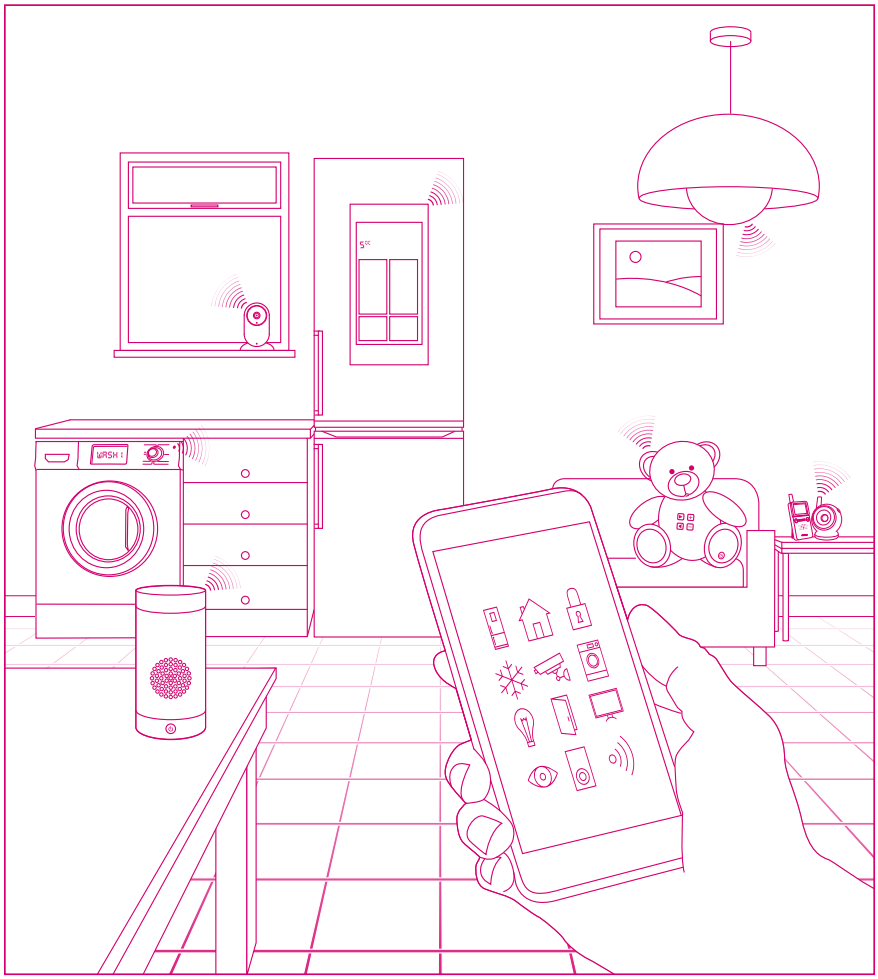
Department for
Digital, Culture,
Media & Sport

Code of Practice for Consumer IoT Security



October 2018

Executive Summary

As we connect more devices in our homes to the internet, products and appliances that have traditionally been offline are now becoming part of the 'Internet of Things' (IoT).

The IoT represents a new chapter of how technology becomes increasingly common in our homes, making people's lives easier and more enjoyable. As people entrust an increasing amount of personal data to online devices and services, the cyber security of these products is now as important as the physical security of our homes.

The aim of this Code of Practice is to support all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in a digital world.

The Code of Practice brings together, in thirteen outcome-focused guidelines, what is widely considered good practice in IoT security. It has been developed by the Department for Digital, Culture, Media and Sport (DCMS), in conjunction with the National Cyber Security Centre (NCSC), and follows engagement with industry, consumer associations and academia. The Code was first published in draft in March 2018 as part of the Secure by Design report.[1]

[1] DCMS, 2018, 'Secure by Design: Improving the cyber security of consumer Internet of Things: Report', https://www.gov.uk/government/publications/secure-by-design

Introduction

The Internet of Things (IoT) brings great opportunities for people. But a significant number of devices on the market today have been found to lack basic security measures. People should be able to benefit from connected technologies safely, confident that adequate security and privacy measures are in place to protect their online activity.

This Code of Practice sets out practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services. Implementing its thirteen guidelines will contribute to protecting consumers' privacy and safety, whilst making it easier for them to use their products securely. It will also mitigate against the threat of Distributed Denial of Service (DDoS) attacks that are launched from poorly secured IoT devices and services.

The guidelines bring together what is widely considered good practice in IoT security. They are outcome-focused, rather than prescriptive, giving organisations the flexibility to innovate and implement security solutions appropriate for their products.

