.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.5	Passwords file(s) are owned by and are only accessible to and writable by the Devices' OS's most privileged account.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.6	All OS non-essential services have been removed from the products' software image or filesystems.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.7	All OS command line access to the most privileged accounts has been removed from the operating system.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.8	The product's OS kernel and its functions are prevented from being called by external product level interfaces and unauthorised applications.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.9	Applications are operated at the lowest privilege level possible.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.6.11	The OS is separated from the application(s) and is only accessible via defined secure interfaces.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.1	The product prevents unauthorised connections to it or other devices the product is connected to. For example is there a firewall on each interface and internet layer protocol.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.2	The network component and firewall (if applicable) configuration has been reviewed and documented for the required/defined secure behaviour	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.3	Products with one or more network interfaces, the uncontrolled, and any unintended packet forwarding function should be blocked.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.6	All the products unused ports are closed and the minimal required number of ports are active.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.18	The product only enables the communications interfaces, network protocols, application protocols and network services necessary for the products' operation.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.7.19	Communications protocols should be at the most secure versions available and/or appropriate for the product. For example, Bluetooth 4.2 rather than 4.0.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.9	The product supports access control measures to the root account to restrict access to sensitive information or system processes.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.11	The product only allows controlled user account access; access using anonymous or guest user accounts are not supported without justification.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.2	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.3	All product related web servers have their webserver HTTP trace and trace methods disabled.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.6	The product related web servers support appropriately secure TLS/DTLS ciphers and disable / remove support for deprecated ciphers. For example those published at ENISA [27] SSL Labs [29], IETF RFC7525 [28]:	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.7	The product related web servers have repeated renegotiation of TLS connections disabled.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.8	The related servers have unused IP ports disabled.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.17	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.18	All the related and network elements servers prevent anonymous/guest access except for read only access to public information.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.14.1	The product has all of the production test and calibration software used during manufacture erased or removed or secured before the product is dispatched from the factory. This is to prevent alteration of the product post manufacture when using authorised production software, for example hacking of the RF characteristics for greater RF ERP. Where such functionality is required in a service centre, it shall be erased or removed upon completion of any servicing activities.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	Security Design Best Practices		Expect software vulnerabilities & validate secure coding using automated & manuals means.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Implement and operate only the system services that are necessary for the function of the system/solution.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Deploy systems and services based on a least-privilege model.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Compartmentalize communication IO in system design wherever possible; and run these services at least-privilege levels.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Run as much system code as possible at the lowest privilege/permission level possible; and as little as you can in highest privilege/permission level.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Consider restricting or tightly controlling access to system components, firmware, and technical data for critical systems.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Validate system security approach and implementation throughout the SDLC.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Conduct security/vulnerability testing on both software code and finished systems.	https://www.iotsi.org/security-best-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Initiative	Security Design Best Practices		Protect the system enclosure and electronics from physical access, probing, and attack.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Shed technology attack surface whenever and wherever possible in design and development.	https://www.iotsi.org/security-best-practices
Microsoft	IoT Security Best Practices	Scope hardware to minimum requirements	The hardware design should include the minimum features required for operation of the hardware, and nothing more. An example is to include USB ports only if necessary for the operation of the device. These additional features open the device for unwanted attack vectors that should be avoided.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Microsoft	IoT Security Best Practices	Make hardware tamper proof	Build in mechanisms to detect physical tampering, such as opening of the device cover or removing a part of the device. These tamper signals may be part of the data stream uploaded to the cloud, which could alert operators of these events.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Microsoft	IoT Security Best Practices	Deploy hardware securely	IoT deployments may require hardware to be deployed in unsecure locations, such as in public spaces or unsupervised locales. In such situations, ensure that hardware deployment is tamper-proof to the maximum extent. If USB or other ports are available on the hardware, ensure that they are covered securely. Many attack vectors can use these as entry points.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Microsoft	IoT Security Best Practices	Physically protect the IoT infrastructure	The worst security attacks against IoT infrastructure are launched using physical access to devices. One important safety practice is to protect against malicious use of USB ports and other physical access. One key to uncovering breaches that might have occurred is logging of physical access, such as USB port use. Again, Windows 10 (IoT and other SKUs) enables detailed logging of these events.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Object Management Group (OMG) Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	System, Application, and Solution Lifecycle Management	Lifecycle management of the IoT system is complex, multi-faceted, and has relationships with identity management, device management, the supply chain, application and software development, through to system operations and change management of deployed and in-service systems. Attention to security in all of these areas is required in order to prevent a variety of attacks ranging from malicious code insertion to inappropriate firmware/software deployment, to effective cryptographic key management.	https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.5	Processes should be implemented to protect the storage. Therefore it is recommended that least-privileges are implemented so that service privileges are minimized as much as possible to reduce risk.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	9	Ensure all IoT devices and associated software have been subjected to rigorous, standardized software development lifecycle testing including unit, system, acceptance, and regression testing and threat modeling, along with maintaining an inventory of the source for any third-party/open source code and/or components. Employ generally accepted code and system hardening techniques across a range of typical use case scenarios, including prevention of any data leaks between the device, apps and cloud services. Developing secure software requires thinking about security from a project's inception through implementation, testing, and deployment. Devices should ship with current software and/or on first boot push automatic updates to address any known critical vulnerabilities.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	11	Design devices to minimum requirements necessary for operation. For example, USB ports or memory card slots should only be included if they are required for the operation and maintenance of the device. Unused ports and services should be disabled.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	37	Implement measures to help prevent or make evident any physical tampering of devices. Such measures help to protect the device from being opened or modified for malicious purposes after installation or from being returned to a retailer in a compromised state.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.3	Paths/ ports used for data entry into or export out of trusted/ crypto-boundary needs to be protected. This includes paths into and out secure execution engine and secure memory. Path protection can be both hardware based (e.g. use of a privileged bus) or software based (using encryption over an untrusted bus).	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf

Open Web Application Security Project (OWASP)	OWASP Secure Coding Practices Quick Reference Guide	Error Handling and Logging	Do not disclose sensitive information in error responses, including system details, session identifiers or account information Use error handlers that do not display debugging or stack trace information Implement generic error messages and use custom error pages The application should handle application errors and not rely on the server configuration Properly free allocated memory when error conditions occur Error handling logic associated with security controls should deny access by default All logging controls should be implemented on a trusted system (e.g., The server) Logging controls should support both success and failure of specified security events Ensure logs contain important log event data Ensure log entries that include un-trusted data will not execute as code in the intended log viewing interface or software Restrict access to logs to only authorized individuals Utilize a master routine for all logging operations Do not store sensitive information in logs, including unnecessary system details, session identifiers or passwords Ensure that a mechanism exists to conduct log analysis Log all input validation failures Log all authentication attempts, especially failures Log all access control failures Log all apparent tampering events, including unexpected changes to state data Log attempts to connect with invalid or expired session tokens Log all system exceptions Log all administrative functions, including changes to the security configuration settings Log all backend TLS connection failures Log cryptographic module failures Use a cryptographic hash function to validate log entry integrity	https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Web Application Security Project (OWASP)	IoT Security Guidance	I3: Insecure Network Services	Ensure all devices operate with a minimal number of network ports active	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I3: Insecure Network Services	Ensure all devices do not make network ports and/or services available to the internet via UPnP for example	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I10: Poor Physical Security	Ensure the device is produced with a minimal number of physical external ports (e.g. USB ports)	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I10: Poor Physical Security	Ensure the firmware of Operating System can not be accessed via unintended methods such as through an unnecessary USB port	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I10: Poor Physical Security	Ensure the product is tamper resistant	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I10: Poor Physical Security	Ensure the product has the ability to limit administrative capabilities in some fashion, possibly by only connecting locally for admin functions	https://www.owasp.org/index.php/IoT_Security_Guidance

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Web Application Security Project (OWASP)	IoT Security Guidance	I10: Poor Physical Security	Ensure the product has the ability to disable external ports such as USB	https://www.owasp.org/index.php/IoT_Security_Guidance
Symantec	An Internet of Things Security Reference Architecture		System hardening, whitelisting, and application sandboxing can provide network protection, closing back doors, limiting network connectivity by application, and restricting both inbound and outbound traffic flow. This can also provide protection against different exploits, restricting app behavior, protecting the system from buffer overflows and zero day attacks, while preserving control of the device. Such solutions can also be used to prevent unauthorized use of removable media as well as locking down device configuration and settings, while also de-escalating user privileges where needed. Such solutions can also provide auditing and alerting functions, helping monitor logs and security events. Policy based technologies can even be run in environments without the connectivity or processing power required to run traditional signature-based technologies.	https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable selective connectivity. Depending on the purpose of the IoT device, providing the consumers with guidance and control over the end implementation can be a sound practice.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Use hardware that incorporates security features to strengthen the protection and integrity of the device. For example, use computer chips that integrate security at the transistor level, embedded in the processor, and provide encryption and anonymity.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Build the device using the most recent operating system that is technically viable and economically feasible. Many IoT devices use Linux operating systems, but may not use the most up-to-date operating system. Using the current operating system ensures that known vulnerabilities will have been mitigated.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Start with basic software security and cybersecurity practices and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.1.7	Reduced Complexity. The principle of reduced complexity states that the system design should be as simple and small as possible. A small and simple design will be more understandable, more analyzable, and less prone to error. This principle applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses to be successful, a small and simple design is essential. Application of the principle of reduced complexity contributes to the ability of system developers to understand the correctness and completeness of system security functions. It also facilitates identification of potential vulnerabilities	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.1.12	Hierarchical Protection. The principle of hierarchical protection states that a component need not be protected from more trustworthy components. In the degenerate case of the most trusted component, it must protect itself from all other components. For example, if an operating system kernel is deemed the most trustworthy component in a system, then it must protect itself from all untrusted applications it supports, but the applications, conversely, do not need to protect themselves from the kernel.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.1.13	Minimized Security Elements. The principle of minimized security elements states that the system should not have extraneous trusted components. This principle has two aspects: the overall cost of security analysis and the complexity of security analysis. Trusted components, necessarily being trustworthy, are generally costlier to construct, owing to increased rigor of development processes. They also require greater security analysis to qualify their trustworthiness.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.1.14	Least Privilege. The principle of least privilege states that each component should be allocated sufficient privileges to accomplish its specified functions, but no more. This limits the scope of the component's actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact; and the security analysis of the component will be simplified.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.2.5	Secure Defaults. The principle of secure defaults states that the default configuration of a system (to include its constituent subsystems, components, and mechanisms) reflects a restrictive and conservative enforcement of security policy. The principle of secure defaults applies to the initial (i.e., default) configuration of a system as well as to the security engineering and design of access control and other security functions that should follow a "deny unless explicitly authorized" strategy.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.1.6	Minimized Sharing. The principle of minimized sharing states that no computer resource should be shared between system components (e.g., subjects, processes, functions) unless it is absolutely necessary to do so. Minimized sharing helps to simplify design and implementation. In order to protect user-domain resources from arbitrary active entities, no resource should be shared unless that sharing has been explicitly requested and granted.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Web of Things (WoT) Security and Privacy Considerations	Minimize Network Interface Functionality	4.1.5	Network interfaces exposed by a TD (WoT Interfaces) should only provide the minimal necessary functionality, which helps to minimize implementation errors, possibilities for exposing potentially sensitive data, DoS attack possibilities etc. Devices should be strongly encapsulated, meaning the network interfaces should not expose implementation details (for example, the use of particular software frameworks). Consider different levels of access for different users.	https://www.w3.org/TR/wot-security/#recommended-security-practices