This Code of Practice is not a silver bullet for solving all security challenges. Only by shifting to a security mindset and investing in a secure development lifecycle can an organisation succeed at creating secure IoT. Products and services should be designed with security in mind, from product development through their entire lifecycle. Organisations should also regularly assess cyber security risks relevant to their products and services and implement appropriate measures to address these.

The supply chains of IoT products can be complex and international, often involving multiple component manufacturers and service providers. The aim of the Code is to initiate and facilitate positive security change throughout the entire supply chain.

A number of industry bodies and international fora are developing security recommendations and standards for IoT.[2] This Code of Practice is designed to be complementary to and supportive of those efforts and relevant published cyber security standards. It has been created directly with industry with the hope that future assurance and trustmark schemes related to consumer IoT will align with it.

Implementing the Code of Practice may help organisations achieve compliance with applicable data protection laws. For example, the EU General Data Protection Regulation (GDPR) requires personal data to be processed securely.[3]

Implementation

The Code of Practice is supported by a mapping document and an open data JSON file that link each of the Code's guidelines against the main industry standards, recommendations and guidance.[4] This mapping gives additional context to the Code's thirteen guidelines and helps industry to implement them. The mapping also shows the relationship between the Code and the work on IoT security that is being carried out by a wide array of global organisations.

Prioritisation and structure

The first three guidelines are prioritised because action on default passwords, vulnerability disclosure and security updates will bring the largest security benefits in the short term.

The supporting text articulates the rationale and adds further detail for each guideline. Additional explanatory notes at the end of the document answer frequently asked questions.

[2] PETRAS, 2018, 'Summary literature review of industry recommendations and international developments on IoT security', https://www.gov.uk/government/publications/secure-by-design
[3] Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data
[4] DCMS, 2018, 'Mapping of IoT Security Recommendations, Guidance and Standards to the Code of Practice for Consumer IoT Security', https://www.gov.uk/government/publications/secure-by-design

Audiences

An indication is given for each guideline as to which stakeholder is primarily responsible for implementation. Stakeholders are defined as:

Device Manufacturer – The entity that creates an assembled final internet-connected product. A final product may contain the products of many other different manufacturers.

IoT Service Providers – Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.

Mobile Application Developers – Entities that develop and provide applications which run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.

Retailers – The sellers of internet-connected products and associated services to consumers.

Terminology

The use of the term 'security-sensitive data' is intended to differentiate between other types of sensitive data – for example special category data (formally known as 'sensitive personal data') as defined in the GDPR. Security-sensitive data could include, for example, cryptographic initialisation vectors.

The term 'consumer' is used throughout for consistency; consumers can generally be considered the end users of IoT products and services.

Scope of applicability

This Code of Practice applies to consumer IoT products that are connected to the internet and/or home network and associated services. A non-exhaustive list of examples includes:

- Connected children's toys and baby monitors,
- Connected safety-relevant products such as smoke detectors and door locks,
- Smart cameras, TVs and speakers,
- Wearable health trackers,
- Connected home automation and alarm systems,
- Connected appliances (e.g. washing machines, fridges),
- Smart home assistants.

'Associated services' are here considered as the digital services that are linked to IoT devices, for example mobile applications, cloud computing/ storage and third party Application Programming Interfaces (APIs) to services such as messaging.

Review

The Department for Digital, Culture, Media and Sport will periodically review the Code and publish updates, at least every two years. Please contact securebydesign@culture.gov.uk to be kept informed.

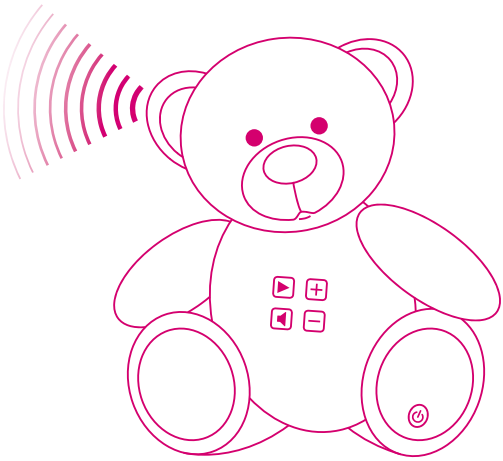
Guidelines

1) No default passwords

All IoT device passwords shall be unique and not resettable to any universal factory default value.

Many IoT devices are being sold with universal default usernames and passwords (such as 'admin, admin') which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed.[5]

Primarily applies to:
Device Manufacturers



[5] For guidance see, for example: NCSC, 2016, 'Password Guidance: Simplifying Your Approach', https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach. Also see: NIST, 2017, 'NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management', https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

2) Implement a vulnerability disclosure policy

All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.