Code of Practice: 7 - Ensure software integrity

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Basic Requirements on APPLICATIONS	Third-party libraries Rules for maintaining, updates, checking for vulnerabilities.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.10	**Secure software supply chain.** Manufacturers should protect the secure software supply chain to prevent introduction of malware during the manufacturing process; vendors and manufacturers should take appropriate measures to secure their software supply chain.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
CableLabs	A Vision for Secure IoT	Increasing Security through an Industry-Led Standards-based Approach	To further ensure device integrity, each device should be "hardened" to minimize the attack surface by closing unnecessary ports, disabling unnecessary services, and using a secure bootloader with configuration validation	https://www.cablelabs.com/insights/vision-secure-iot/
CableLabs	A Vision for Secure IoT	Integrity	The data created or received by a device must be trustworthy, and protected from unauthorized modification. This requires that the device identity, execution environment, configuration, and communications are secured using well-established methods.	https://www.cablelabs.com/insights/vision-secure-iot/
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-02	Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-03	The boot process initialises the main hardware components, and starts the operating system. Trust must be established in the boot environment before any trust in any other software or executable program can be claimed, so the booted environment must be verified and determined to be in an uncompromised state.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-06	Restore Secure State - Enable a system to return to a state that was known to be secure, after a security breach has occured or if an upgrade has not been successful.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-16	Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-04	Sign code cryptographically to ensure it has not been Management tampered with after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded. Only run signed code and never unsigned code. Measuring the bootprocess enables the detection of manipulation of the host OS and software, so that malicious changes in the behaviour of the devices can be detected. It enables boot-time detection of rootkits, viruses and worms.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-01	Employ a hardware-based immutable root of trust. The Hardware Root of Trust is a trusted hardware component which receives control at power-on. It then extends the chain of trust to other hardware, firmware, and software components. The Root of Trust should then be attestable by software agents running within and throughout the infrastructure.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	5.2, sixth bullet point	Self-protection: HW and SW self-protection measures should be in place to protect previous security functions. Data used to enforce these security functions should be protected, and hardening should be used to reduce the attack surface	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.1	Implement a Trusted Computing Base	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.16	Critical applications stored in executable regions of memory, such as first-stage bootloaders or Trusted Computing Bases, should be stored read-only. This ensures that the device can be booted into a valid configuration without interjection from an adversary. Without this assurance, executable code loaded after the first stage of execution will not be able to trust that it was booted into a valid configuration or state.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.12	Do not embed remote administrative capabilities into a publicly accessible application or API, use a separate and distinct communications channel	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_8.4	IoT Endpoints that have user interfaces such as touch screens, rich displays, or alternative interface technologies, must be able to render information to the user and take information from a user in a secure manner. While attributes of the user interface, such as passwords, have already been covered in this document, there are some more subtle issues that must be discussed: Alerting systems Action confirmation When an anomaly has occurred, such as physical tampering or an application behaving in an unintended fashion, the user should receive a visible alert. Alternatively, the user should be able to review alerts from the system from within the User Interface.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_5.3	In order for an application to run properly, it must be loaded and executed in a consistent way on a reliable, high quality, and secure platform. The TCB defines how to formulate this platform, but the Bootstrap model defines how the application shall be ran on top of it.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.7.1	**BOOT PROCESS INTEGRITY.** The boot process initializes the main hardware components, and starts the operating system. Trust must be established in the boot environment before any trust in any other software or executable program can be claimed. So the booted environment must be verified and determined to be in an uncompromised state.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS.** Intercepts or overrides of the system boot process, ②+③: The endpoint boot process can be altered by modifying the firmware interface between the hardware platform firmware and the operating system such as the unified extensible firmware interface (UEFI) or basic Input/output system (BIOS)1. Changes to the bootloader are another threat as changes could compromise the integrity of the endpoint by starting unauthorized or insecure versions of the operating system. Attacks at this level could also affect the normal or secure boot process of the endpoint, the recognition of all the hardware resources and the establishment of a solid root of trust for securing other components. • Compromises to the Guest OS, Hypervisors and Separation Kernels, ④+⑤: These	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS.** Compromises to the Guest OS, Hypervisors and Separation Kernels, ④+⑤: These software layers control allocation of hardware resources to applications. Attacks to these layers can alter the behavior of the system, allow information flows to bypass security controls and enable attackers to gain privileged access to endpoint hardware and software resources. Once access is gained to this layer, attackers will have opportunity to affect the entire software stack and further alter security controls built in to this level.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS.** Illicit changes to Application Software or exposed Application Programming Interface (API), ⑥+⑦+⑧+⑨: Endpoint applications are often the target for malware or an attacker seeking to infiltrate and compromise the endpoint. Execution of malicious applications or overriding of application APIs can adversely impact the trustworthiness of the endpoint. Exposed APIs should also be protected against denial of service attack where continuous access from unauthorized users could limit the responsiveness and access to the exposed functionality.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS.** Vulnerabilities of the Deployment Process, ⑩: Errors and potential malicious code may also infiltrate the endpoint as part of the deployment process, for example, incorrect or malicious installation scripts, intercepted communications, or unauthorized replacement of a package on the update server. Reduction of possible endpoint configurations in large-scale endpoint deployments will be important in reducing complexity and vulnerabilities in the deployment process.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS.** Vulnerabilities in the Development Environment, ⑮: The introduction of weaknesses during the software development lifecycle can leave the IIoT systems susceptible to attack. These weaknesses may be introduced during architecting, designing, or writing of the code. Use of vulnerable or malicious libraries or untrusted development frameworks may lead to their inclusion in the resulting code running in the IIoT system.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.4	**ESTABLISH ROOTS OF TRUST.** The roots of trust (RoT), or trust roots, consisting of hardware, software, people and organizational processes, establish confidence in the system. An endpoint without a correctly implemented RoT will lack the ability to establish confidence that it will behave as intended. The root of trust on a device determines the level of confidence in the authenticity of the credentials belonging to that particular device. The root of trust should be able to generate, manage and store at least one identity.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.7.2	**RUNTIME INTEGRITY.** After the boot-process integrity has been attested to, the OS is running and applications can execute. Runtime integrity controls monitor, and ideally, enforce the integrity of the endpoint beyond the boot process	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Society (ISOC)	The Internet of Things: An Internet Society Public Policy Briefing	Security	Ensuring lifetime security in IoT products and services must be a fundamental priority to maintain overall user trust in this technology. Users need to trust that IoT devices and related data services are secure, especially as they become more pervasive and integrated into our daily lives.	https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-IoT.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.4.1	The product's processor system has an irrevocable Secure Boot process.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.4.4	The Secure Boot process is enabled by default.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.8.2	Where the product has a secure source of time there is a method of validating its integrity, such as Secure NTP. https://www.ntpsec.org/.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.1	The product has measures to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or sandbox.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.6	To prevent the stalling or disruption of the devices software operation any watchdog timers for this purpose cannot be disabled.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.7	The product's software signing root of trust is stored in tamperresistant memory.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.8	The product has protection against reverting the software to an earlier and potentially less secure version.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.22	The device remains secure and maintains state during a side channel attack.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.5.24	The software has been designed to fail safely, i.e. in the case of unexpected invalid inputs, or erroneous software operation, the product does not become dangerous, or compromise security of other connected systems.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.14.5	Where a product includes a trusted secure boot process, the entire production test and any related calibration is executed with the processor system operating in its secured boot, authenticated software mode.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	Security Design Best Practices		Fingerprint and validate the integrity of critical system operating thresholds or parameters.	https://www.iotsi.org/security-best-practices
IoT Security Initiative	Security Design Best Practices		Make use of secure boot, secure micro-kernels and hardware virtualization capabilities whenever possible.	https://www.iotsi.org/security-best-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Microsoft	IoT Security Best Practices	Follow secure software development methodology	Development of secure software requires ground-up thinking about security, from the inception of the project all the way to its implementation, testing, and deployment. The choices of platforms, languages, and tools are all influenced with this methodology. The Microsoft Security Development Lifecycle provides a step-by-step approach to building secure software.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Microsoft	IoT Security Best Practices	Choose open-source software with care	Open-source software provides an opportunity to quickly develop solutions. When you're choosing open-source software, consider the activity level of the community for each open-source component. An active community ensures that software is supported and that issues are discovered and addressed. Alternatively, an obscure and inactive open-source software project might not be supported and issues are not likely be discovered.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Microsoft	IoT Security Best Practices	Integrate with care	Many software security flaws exist at the boundary of libraries and APIs. Functionality that may not be required for the current deployment might still be available via an API layer. To ensure overall security, make sure to check all interfaces of components being integrated for security flaws.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.2.1	In order to ensure that all components of a device are operating properly and have not been tampered with, it is best to ensure that the device is booted properly. There may be multiple stages of boot. The end result is an application running on top an operating system that takes advantage of memory, CPU and peripherals through drivers.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1	15.1.1.3	Secure download and boot – To prevent the loading and execution of malicious software, where it is practical, it is recommended that Secure Download and Secure Boot methods that authenticate a binary’s source as well as its contents be used.	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Software and Information Industry Association (SIIA)	Empowering the Internet of Things: Benefits	6	Policies for Embedded Software Should Provide for Product Integrity	http://www.siia.net/Portals/0/pdf/Policy/Reports/Empowering%20the%20Internet%20of%20Things.pdf
Symantec	An Internet of Things Security Reference Architecture		In powering up, each device boots and runs some code. In that context, it is crucial that we ensure devices only do what we programmed them to do, and ensure that others cannot reprogram them to behave maliciously. In other words, the first step in protecting a device is to protect the code to be sure the device only boots and runs code that you want it running. Fortunately, many chipmakers already build “secure boot” capabilities into their chips. Similarly, for “higher level” code, a number of time-proven, opensource, and client-side libraries like OpenSSL can easily be used to check signatures of code, and accept code only if it comes from an authorized source. In that context, signing firmware, boot images, and higherlevel embedded code are all increasingly common, including signing the underlying software components such as any operating system, and not just applications, but all code on the device. This approach can ensure that all critical components, sensors, actuators, controllers, and relays are all properly configured to only run signed code and never run unsigned code.	https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.1.8	**Secure Evolvability.** The principle of secure evolvability states that a system should be developed to facilitate the maintenance of its security properties when there are changes to its functionality structure, interfaces, and interconnections (i.e., system architecture) or its functionality configuration (i.e., security policy enforcement). These changes may include for example: new, enhanced, and upgraded system capability; maintenance and sustainment activities; and reconfiguration. Although it is not possible to plan for every aspect of system evolution, system upgrades and changes can be anticipated by analyses of mission or business strategic direction; anticipated changes in the threat environment; and anticipated maintenance and sustainment needs.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.1.16	**Self-Reliant Trustworthiness.** The principle of self-reliant trustworthiness states that systems should minimize their reliance on other systems for their own trustworthiness. A system should be trustworthy by default with any connection to an external entity used to supplement its function.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.2.3	**Self-Analysis.** The principle of self-analysis states that a component must be able to assess its internal state and functionality to a limited extent at various stages of execution, and that this self-analysis capability must be commensurate with the level of trustworthiness invested in the system. At the system level, self-analysis can be achieved via hierarchical trustworthiness assessments established in a bottom up fashion. In this approach, the lower-level components check for data integrity and correct functionality (to a limited extent) of higher-level components. For example, trusted boot sequences involve a trusted lower-level component attesting to the trustworthiness of the next higher-level components so that a transitive chain of trust can be established.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.4.2	**Defense in Depth.** Defense in depth describes security architectures constructed through the application of multiple mechanisms to create a series of barriers to prevent, delay, or deter an attack by an adversary.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Code of Practice: 8 - Ensure that personal data is protected