Knowing about a security vulnerability allows companies to respond. Companies should also continually monitor for, identify and rectify security vulnerabilities within their own products and services as part of the product security lifecycle. Vulnerabilities should be reported directly to the affected stakeholders in the first instance. If that is not possible vulnerabilities may be reported to national authorities.[6] Further details of the different approaches to take in different circumstances are included in the explanatory notes. Companies are also encouraged to share information with competent industry bodies.[7]

Primarily applies to:
Device Manufacturers
IoT Service Providers
Mobile Application Developers

[6] In the UK, reports of vulnerabilities can be sent to: https://www.ncsc.gov.uk/contact
[7] Competent industry bodies include the GSMA and the IoT Security Foundation. Guidance on Coordinated Vulnerability Disclosure is available from the IoT Security Foundation which references the ISO/IEC 29147 standard on vulnerability disclosure. The GSMA's industry level Coordinated Vulnerability Disclosure programme is located at: https://www.gsma.com/cvd

3) Keep software updated

Software components in internet-connected devices should be securely updateable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

The provenance of security patches should also be assured and they should be delivered over a secure channel. The basic functions of a device should continue to operate during an update wherever possible, for example a watch should continue to tell the time, a home thermostat should still operate and a lock should continue to unlock and lock. This may seem primarily a design consideration, but can become a critical safety issue for some types of devices and systems if not considered or managed correctly.

Software updates should be provided after the sale of a device and pushed to devices for a period appropriate to the device. This period of software update support shall be made clear to a consumer when purchasing the product. The retailer and/or manufacturers should inform the consumer that an update is required. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear.

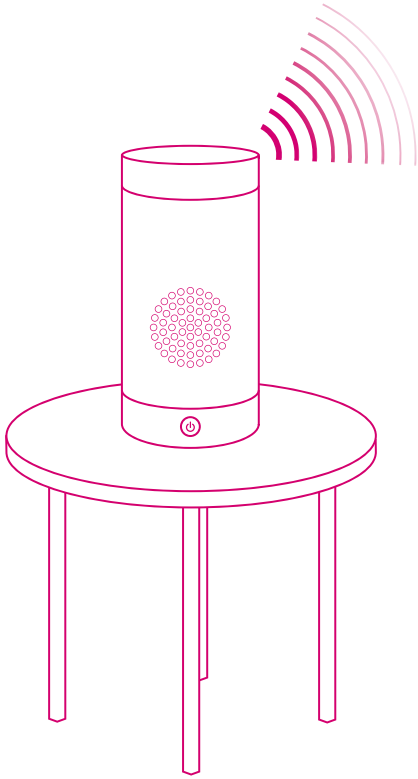
Primarily applies to:
Device Manufacturers
IoT Service Providers
Mobile Application Developers

4) Securely store credentials and security-sensitive data

Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.

Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be stored securely includes, for example, cryptographic keys, device identifiers and initialisation vectors. Secure, trusted storage mechanisms should be used such as those provided by a Trusted Execution Environment and associated trusted, secure storage.

Primarily applies to:
Device Manufacturers
IoT Service Providers
Mobile Application Developers



5) Communicate securely

Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.

The use of open, peer-reviewed internet standards is strongly encouraged.

Primarily applies to:
Device Manufacturers
IoT Service Providers
Mobile Application Developers

6) Minimise exposed attack surfaces

All devices and services should operate on the 'principle of least privilege'; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.

The principle of least privilege is a foundation stone of good security engineering, applicable to IoT as much as in any other field of application.

Primarily applies to:
Device Manufacturers
IoT Service Providers

7) Ensure software integrity

Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.

The ability to remotely recover from these situations should rely on a known good state, such as locally storing a known good version to enable safe recovery and updating of the device. This will avoid denial of service and costly recalls or maintenance visits, whilst managing the risk of potential takeover of the device by an attacker subverting update or other network communications mechanisms.

Primarily applies to:
Device Manufacturers

8) Ensure that personal data is protected

Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Device manufacturers and IoT service providers shall provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this shall be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time.

This guideline ensures that:

i. IoT manufacturers, service providers and application developers adhere to data protection obligations when developing and delivering products and services;

ii. Personal data is processed in accordance with data protection law;

iii. Users are assisted in assuring that the data processing operations of their products are consistent and that they are functioning as specified;

iv. Users are provided with means to preserve their privacy by configuring device and service functionality appropriately.

Primarily applies to:
Device Manufacturers
IoT Service Providers
Mobile Application Developers
Retailers

9) Make systems resilient to outages

Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.

IoT systems and devices are relied upon by consumers for increasingly important use cases that may be safety-relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures may include building redundancy into services as well as mitigations against DDoS attacks. The level of resilience necessary should be proportionate and determined by usage but consideration should be given to others that may rely on the system, service or device as there may be a wider impact than expected.

Primarily applies to:
Device Manufacturers
IoT Service Providers

10) Monitor system telemetry data

If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.