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Report: Working Group 4 – Policy	5	1. Proactive not Reactive; Preventative not Remedial Privacy by Design is characterised by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. It does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.	https://aioti.eu/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Report: Working Group 4 – Policy	5	2. Privacy as the Default Setting Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the product, by default.	https://aioti.eu/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf
Alliance for Internet of Things Innovation (AIOTI)	Report: Working Group 4 – Policy	5	3. End-to-End Security – Full Lifecycle Protection Privacy by Design extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion.	https://aioti.eu/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf
Alliance for Internet of Things Innovation (AIOTI)	Report: Working Group 4 – Policy	5	5. Respect for User Privacy – Keep it User-Centric Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.	https://aioti.eu/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Basic Requirements on PRACTICAL PRIVACY IN IoT	No Personal Data by Default, 'As-If' by Design & De-Identification by Default Data minimalisation starts with only requesting, collecting, obtaining, deriving and processing personal data to the extent necessary (need-to-know principle), and. The 'As-If' principle it to design and engineer ecosystems in IoT as if these will (now or in a later phase) process personal data. The As-If principle is closely related to the privacy by design and privacy by default principles. Design de-Identification capabilities so personal data is de-identified as soon as legally possible.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Manufacturer-Implemented Parametrization	Rights management for accessing data controlled by the user based on the assessment where and when a Thing or IoT ecosystems in its lifecycle comes into contact with personal data, creates/derives (new) personal data, or otherwise processes personal data, while keeping in my mind the contextuality of purposes and use, as well as multi-purpose Things and IoT ecosystems.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Awareness & Information Supplied with Indication of Purpose	Technically regulating access to data to define who can use it for what purpose, and how that can be made transparent, and subsequently measured and monitored. Design in a transparent way, so the data subject is and remains clear and aware of privacy issues, choices it makes and possible consequences thereof.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
Alliance for Internet of Things Innovation (AIOTI)	AIOTI Digitisation of Industry Policy Recommendations	3.32 (ii) First bullet point	Promote transparency about what data is collected (including passive collection in smart spaces and smart cities) and do so in a way which is clear and simple for the user	https://aioti.eu/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf
Alliance for Internet of Things Innovation (AIOTI)	AIOTI Digitisation of Industry Policy Recommendations	3.32 (ii) Second bullet point	Implement privacy enhancing techniques such as data segmentation, segregation, aggregation, pseudonymisation, tokENISAtion and anonymization to the extent possible.	https://aioti.eu/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Atlantic Council Scowcroft Center for Strategy and Security	Smart Homes and the Internet of Things		Describe the ways in which customer data is used or will be used, as well as methods for consumers to opt out. This includes change in ownership of the company, or sharing information with third-parties.	http://www.atlanticcouncil.org/images/publications/Smart_Homes_0317_web.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.7	**IoT Devices Should Ship with a Privacy Policy That is Easy to Find & Understand.** BITAG recommends that IoT devices ship with a privacy policy, but that policy must be easy for a typical user to find and understand.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
City of New York (NYC) Guidelines for the Internet of Things	Privacy + Transparency	1.1	The City should make processes and policies related to IoT and IoT-related data publicly available in an up-to-date, clear and comprehensive manner. IoT principles, guidelines, operational policies and responsibilities should be transparent and made public via a City government website.	https://iot.cityofnewyork.us/privacy-and-transparency/
City of New York (NYC) Guidelines for the Internet of Things	Privacy + Transparency	1.3	Data and information collected by IoT devices should be classified and treated accordingly, per the City of New York's Data Classification Policy, as Public, Sensitive, Private or Confidential. All personally identifiable information (PII) should be classified at a minimum as private. All data that is classified as being confidential, or personally identifiable, should be protected from unauthorized use and disclosure.	https://iot.cityofnewyork.us/privacy-and-transparency/
City of New York (NYC) Guidelines for the Internet of Things	Privacy + Transparency	1.4	PII should by default be anonymized before being shared in any way that could make the information publicly searchable or discoverable. Any copies and reproductions must have the same or higher level of classification as the original. Any combinations of data should be reclassified according to the City's Data Classification Policy.	https://iot.cityofnewyork.us/privacy-and-transparency/

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
City of New York (NYC) Guidelines for the Internet of Things	Privacy + Transparency	1.5	PII data types should have a clearly associated retention policy and disposal procedure. Sensitive, private or confidential data should be kept for no longer than is operationally necessary or required for the specified, explicit and legitimate purposes.	https://iot.cityofnewyork.us/privacy-and-transparency/
City of New York (NYC) Guidelines for the Internet of Things	Privacy + Transparency	1.6	Before any sensitive, private, or confidential data is shared outside the originating City agency, the agency should ensure that the need cannot be met by using anonymized or aggregated data and that the appropriate protections are in place to preserve the confidentiality of the data.	https://iot.cityofnewyork.us/privacy-and-transparency/
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.1.1	Users of IoT systems should be made aware of all of the data collected from or about them, and should be given the opportunity to opt out of data collection practices at a granular level. Recognizing the concerns that many of the IoT devices may not have proper user interface, companies should find suitable methods to provide the choice and notice to consumers.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.1.4	Within the IoT, data collected will have a long lifespan. It is important to consider the full lifespan of the data collected, both within the collecting organization and within any third parties to which it is provided. Stakeholders should be made aware of when data is provided to third parties, the controls used to secure it, and how and when the data is disposed of	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.1.5	Stakeholders should be able to easily identify the data collected from them for any particular IoT system, as well as the planned or potential uses for that data. Stakeholders should also be allowed to opt in to data collection, at both a coarse and granular level.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.3.3	Limit the data that is being collected or aggregated by a gateway to what is really necessary.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
European Commission and AIOTI	Report on Workshop on Security & Privacy in IoT	1) 1)	Data control by the user – in any phase of the data life cycle and product life cycle	http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf
European Commission and AIOTI	Report on Workshop on Security & Privacy in IoT	1) 2)	Transparency and user interface control – empower the user to obtain sufficient knowledge on what its devices and related system are doing and sharing, even if it concerns M2M communications and transactions	http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-10	Personal data must be collected and processed fairly and lawfully. The fairness principle specifically requires that personal data should never be collected and processed without the data subject's consent.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-11	Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-12	Minimise the data collected and retained. Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion should take place at the nearest point of data collection of raw data (e.g. on the same device after processing).	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-13	IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR). The complex mesh of stakeholders involved asks for/implies the necessity of a precise allocation of legal responsibilities among them with regard to the processing of the individual's personal data, based on the specificities of their respective interventions.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-14	Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-12	Data processed by a third-party (i.e., if the organisation utilises a cloud email provider), must be protected by a data processing agreement with the third-party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-OP-13	Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require that thirdparty service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorised access.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-PS-08	Privacy must be a guiding principle when designing and developing systems, in order to make privacy an integral part of the system.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-29	Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy. The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software management or hardware security).	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	5.2, fourth bullet point	User data protection: the integrity, confidentiality and authenticity of user data must be protected. Confidentiality protection must be defined with regards to privacy issues.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	7.1	Users shall verify the authorisations given to devices and services for data access and data exchange. This is particularly true in case of an update where access rights may be modified without user's consent. For example, devices and services can display a comprehensive view of their communications with external devices and services, their requirement to use private data, etc.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
GSMA	GSMA IoT Security Assessment	CLP11_6	Privacy Considerations	https://www.gsma.com/iot/iot-security-assessment/
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.7	An imperative aspect of IoT technology is their ability to connect the physical world to the digital world. The result of this is a gap in privacy, as the user's physical environment is directly associated with the things they like and view online. This may cause undesirable effects over time. As a result, it is important that IoT Service Providers consider the privacy of their consumers and develop Privacy Management interfaces that are integrated into both the Endpoint, where possible, and the product or service's web interface. This technology should allow the user to determine what attributes of their privacy are being utilized by the system, what the Terms of	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			Service are, and the ability to turn off the exposure of this information to the business or its partners. This granularity and opt-out system will help to ensure that users have the right and the ability to control the information that they share about themselves and their physical world.	
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_8.3	Build an API for Users to Control Privacy Attributes. All users must be able to control what information they offer to third parties, through service APIs. The information should be classified into types of data, and attributed with security classifications. Users should be able to retrieve the types of data and classifications that are used in the modelling of their account. The user should be able to apply constraints to the types of data, to allow them to grant or revoke access to this data to Partners.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_5.11	To properly manage interactions with Partner organizations effectively, security classifications must be defined. This will set the tone for not only the internal organizational policy on data security, but will help define the level of security Partner organizations apply to the business's data, their own data, and customer's data.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_5.12	After defining security classifications, the organization should define types of data to be used by the overall IoT product or service. This will enable the organization to clearly define what types of information are acquired, generated, and disseminated to peers in the IoT system, and how the organization should treat these types of data. This data will provide context and value to the overall components used throughout the IoT environment. While this document will not attempt to model all variations of data that may be relevant to a specific organization, certain types may be as follows: • Users • Actions • Images • Editable documents • Personally-Identifiable Information • Protected Health Information	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.1	While the privacy model deals with the way user's information is offered to Partners, the authorization model defines how the business or Partners will act on behalf of a user. This, for instance, would come in handy for a home automation system where a Partner's metrics could optimize the use of heating or cooling in a given home. The authorization model would grant the Partner the ability to change heating or cooling controls for that user's home when certain metrics were detected by the Partner.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_6.7	Defining policies and procedures for the classification of data is not enough. There must also be a model for detecting whether the data has been exposed by a Partner. The organization must have a plan in place to evaluate whether a Partner was involved in business practices that breach the technological controls or policies set in place to guard user's data and privacy.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_7.4	After security classifications have been defined, and data types have been attributed a valid classification, and a breach policy has been enacted, a data distribution policy should be generated. A data distribution policy describes how information should be processed through technical controls and out to service applications that have been granted permission to access the data. The permissions model is a part of the data distribution policy, and pairs with the user's ability to create granular data permissions.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_8.3	All users must be able to control what information they offer to third parties, through service APIs. The information should be classified into types of data, and attributed with security classifications. Users should be able to retrieve the types of data and classifications that are used in the modelling of their account. The user should be able to apply constraints to the types of data, to allow them to grant or revoke access to this data to Partners. This can come in the form of an authenticated API, or a GUI that allows simple Yes or No controls on a general, and per-Partner basis.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
IEEE	IoT Security Principles and Best Practices	9	The basic idea of IoT is to connect everyday objects via Internet or ad-hoc network. IoT devices provide services that are discoverable by other IoT devices. Most of the protocols leak sensitive personally identifiable information (PII,) like owner's name or information that may be linkable to an individual, like a device's host name. This information can be linked to other information sources to target attacks. Service mechanisms and authentication protocols are required so that only authorized clients can discover the device.	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IERC-European Research Cluster on the Internet of Things (IERC)	IoT Governance, Privacy and Security Issues - IERC Position Paper		Stick flow policies combine sticky policies for data with their flow policies, i.e. a data item in a system using this technology is annotated with a security policy which describes how a data item can be used and which conditions have to be satisfied before an item can flow to another entity.	http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf
IERC-European Research Cluster on the Internet of Things (IERC)	IoT Governance, Privacy and Security Issues - IERC Position Paper		Context-sharing enabled objects must be able to answer the question which information should be shared with whom. This question can be automatically answered, if the object has a fine-grained privacy policy that contains both the trusted objects and the context characteristics allowed for sharing. Additionally, an object needs mechanisms that enforce this policy. The contents of a policy are typically user and thus, object dependent. Many users have different opinions about what kind of context should be regarded as private and not every object supports all types of context. As a consequence, we can expect that some policies might be more restrictive than others.	http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf
IERC-European Research Cluster on the Internet of Things (IERC)	IoT Governance, Privacy and Security Issues - IERC Position Paper		The same ability of third parties to know that two entities are exchanging data can be a violation of privacy. Both users and services might need to operate in given scenarios without releasing identification, addressing or other sensitive information the other endpoint. This can be in conflict with the some requirements related to authentication, authorization and non-repudiation.	http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.8.1	**DATA CONFIDENTIALITY.** Data confidentiality refers to ensuring that information is not disclosed to unauthorized parties. To implement this, cryptography renders data unintelligible to unauthorized entities that do not have the proper key for decryption of the data. The algorithm must be designed and implemented to ensure that no unauthorized party can determine the keys associated with the encryption or derive the plaintext. Data confidentiality is often mandated by regulations, in particular when privacy of the records is important or the record contains personally identifiable information (PII). Some fields in a record may contain sensitive data that requires confidentiality while other fields need to be processed by an application. In this case, data tokenization can replace sensitive fields or the value can be modified so confidentiality and privacy of those fields is preserved	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Intel	Policy Framework for the Internet of Things (IoT)	Privacy and Security	Privacy and security are critical building blocks for our nation's IoT ecosystem – and capabilities that must be designed into our IoT systems from the outset using the best known Privacy-by-Design methodologies.	https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-framework.pdf
Intel	Policy Framework for the Internet of Things (IoT)	Privacy and Security	The IoT presents new challenges for traditional privacy principles. Consumer notice and consent will continue to be important, however other privacy principles must also be emphasized to ensure consumer privacy is adequately protected. For example, focusing on accountability for the appropriate collection, use, and protection of the consumer's data.	https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-framework.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Intel	Policy Framework for the Internet of Things (IoT)	Privacy and Security	Optimal privacy and security methods must be developed as required for different IoT solutions. Use cases should be used to proactively identify privacy and security risks and to develop robust strategies to mitigate those risks.	https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/policy-iot-framework.pdf
International Electrotechnical Commission (IEC)	IoT 2020: Smart and secure IoT platform	5.2.2.1.3	Performance requirements of future IoT systems will result in scenarios in which computations on data collected from devices will have to be executed as close as possible to devices. Often, those domains may not meet the security requirements of the data owner, i.e. the data should not be disclosed to the component of the IoT system which processes it. Thus mechanisms are required which will make it possible to protect the confidentiality and integrity of data, while still allowing execution of computations and production of meaningful results for the data owner.	http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.6	An IoT device user/owner would like to monitor and verify its operational behavior. For instance, the user might want to know if the device is connecting to the server of the manufacturer for any reason. This feature - connecting to the manufacturer's server – may be necessary in some scenarios, such as during the initial configuration of the device. However, the user should be kept aware of the data that the device is sending back to the vendor. For example, the user might want to know if his/her TV is sending data when he/she inserts a new USB stick.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.9	1. Identification - refers to the identification of the users, their IoT devices, and generated data. 2. Localization - relates to the capability of locating a user and even tracking them, e.g., by tracking MAC addresses in Wi-Fi or Bluetooth. 3. Profiling - is about creating a profile of the user and their preferences. 4. Interaction - occurs when a user has been profiled and a given interaction is preferred, presenting (for example, visually) some information that discloses private information. 5. Lifecycle transitions - take place when devices are, for example, sold without properly removing private data. 6. Inventory attacks - happen if specific information about IoT devices in possession of a user is disclosed. 7. Linkage - is about when information of two of more IoT systems (or other data sets) is combined so that a broader view of the personal data captured can be created.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			When IoT systems are deployed, the above issues should be considered to ensure that private data remains private. These issues are particularly challenging in environments in which multiple users with different privacy preferences interact with the same IoT devices. For example, an IoT device controlled by user A (low privacy settings) might leak private information about another user B (high privacy settings). How to deal with these threats in practice is an area of ongoing research.	
Internet Society (ISOC)	The Internet of Things: An Internet Society Public Policy Briefing	Encourage responsible design practices for IoT services	Security-by-design and privacy-by-design practices for IoT devices should be encouraged. Whether via privacy and data protection regulation, voluntary industry selfregulation, or other incentives or policy means, IoT device developers should be encouraged to respect the end-user's privacy and data security interests and	https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-IoT.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			consider those interests a core element of the product-development process.	
Internet Society (ISOC)	The Internet of Things: An Internet Society Public Policy Briefing	Privacy	IoT devices that collect data about people in one jurisdiction may transmit that data to another jurisdiction for data storage or processing. Challenges can arise if the data collected is deemed to be personal or sensitive and is subject to data protection laws in multiple jurisdictions. Enabling cross-border data flows that protect privacy and promote legal certainty for users and IoT service providers will be key for promoting the global growth of IoT	https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-IoT.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.1	The product/service stores the minimum amount of Personal Information from users.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.2	The product/service ensures that all Personal Information is encrypted at rest and in transit.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.3	The product/service ensures that only authorised personnel have access to personal data of users.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.4	The product/service ensures that Personal Information is anonymised whenever possible and in particular in any reporting.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.5	The Product Manufacturer or Service Provider shall ensure that a data retention policy is in place, and compliant with the legal requirements for the territories the product or service is deployed.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.6	There is a method or methods for the product owner to be informed about what Personal Information is collected, why, where it will be stored.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.7	There is a method or methods for the product owner to check/verify what Personal Information is collected and deleted.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.8	The product / service can be made compliant with the local and/or regional Personal Information protection legislation where the product is to be sold.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.9	The supplier or manufacturer of any device shall provide information about how the device(s) functions within the end user's network.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.10	The supplier or manufacturer of any devices or devices shall provide information about how the device(s) shall be setup to maintain the end user's privacy and security.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.11	The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal shall be carried out to maintain the end user's privacy and security.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.12	The supplier or manufacturer of any devices or services shall provide clear information about the end user's responsibilities to maintain the devices and/or services privacy and security.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 19	A device is designed and architected to protect personal privacy through data collection transparency and anonymization of user activity.	https://www.iotsi.org/iot-cybersecurity-principles
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 20	A device clearly identifies the collection or processing of personally identifiable data in the Device Support-Level Agreement (DSLA).	https://www.iotsi.org/iot-cybersecurity-principles
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 21	A device in active use to identify and/or track persons and their activity is overtly identified as such to the public in the devices operating environment.	https://www.iotsi.org/iot-cybersecurity-principles
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 22	A published Device Security Level Agreement (DSLA) is maintained once initially created to provide the change history of material modifications to this public information.	https://www.iotsi.org/iot-cybersecurity-principles

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Object Management Group (OMG) Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	Data Sovereignty	The physical location in which data is stored may be regulated, with the regulations varying from country to country. This is particularly the case for personally identifiable information (PII) and for sensitive data such as health data and financial records. The European Union has particularly stringent regulations that apply to the PII of European citizens. As a result, any IoT cloud system must take into account data sovereignty rules and store and process data only in those locations permitted by the regulations – this requires that the provider cloud used provides the cloud service customer with control over storage and processing locations.	https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	9.3	Although a user of a M2M System is generally considered to be an application or functional agent that represents a human, there are links between a device and its user that can be either directly derived or indirectly deduced. Consequently, identifiers used for communication in the M2M System should not be directly related to the real identity of either the device or its user, except where this is a requirement for operation of a specific M2M Application. The use of pseudonyms is a means to support this requirement.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	20	Conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used, limiting collection to data which is reasonably useful for the functionality and purpose for which it is being collected. Disclose and provide consumer opt-in for any other purposes.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	22	. Disclose the data retention policy and storage duration of personally identifiable information.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	25	Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require that third-party service providers are held to the same polices, including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorized access.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	26	Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the "factory default."	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	27	Commit to not sell or transfer any identifiable consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, provided the acquiring party's privacy policy does not materially change the terms. Otherwise notice and consent must be obtained.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	29	Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to product features or functionality. It is recommended the end-user value of opting in and/or sharing data be communicated to the end user.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	30	Comply with applicable regulations, including but not limited to the Children's Online Privacy Protection Act (COPPA) and international privacy, security and data transfer regulatory requirements. 3 4	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	31	Publicly post the history of material privacy notice changes for a minimum of two years. Best practices include date stamping, redlines, and summary of the impacts of the changes.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Web Application Security Project (OWASP)	IoT Security Guidance	I5: Privacy Concerns	Ensure only the minimal amount of personal information is collected from consumers	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I5: Privacy Concerns	Ensure all collected personal data is properly protected using encryption at rest and in transit	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I5: Privacy Concerns	Ensure only authorized individuals have access to collected personal information	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I5: Privacy Concerns	Ensuring data is de-identified or anonymized	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I5: Privacy Concerns	Ensuring a data retention policy is in place	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I5: Privacy Concerns	Ensuring end-users are given a choice for data collected beyond what is needed for proper operation of the device	https://www.owasp.org/index.php/IoT_Security_Guidance

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Software and Information Industry Association (SIIA)	Empowering the Internet of Things: Benefits	2	Privacy Rights for the IoT Should Be Based on Risk and Societal Benefits.	http://www.siia.net/Portals/0/pdf/Policy/Reports/Empowering%20the%20Internet%20of%20Things.pdf
Telecommunications Industry Association (TIA)	Realizing the Potential of the Internet of Things: Recommendations to Policy Makers		Industry believes that IoT services must adopt principles similar to those that have worked successfully on the Internet to enable informed consumer choice: transparency about what data will be collected, how it will be used, and who will have access.	https://www.tiaonline.org/wp-content/uploads/2018/05/Realizing_the_Potential_of_the_Internet_of_Things_-_Recommendations_to_Policymakers.pdf
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.2.10	**Acceptable Security.** The principle of acceptable security requires that the level of privacy and performance the system provides should be consistent with the users' expectations. The perception of personal privacy may affect user behavior, morale, and effectiveness. Based on the organizational privacy policy and the system design, users should be able to restrict their actions to protect their privacy. When systems fail to provide intuitive interfaces, or meet privacy and performance expectations, users may either choose to completely avoid the system or use it in ways that may be inefficient or even insecure.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Code of Practice: 9 - Make systems resilient to outages

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Atlantic Council Scowcroft Center for Strategy and Security	Smart Homes and the Internet of Things		**Standalone Operation.** Document which specific features and benefits will continue to work without Internet access and chronicle negative impacts from compromised devices or cloud-based systems. The most proactive companies may find it less expensive to buy back obsolete devices, rather than continue to support them."	http://www.atlanticcouncil.org/images/publications/Smart_Homes_0317_web.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.4	**IoT Devices Should Continue to Function if Internet Connectivity is Disrupted.** BITAG recommends that an IoT device should be able to perform its primary function or functions (for example, a light switch or a thermostat should continue to function with manual controls), even if it is not connected to the Internet. This is because Internet connectivity may be disrupted due to causes ranging from accidental misconfiguration or intentional attack (e.g., a denial of service attack); device function should be robust in the face of these types of connectivity disruptions. IoT devices that have implications for user safety should continue to function under disconnected operation to protect the safety of consumers. In these cases, the device or backend system should notify the user about the failure. When possible, device manufacturers should make it easy for users to disable or block (e.g.,with a firewall) various network traffic without hampering the device's primary function.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.5	**IoT Devices Should Continue to Function If the Cloud Back-End Fails**. Many services that depend on or use a cloud back-end can continue to function, even if in a degraded or partially-functional state, when connectivity to the cloud back-end is interrupted or the service itself fails. For example, a thermostat whose setting can be altered via a cloud service should in the worst case continue to operate using either lastknown or default settings. A cloud-hosted	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			home security camera should be accessible from within the home, even when Internet connectivity fails.	
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.1	**The IoT Supply Chain Should Play Their Part In Addressing IoT Security and Privacy Issues.** Manufacturers should support for an IoT device throughout the course of its lifespan, from design to the time when a device is retired, including transparency about the timespan over which they plan to provide continued support for a device, and what the consumer should expect from the device's function at the end of the device's lifespan.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
CableLabs	A Vision for Secure IoT	DDoS Monitoring and Mitigation Systems	Many cable operators have deployed DDoS monitoring and mitigation systems to ensure the continued availability of their broadband Internet access services during an attack. A DDoS attack seeks to make a device, service, or network resource unavailable to its intended users by flooding the target with superfluous network traffic in an attempt to overload systems and prevent legitimate traffic from getting through to the target of the attack. A significant DDoS attack will typically originate from many thousands or hundreds of thousands of compromised devices. Both the frequency and magnitude of DDoS attacks continue to grow, fueled in large part by the proliferation of insecure IoT.	https://www.cablelabs.com/insights/vision-secure-iot/

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
CableLabs	A Vision for Secure IoT	Availability	A secure IoT device is available when it is needed for its legitimate use and unavailable when it is not. IoT devices should be designed to function in a predictable and expected manner, if and when there is a loss of broadband connectivity or a loss of communications with any associated cloud service. Conversely, devices should use restrictive, rather than permissive, default network traffic policies to limit communications to expected norms, guarding against both unintended as well as malicious denial of service attacks that can disrupt the availability of the device or other devices on the network.	https://www.cablelabs.com/insights/vision-secure-iot/
CableLabs	A Vision for Secure IoT	Prevention of IP Address Spoofing	Source Address Validation (SAV) is a recommended best practice for all ISPs, hosting providers, cloud providers and others to prevent reflective DDoS attacks.[SAV with spoofed packet dropping is supported in Cable Modem Termination Systems (CMTS) equipment deployed in cable access networks globally. This feature became available in the Data Over Cable Service Interface Specification (DOCSIS) release 3.0, first issued in 2006, as a mandatory requirement. Moreover, the DOCSIS specification requires that SAV be turned on by default for DOCSIS 3.0 and 3.1 compliant CMTS devices.	https://www.cablelabs.com/insights/vision-secure-iot/
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-46	Rate limiting – controlling the traffic sent or received by a network to reduce the risk of automated attacks.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information	Baseline Security Recommendations for IoT	GP-TM-51	Implement a DDoS-resistant and Load-Balancing infrastructure to protect the services against DDoS attacks which can affect the device itself or other devices and/or users on the local network or other networks.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Security (ENISA)				
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-15	Design with system and operational disruption in mind. Build IoT devices to fail safely and securely, so that the failure does not lead to a greater systemic disruption. Have a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g. energy, gas, heat or water), preventing the system from causing unacceptable risk of injury or physical damage, protecting the environment against harm, and avoiding interruption of safety-critical processes.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	6.1	Hardware must provide basic reliability measures to resist outages and jamming The typical examples are: • In case of outage (power, network or simply the associated cloud services): o Provide the user with a notification o Provide smart fail-safe mechanism or standalone option (if an outage or denial of service happens, devices should be able to go offline, continue to provide their functionalities, and synchronize to remote services as soon as they become available again). • For network: use the diversity of available interfaces (including hardwired connections) or RF spectrum to maintain connection. • For power: use battery back-up and/or alternate charging options.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-PS-03	Security must consider the risk to human safety	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-PS-04	Designing for power conservation should not compromise security.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_5.4	For publicly accessible services, several pieces of security and reliability technology are required to maintain the availability, confidentiality, and integrity of the service: DDoS-resistant infrastructure Load-Balancing infrastructure Redundancy systems Web Application Firewalls (optional) Traditional Firewalls	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.12-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_9.1	For radio communications, there is a constant threat of jamming, or the intentional broadcasting of noise or patterns that can be used to scramble legitimate signals. As radio signals are simply composed of electrons flying through space in a specific pattern, it is fairly easy to concoct a series of signals that interrupt or mangle the pattern that forms communications data.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_9.1	Intentional or Unintentional Denial of Service	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_8.7	Components within an embedded system are designed to be used within certain environmental thresholds. This includes voltage levels, current draw, ambient or operating temperature, and humidity. Each component is typically rated for certain windows of approved levels. If the device is subjected to states above or below a given window, the component may act erratically, or behave in a fashion that is useful to an adversary. Therefore, it is important to detect changes to these environmental levels to determine whether the device should continue running, or if it should power off. It should be noted, however, that powering off may be a desired effect, and that the adversary may abuse this engineering decision to leverage a denial of service. The engineering team should evaluate this model to determine if it is more beneficial to shut down or more beneficial to attempt to stay online	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_8.8	Endpoints that provide critical services to the user must be enabled with a warning threshold that indicates power-related events. These events may include: Low battery state Critically low battery state Black-out events Brown-out events Switch to battery back-up events	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_5.8.3	Backup channels in case of physical or logical link failure	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_5.8.3	Protection against Denial of Service attacks	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_5.8.3	Restrict communications options to the strict minimum required for a given IoT Service.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS.** Unwanted changes to Endpoint Data, ⑪: Data throughout the endpoint from low-level firmware all the way up the software stack represents a key area of vulnerability. These vulnerabilities include unauthorized access to mission-critical or private data. Attackers may adversely affect the behavior of the system by injecting false data. Denial-of-service attacks on data access may impede timely and accurate execution of the endpoint functionality resulting in costly outcomes.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.1	**SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS.** Breach of the Monitoring & Analysis system, ⑫: An attacker could gain visibility on the functions of the monitored system. For example, an attacker could modify monitoring data to make it appear as if a particular event did not occur. Modification of the security logs and monitoring data may result in undetected vulnerabilities or compromised states. As a result, attackers would benefit from a coverage gap, compromising endpoint hardware and software or destroying evidence of their activities after an attack.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
International Electrotechnical Commission (IEC)	IoT 2020: Smart and secure IoT platform	5.2.5.4	Reliable and trustworthy actuation requires new technologies and extended system architectures to ensure reliable execution of tasks and to be able to recover from system failures, e.g. from the network or from devices.	http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices	2.2.3	A device SHOULD be designed to gracefully tolerate excessive numbers of authentication attempts, for instance by giving CPU priority to existing protocol sessions that have already successfully authenticated, limiting the number of concurrent new sessions in the process of authenticating, and randomly discarding attempts to establish new sessions beyond that limit. The specific mechanism is a design choice to be made in light of the specific function of the device and the protocols used by the device. What's important for this requirement is that this be an explicit choice.	https://tools.ietf.org/html/draft-moore-iot-security-bcp-01
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.1.2	The tight memory and processing constraints of things naturally alleviate resource exhaustion attacks.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.20	Where a Product or Services includes any safety critical or lifeimpacting functionality, the services infrastructure shall incorporate protection against DDOS attacks, such as dropping of traffic or sinkholing. See NIST 800-53 SC-5 [32]	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.13.21	Where a Product or Services includes any safety critical or lifeimpacting functionality, the services infrastructure shall incorporate redundancy to ensure service continuity and availability.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 18	Devices supporting sensitive or safety-critical functions are designed and architected to continue safe and secure operation during communications interruption or failure.	https://www.iotsi.org/iot-cybersecurity-principles
Object Management Group (OMG) Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	Resilience	In IoT systems resilience and fault tolerance is very important. IoT systems should not depend on one single component at any point and should tolerate the failure of a single component, such as a single IoT device. Components in the provider cloud can be made resilient through the use of multiple instances of programs and cloud services allied with data replication and redundancy on multiple storage systems. The networks should also be resilient, for example with multiple paths and multiple providers in the public network.	https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf
Open Web Application Security Project (OWASP)	IoT Security Guidance	I3: Insecure Network Services	Review all required network services for vulnerabilities such as buffer overflows or denial of service	https://www.owasp.org/index.php/IoT_Security_Guidance
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Design with system and operational disruption in mind. Understanding what consequences could flow from the failure of a device will enable developers, manufacturers, and service providers to make more informed risk-based security decisions. Where feasible, developers should build IoT devices to fail safely and securely, so that the failure does not lead to greater systemic disruption.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.2.6	**Secure Failure and Recovery.** The principle of secure failure and recovery states that neither a failure in a system function or mechanism nor any recovery action in response to failure should lead to a violation of security policy. This principle parallels the principle of continuous protection to ensure that a system is capable of detecting (within limits) actual and impending failure at any stage of its operation (i.e., initialization, normal operation, shutdown, and maintenance) and to take appropriate steps to ensure that security policies are not violated.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
W3C	Web of Things (WoT) Security and Privacy Considerations	4.1.3	**Avoid Heavy Functional Processing without Authentication.** When defining WoT Interfaces exposed by a TD, it is important to avoid any heavy functional processing before the successful authentication of a WoT client. Any publicly exposed network interface should avoid heavy processing altogether.	https://www.w3.org/TR/wot-security/#recommended-security-practices

Code of Practice: 10 - Monitor system telemetry data

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
City of New York (NYC) Guidelines for the Internet of Things	Security	4.6	The City and its partners should engage in both audit-based and continuous monitoring to ensure that systems are working and that devices have not been compromised.	https://iot.cityofnewyork.us/security/
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.5.4	Monitoring for security events within an IoT infrastructure should also be done, ideally on a 24/7 basis. Planning for the capture of security-relevant data and establishment of rules for identifying events or combinations of events-of-interest should be conducted early on in the engineering lifecycle. Consider having security analysts charged with near-real time monitoring of the security posture of your implementation	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.7	As can be seen, it is important to understand what components within the IoT ecosystem will actually provide audit data feeds and which components should actually be mined for anomalous behavior within their operational data stream. As an example, considering which components are owned by a consumer will allow for a plan to captured and analyze appropriate data (e.g. failed logins). It is also important to ensure that no sensitive (privacy-related) information is included in the audit logs unless it is protected using sufficient security safeguards (e.g. encryption).	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.7.2	In general, it is important to log data that may indicate that an incident has occurred or will occur. Whenever possible, the following minimum data elements should be logged.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-56	Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-57	The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches. Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-55	Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. The logs must also be preserved on durable storage and retrievable via an authenticated connection.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	5.2, first bullet point	Security audit: security events must be logged, and users should be notified whenever needed.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
GSMA	GSMA IoT Security Assessment	CLP13_6.13	Logging and Diagnostics	https://www.gsma.com/iot/iot-security-assessment/

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	Analytics-based Security	CLP14_5.8.2	Network Operators can provide data analytics and deep packet inspection services to identify threats and anomalies in the data generated by IoT Services. An example could be that a Network Operator could periodically perform deep packet inspection for specific strings like social security numbers and GPS coordinates that might suggest that such information is not protected properly and alert the IoT Service Provider responsible that information could be leaking.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.14-v2.0.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_7.2	Modelling Endpoint behaviour is an imperative part of IoT security. This is because a compromised Endpoint can be indistinguishable from an Endpoint behaving normally if only successful interactions with the device are logged and analysed. For a more comprehensive perspective of an IoT environment, the full behavioural fingerprint of a device should be catalogued to identify anomalies that may be indicative of adversarial behaviour.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_5.7	Each system must be monitored to allow administrators and Information Technology (IT) works to detect and diagnose anomalies. Monitoring must be performed at multiple dimensions. For example, network monitoring at the infrastructure level helps diagnose application attacks or DDoS against network components	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_7.2	Use Partner-Enhanced Monitoring Services. This will allow the IoT business to more quickly identify whether a particular user or Endpoint is either a threat, or has been compromised by an adversary. As a result, businesses may react more effectively to pre-empt attacks against other areas of the business's infrastructure.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
GSMA	IoT Security Guidelines for Service Ecosystems	CLP12_8.4	While false positive analysis is an extremely complex topic, there is a simple way to identify whether a technology is more likely to present false positives. This is by evaluating the following items: • Is the data source trustworthy • Can the data source be tampered with or spoofed • Is the data source from the analogue domain • Can the data be corroborated from multiple points of origin • Do the corroborating data sources exist on the same endpoint system • Are corroborating data sources easy to tamper with or spoof • Are tools readily available to manipulate the data source • What level of expertise or cost is required to manipulate the data source • Is the device attached to the data source trustworthy	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.3	**ENDPOINT PROTECTION.** Endpoint Monitoring and Analysis includes integrity checking, detecting malicious usage patterns, denial of service activities, enforcement of security policies and analytics that track security performance indicators.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.3	**ENDPOINT PROTECTION.** Endpoint Monitoring & Analysis is responsible for ensuring the prevention, detection and recovery from any activity deviant from policy, while Endpoint Configuration & Management ensures that all changes made to the endpoints are performed in a controlled and managed manner.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.3	**ENDPOINT PROTECTION.** Endpoint Data Protection is responsible for protecting access and preventing tampering with data-at-rest and data-in-use on the endpoint through encryption, isolation and access control. Data protection spans all data on the endpoint, including configuration, monitoring, and operational data.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.4	**COMMUNICATIONS AND CONNECTIVITY PROTECTION.** Information Flow Protection ensures that only permitted kinds of messages and content reach sensitive systems and networks by isolating network flows using network segmentation and perimeter protection technologies	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.4	**COMMUNICATIONS AND CONNECTIVITY PROTECTION.** Network Monitoring and Analysis collects network data for analysis and includes intrusion detection, network access control, deep packet inspection and network log analysis.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.5	**SECURITY MONITORING AND ANALYSIS.** Monitor. As determined by the security model and policy, monitoring captures and aggregates data from each of the sources in the system: • Endpoints & Communications: Monitoring data is gathered by a local agent running on each of the endpoints and communications in the system obtaining information on the implementation of security controls in accordance with the system security policy. • Secure Remote Logging: The sending and receiving of log messages using secure communications. • Supply Chain: Collecting data from all components builders and integrators in the supply chain to assure that security requirements are met.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.5	**SECURITY MONITORING AND ANALYSIS.** Analyze. Analysis uses looks for events (for example, violation of security thresholds) and trends that may uncover certain system security vulnerabilities or threats. This phase stores and saves the information for audit or other mining purposes. There are two types of analysis: • Behavioral Analysis observes the usage patterns in the system and learns what is appropriate behavior for the system. • Rule-Based Analysis monitors for violations of predefined policy rules that define events that should never occur in the system.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.5	**SECURITY MONITORING AND ANALYSIS.** Act. Having analyzed events and trends, action must be taken. There are three types: • Proactive/Predictive attempts to mitigate threats before the attack begins by observing leading indicators of an imminent attack. • Reactive detection & Recovery provides manual and automated responses to attacks in progress and tries to mitigate them to recover and return to normal runtime state. • Root Cause/Forensics analysis and forensics investigates the underlying vulnerabilities and exploits after the attack.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.7	**ENDPOINT INTEGRITY PROTECTION.** Measuring the device boot process enables the validation of its integrity, so we may assert that a device has powered up in a known good state. Given that devices may not be rebooted for long periods of time in OT environments, both static and dynamic integrity assurance of the runtime should also be implemented. Identity material must be properly secured in the trust roots to maintain its integrity and avoid identity spoofing, and data integrity must be monitored and maintained to establish trust in the data, including both data-at-rest and data-in-motion.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.8.2	**DATA INTEGRITY.** Data integrity assures that data alteration is detected. Traditional OT data integrity techniques (e.g. a CRC checksum) increase reliability and resilience of a system but are not effective against some malicious alterations due to their lack of cryptographic strength. Newer techniques such as digital signatures provide greater trust in the integrity measurements.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	8.9	**ENDPOINT MONITORING AND ANALYSIS.** Monitoring mechanisms should also be protected. Endpoint monitoring concerns itself with detection of possible tampering with or compromise of devices, which would result in incorrect reporting of events. Monitoring of the endpoint security status may be performed internally on the endpoint or may be performed externally to the endpoint. Monitoring of least-capable edge devices	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			will most likely be executed from another endpoint in the operational domain.	
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	10	**SECURITY MONITORING AND ANALYSIS.** Security monitoring aggregates and stores a variety of types of data from running Industrial Internet of Things systems, enabling analysis into past compromises, current security events and the prediction of future risks. Security analytic tools provide useful feedback to the organization via parameters suitable for high-level dashboard display.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	10.3.1	**LOGGING AND EVENT MONITORING.** All security monitoring designs must consider the risk that a successful intruder can erase all evidence of their activities. Transmitting the most important security monitoring data to external monitoring systems in a secure and timely manner mitigates this risk. Endpoints must log data based on both local endpoint events and communications events. Logging to a network log system can also mitigate attempts of intruders to interfere with the integrity of log data.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	10.3.2	**CAPTURING AND MONITORING SECURITY DATA.** Monitoring data can come from many sources, in particular endpoints and the network. This data should be communicated securely to monitoring and analytics systems.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	11.9	**CONFIGURATION AND MANAGEMENT DATA PROTECTION.** Security management maintains the consistency of security over time, and must not interfere with operational processes. Security metadata such as connection status and characteristics (encrypted or authenticated), and the state of security controls on the device should be gathered and shared with operation management systems so that it can be tracked. The security metadata should be sent on a separate communications channel from the operational application data.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
International Electrotechnical Commission (IEC)	IoT 2020: Smart and secure IoT platform	5.2.6	The platform will also provide capabilities for the monitoring of devices in the IoT system and for anomaly detection. Important to these capabilities are additional capabilities for the coordination and analysis of data to determine events. This is half of the observe-orient-decide-act (OODA) cycle for detection and response to system threats.	http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security	5.6	An IoT device user/owner would like to monitor and verify its operational behavior. For instance, the user might want to know if the device is connecting to the server of the manufacturer for any reason. This feature - connecting to the manufacturer's server – may be necessary in some scenarios, such as during the initial configuration of the device. However, the user should be kept aware of the data that the device is sending back to the vendor. For example, the user might want to know if his/her TV is sending data when he/she inserts a new USB stick.	https://datatracker.ietf.org/doc/draft-irtf-t2trg-iot-seccons/
IoT Security Foundation	Connected Consumer Secure Design Best Practice Guidelines	N/A	K: Logging	https://www.iotsecurityfoundation.org/best-practice-guidelines/

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Microsoft	IoT Security Best Practices	Audit frequently	Auditing IoT infrastructure for security-related issues is key when responding to security incidents. Most operating systems provide built-in event logging that should be reviewed frequently to make sure no security breach has occurred. Audit information can be sent as a separate telemetry stream to the cloud service where it can be analyzed.	https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices
Object Management Group (OMG) Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	Security Monitoring, Analysis, and Response	Every system must have monitoring of the environment built in so that active attacks as well as anomalous behavior is detected and acted upon. Because of the scale of IoT systems, both in the number of devices as well as the amount of information being processed, there is a requirement for automated response to known attacks as well as automatic detection of suspicious behavior.	https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf
Object Management Group (OMG) Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	Security	As more data about people, financial transactions and operational decisions is collected, refined and stored, the challenges related to information governance and security increase. The data privacy and identity management of devices and individual is very important from the cloud computing point of view. The cloud generally allows for faster deployment of new compliance and monitoring tools that encourage agile policy and compliance frameworks. Cloud data hubs can be a good option by acting as focal points for data assembly and distribution. Tools that monitor activity and data access can actually make cloud systems more secure than standalone systems. Hybrid systems offer unique application governance features: Software can be centrally maintained in a distributed environment with data stored in-house to meet jurisdictional policies.	https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	4	IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least semi-annually.2	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Open Web Application Security Project (OWASP)	OWASP Secure Coding Practices Quick Reference Guide	Error Handling and Logging	Do not disclose sensitive information in error responses, including system details, session identifiers or account information Use error handlers that do not display debugging or stack trace information Implement generic error messages and use custom error pages The application should handle application errors and not rely on the server configuration Properly free allocated memory when error conditions occur Error handling logic associated with security controls should deny access by default All logging controls should be implemented on a trusted system (e.g., The server) Logging controls should support both success and failure of specified security events Ensure logs contain important log event data Ensure log entries that include un-trusted data will not execute as code in the intended log viewing interface or software Restrict access to logs to only authorized individuals Utilize a master routine for all logging operations Do not store sensitive information in logs, including unnecessary system details, session identifiers or passwords Ensure that a mechanism exists to conduct log analysis Log all input validation failures Log all authentication attempts, especially failures Log all access control failures Log all apparent tampering events, including unexpected changes to state data Log attempts to connect with invalid or expired session tokens Log all system exceptions Log all administrative functions, including changes to the security configuration settings Log all backend TLS connection failures Log cryptographic module failures Use a cryptographic hash function to validate log entry integrity	https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Open Web Application Security Project (OWASP)	IoT Security Guidance	I8: Insufficient Security Configurability	Ensure secure logging is available for security events	https://www.owasp.org/index.php/IoT_Security_Guidance
Symantec	An Internet of Things Security Reference Architecture		Of course, no matter how well you protect the device, protect the code, protect the communications, and no matter how well you manage your security posture, even using the best possible OTA management framework, some adversaries still have the resources and capabilities to rise above those defenses. For such reasons, strategic threats require strategic mitigation technologies. Security analytics can leverage security telemetry from devices and network hardware to help provide an understanding of what is happening in the environment, including detection of stealthier threats. Equally importantly, “monitoring” and analytics can often be deployed as an interim solution in environments where upgrading devices to conform to the first three cornerstones above will take years. Examples of such environments include legacy devices such as industrial control systems (manufacturing, oil and gas, utilities) that cannot be modified until an end-to-end replacement system is ready, automotive cars already on the road whose deeply embedded microcontrollers obviously cannot be “torn out and replaced,” and healthcare environments where suppliers prohibit hospitals from modifying the equipment to add security. In such cases, anomaly detection solutions can be extremely valuable. The deterministic nature of many IoT networks allows the system to be baselined and deviations quickly identified. The wide variety of industrial and IoT protocols can make the problem harder, but newer techniques using advanced machine learning can allow the problem to be solved. Considering that many IoT systems have high demands on availability, this solution is less invasive in “detect” mode while ensuring that any false positives do not bring down the system.	https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.2.4	**Accountability and Traceability.** The principle of accountability and traceability states that it must be possible to trace securityrelevant actions (i.e., subject-object interactions) to the entity on whose behalf the action is being taken. This principle requires a trustworthy infrastructure that can record details about actions that affect system security (e.g., an audit subsystem). To do this, the system must not only be able to uniquely identify the entity on whose behalf the action is being carried out, but also record the relevant sequence of actions that are carried out.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Code of Practice: 11 - Make it easy for customers to delete personal data

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Workshop on Security and Privacy in the Hyper connected World	Awareness & Information Supplied with Indication of Purpose	Technically regulating access to data to define who can use it for what purpose, and how that can be made transparent, and subsequently measured and monitored. Design in a transparent way, so the data subject is and remains clear and aware of privacy issues, choices it makes and possible consequences thereof.	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf
AT&T	The CEO's Guide to Securing the Internet of Things		**System reset.** Every device should include a way to reset it to its original manufactured clean state.	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.10	**Reset mechanism.** Devices should have a reset mechanism for IoT devices that clears all configuration for use when a consumer returns or resells the device. The device manufacturers should also provide a mechanism to delete or reset any data that the respective device stores in the cloud.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.5.5.1	Due to the quantities involved with many IoT implementations, it is likely that many edge devices will be replaced on a regular basis. It is important to establish policies and procedures for the secure disposition of devices that have held sensitive information or key material that could provide access to sensitive information. Devices that have held sensitive information should be securely wiped to include removal of key material and certificates from each device.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)	5.5	Life cycle controls for IoT edge devices require the management and monitoring of assets to ensure that they are authorized, and secure and regularly updated with the latest firmware, software and patches. In addition, organization's must have a documented method for securely disposing of IoT assets at the end of the life-cycle. Define a life-cycle management approach for IoT devices.	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
European Union Agency for Network and Information Security (ENISA)	Security and Resilience of Smart Home Environments	7.3	The end-user must have a way to securely erase its private data collected by or stored on a Smart Home device.	https://www.ENISA.europa.eu/publications/security-resilience-good-practices
GSMA	GSMA IoT Security Assessment	CLP11_6	Privacy Considerations	https://www.gsma.com/iot/iot-security-assessment/
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_8.10	All Endpoint devices have a lifecycle, as discussed elsewhere in this document. Some devices must be decommissioned due to a user cancelling their subscription, while other devices must be decommissioned due to anomalous or adversarial behaviour. Regardless of the reason, the business must be prepared to decommission the device securely using their TCB and communications model.	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
IEEE	IoT Security Principles and Best Practices	4	We suggest manufacturers prepare a formal plan for users to sanitize and dispose of obsolete IoT devices. Industry practice in other fields prescribes a "discard, recycle or destroy" (DRD) policy with periodic review of the plan to determine which devices require disposal and how to dispose of them. Some manufacturers encourage users to dispose of products directly through the manufacturer. This may be sensible for laptops and servers, but for IoT devices that may be small and cheap, or that are part of a much	https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
			larger device (like a refrigerator) special accommodations may be required.	
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.7	There is a method or methods for the product owner to check/verify what Personal Information is collected and deleted.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.10	The supplier or manufacturer of any devices or devices shall provide information about how the device(s) shall be setup to maintain the end user's privacy and security.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.11	The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal shall be carried out to maintain the end user's privacy and security.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.12	The supplier or manufacturer of any devices or services shall provide clear information about the end user's responsibilities to maintain the devices and/or services privacy and security.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.16.1	Where a device or devices are capable of having their ownership transferred to a different owner, all the previous owners Personal Information shall be removed from the device(s) and registered services. This option must be available when a transfer of ownership occurs or when an end user wishes to delete their Personal Information from the service or device.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.16.2	Where a device or devices user wishes to end the service, all that owners Personal Information shall be removed from the device and related services.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	CyberSecurity Principles of IoT	PRINCIPLE 17	A device storing personal or operationally sensitive information integrates data wipe capabilities into its design and architecture for standard use and decommissioning scenarios.	https://www.iotsi.org/iot-cybersecurity-principles
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	24	Disclose if and how IoT device/product/service ownership and the data may be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker).	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	26	Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the “factory default.”	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	32	Provide the ability for the user or proxy to delete, or make anonymous, personal or sensitive data stored on company servers (other than purchase transaction history) upon discontinuing use, loss or sale of device.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

Code of Practice: 12 - Make installation and maintenance of IoT devices easy

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Alliance for Internet of Things Innovation (AIOTI)	Digitisation of Industry Policy Recommendations	3.32 (iii) first bullet point	Promote products and services which help deliver flexibility and openness in service provision.	https://aioti.eu/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
AT&T	The CEO's Guide to Securing the Internet of Things		**Device support.** Device makers should provide online access to operators' manuals, access to updates, and updated instructions. Support information should include a clear explanation of the product's support lifecycle.	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
AT&T	The CEO's Guide to Securing the Internet of Things		**Contact information and support forum.** Vendors should provide contact details or a support forum to which organizations can report any problems with the device or its software.	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
AT&T	The CEO's Guide to Securing the Internet of Things		**Basic support label.** Each device should carry a label that helps the authorized operator identify it and find support information.	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
Atlantic Council Scowcroft Center for Strategy and Security	Smart Homes and the Internet of Things		Give owners clear guidance on why and how to configure devices to their own particular preferences, and ensure that defaults are reasonably safe and secure.	http://www.atlanticcouncil.org/images/publications/Smart_Homes_0317_web.pdf
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.10	**Clear methods for consumers to determine who they can contact for support.** Manufacturers should provide clear methods for consumers to determine who they can contact for support and methods to contact consumers to disseminate information about software vulnerabilities or other issues.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations	7.1	**IoT Device Configurations Should Be Tested and Hardened.** Some IoT devices allow a user to customize the behavior of the device. BITAG recommends that manufacturers test the security of each device with a range of possible configurations, as opposed to simply the default configuration. A device's interface should prevent—or at least actively discourage—users from configuring the device in a way that makes it less secure.	http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf
GSMA	IoT Security Guidelines Endpoint Ecosystem	CLP13_6.8	Uniquely Provision Each Endpoint	https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	7.9	**FROM FUNCTIONAL TO IMPLEMENTATION VIEWPOINT.** Principle of psychological acceptability: it is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0	11.7.1	**ENROLLMENT PHASE.** There are three steps to the enrollment phase: initiation, entity verification and registration. Initiation declares the desire to bring the entity under management and give it identity and credentials. Verification involves proving that the entity is the one for which the identity is to be created and issued. Registration (see Figure 11-6) means the entity is ready to have credentials created and delivered, or to have the entity generate the credentials itself. Always validate that the identity that was registered was the one bound to the credential that was generated for the entity.	https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.12	The supplier or manufacturer of any devices or services shall provide clear information about the end user's responsibilities to maintain the devices and/or services privacy and security.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.12.13	Security Usability: Devices and services should be designed with security usability in mind, reducing where possible, security friction and decision points that may have a detrimental impact on security. Best practices on usable security should be followed, particularly for user interaction and user interfaces.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	23	IoT devices must provide notice and/or request user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5	26	Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the “factory default.”	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
Open Web Application Security Project (OWASP)	IoT Security Guidance	I8: Insufficient Security Configurability	Ensure alerts and notifications are available to the user for security events	https://www.owasp.org/index.php/IoT_Security_Guidance
U.S. Department of Homeland Security	Strategic Principles for Securing The Internet of Things (IoT)		Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable selective connectivity. Depending on the purpose of the IoT device, providing the consumers with guidance and control over the end implementation can be a sound practice.	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link
US National Institute of Standards and Technology (NIST)	NIST SP.800-160 Systems Security Engineering	F.2.9	**Human Factored Security.** The principle of human factored security states that the user interface for security functions and supporting services should be intuitive, user friendly, and provide appropriate feedback for user actions that affect such policy and its enforcement. The mechanisms that enforce security policy should not be intrusive to the user and should be designed not to degrade user efficiency. They should also provide the user with meaningful, clear, and relevant feedback and warnings when insecure choices are being made.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Code of Practice: 13 - Validate input data

Organisation	Standard / Recommendation Name	Recommendation Number / Section	Recommendation Extracted from Linked Source	Web Link

European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-54	Data input validation (ensuring that data is safe prior to use) and output filtering. Security is a concern for decision triggers (malware or general defects). Other possibilities here might be indirect manipulation of input values to the trigger by tampering with or restricting the input values. Reliability is a concern for decision triggers (general defects). Decision triggers could be inconsistent, self-contradictory, and incomplete. Understanding how bad data propagates to affect decision triggers is paramount. Failure to execute decision triggers at time may have undesired consequences	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT	GP-TM-42	Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for trustable solutions and services. For example, a device measures its own integrity as part of boot, but does not validate those measurements - when the device applies to join a network, part of joining involves sending an integrity report for remote validation. If validation fails, the end point is diverted to a remediation network for action.	https://www.ENISA.europa.eu/publications/baseline-security-recommendations-for-iot
GSMA	GSMA IoT Security Assessment	CLP12_6.9	Implement Input Validation	https://www.gsma.com/iot/iot-security-assessment/
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.10.1	Where the product or service provides a web based interface, Strong Authentication is used	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.10.10	All data being transferred over interfaces should be validated where appropriate. This could include checking the Data Type, Length, Format, Range, Authenticity, Origin and Frequency."	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.10.11	Sanitise input in Web applications by using URL encoding or HTML encoding to wrap data and treat it as literal text rather than executable script	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.10.12	All inputs and outputs are validated using for example a whitelist containing authorised origins of data and valid attributes of such data.	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.11.7	All data being transferred over interfaces should be validated where appropriate. This could include checking the Data Type, Length, Format, Range, Authenticity, Origin and Frequency."	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf

IoT Security Foundation	IoT Security Compliance Framework 1.1	2.4.11.9	All application inputs and outputs are validated using for example a whitelist containing authorised origins of data and valid attributes of such data see NIST SP 800-167 [34]	https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf
IoT Security Initiative	Security Design Best Practices		Do not trust data input – sanitize to what is needed and expected for the function on intake.	https://www.iotsi.org/security-best-practices
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.20	Implement secure coding practices that enforce rigorous input data validation in system and services, database applications, and web services	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.21	Preventing injection requires keeping un-trusted data separate from commands and queries. If a parameterized API is not available, escaping special characters using the specific escape syntax for that interpreter should be done.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.22	Put in place encryption and/or strong session management security controls. Implement secure coding practices that enforce rigorous input data validation in system and services, database applications, and web services.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf
oneM2M	TR-0008-V2.0.1 Security (Technical Report)	8.2.26	Positive or "whitelist" input validation helps to protect against cross scripting. Such validation should decode any encoded input, and then validate the length, characters, and format on that data before accepting the input.	http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf

Open Web Application Security Project (OWASP)	OWASP Secure Coding Practices Quick Reference Guide	Input validation	Conduct all data validation on a trusted system (e.g., The server) Identify all data sources and classify them into trusted and untrusted. Validate all data from untrusted sources (e.g., Databases, file streams, etc.) There should be a centralized input validation routine for the application Specify proper character sets, such as UTF-8, for all sources of input Encode data to a common character set before validating (Canonicalize) All validation failures should result in input rejection Determine if the system supports UTF-8 extended character sets and if so, validate after UTF-8 decoding is completed Validate all client provided data before processing, including all parameters, URLs and HTTP header content (e.g. Cookie names and values). Be sure to include automated post backs from JavaScript, Flash or other embedded code Verify that header values in both requests and responses contain only ASCII characters Validate data from redirects (An attacker may submit malicious content directly to the target of the redirect, thus circumventing application logic and any validation performed before the redirect) Validate for expected data types Validate data range Validate data length Validate all input against a "white" list of allowed characters, whenever possible If any potentially hazardous characters must be allowed as input, be sure that you implement additional controls like output encoding, secure task specific APIs and accounting for the utilization of that data throughout the application . Examples of common hazardous characters include: < > " ' % ( ) & + \ \' \" If your standard validation routine cannot address the following inputs, then they should be checked discretely Check for null bytes (%00) Check for new line characters (%0d, %0a, \r, \n)	https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

			Check for “dot-dot-slash" (../ or ..\) path alterations characters. In cases where UTF-8 extended character set encoding is supported, address alternate representation like: %c0%ae%c0%ae/	
Open Web Application Security Project (OWASP)	IoT Security Guidance	I1: Insecure Web Interface	Ensure that any web interface in the product has been tested for XSS, SQLi and CSRF vulnerabilities	https://www.owasp.org/index.php/IoT_Security_Guidance
Open Web Application Security Project (OWASP)	IoT Security Guidance	I6: Insecure Cloud Interface	Ensure that any cloud-based web interface has been tested for XSS, SQLi and CSRF vulnerabilities	https://www.owasp.org/index.php/IoT_Security_Guidance

Disclaimer and copyright

The information in this document is for general guidance and is not to be relied upon as professional advice.

DCMS has used reasonable endeavours to ensure that the information in this document is accurate and up to date. DCMS shall not accept liability for any loss, damage or inconvenience arising as a consequence of any use of or the inability to use any links contained in this document. DCMS shall not be responsible for claims brought by third parties arising from your use of this document.

DCMS assumes no responsibility for the contents of linked websites. The inclusion of any link should not be taken as endorsement of any kind by DCMS of the linked website or any association with its operators. Further, DCMS has no control over the availability of the linked pages. References to organisations do not imply endorsement by DCMS.

Department for Digital, Culture, Media & Sport

4th Floor, 100 Parliament Street
London, SW1A 2BQ
GOV.UK/DCMS