Monitoring telemetry, including log data, is useful for security evaluation and allows for unusual circumstances to be identified early and dealt with, minimising security risk and allowing quick mitigation of problems. In accordance with Guideline 8, however, the processing of personal data should be kept to a minimum and consumers shall be provided with information on what data is collected and the reasons for this.

Primarily applies to:
IoT Service Providers

11) Make it easy for consumers to delete personal data

Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.

IoT devices may change ownership and will eventually be recycled or disposed of. Mechanisms can be provided that allow the consumer to remain in control and remove personal data from services, devices and applications.

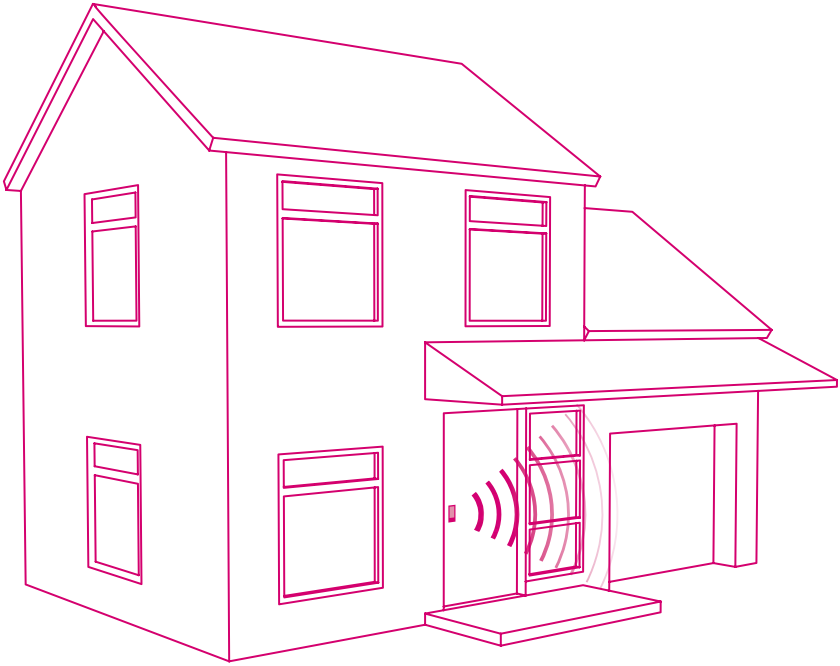
Primarily applies to:
Device Manufacturers
IoT Service Providers
Mobile Application Developers

12) Make installation and maintenance of devices easy

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.

Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats.

Primarily applies to:
Device Manufacturers
IoT Service Providers
Mobile Application Developers



13) Validate input data

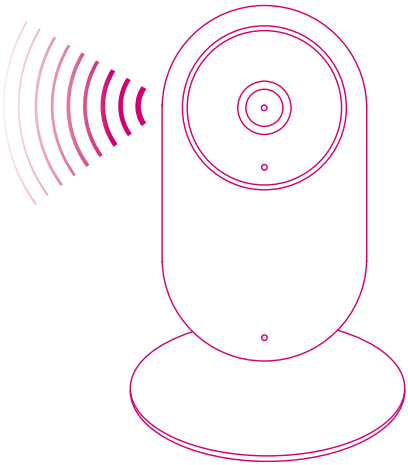
Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

Systems can be subverted by incorrectly formatted data or code transferred across different types of interface. Automated tools are often employed by attackers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is:

i. Not of the expected type, for example executable code rather than user inputted text.

ii. Out of range, for example a temperature value which is beyond the limits of a sensor.

Primarily applies to:
Device Manufacturers
IoT Service Providers
Mobile Application Developers



Additional explanatory notes

Guideline 1 on no default passwords: Whilst much work has been done to eliminate reliance on passwords and providing alternative methods of authenticating users and systems, some IoT products are still being brought to market with default usernames and passwords from user interfaces through to network protocols. This is not an acceptable practice and it should be discontinued. Device security can further be strengthened by having unique and immutable identities.

Guideline 2 on Coordinated Vulnerability Disclosure (CVD): CVD is standardised by the International Organization for Standardization (ISO), is simple to implement and has been proven to be successful in some large software companies around the world.[8] CVD is, however, still not established in the IoT industry and some companies may be reticent about dealing with security researchers. CVD provides a way for security researchers to contact companies to inform them of security issues putting the company ahead of the threat of malicious exploitation and giving them an opportunity to resolve vulnerabilities in advance of a public disclosure.

Companies that provide internet-connected devices and services have a duty of care to third parties who may be harmed by their failure to have a CVD programme in place. Additionally, companies that share this information through industry bodies can assist others who may be suffering from the same problem.

Disclosures may require different approaches depending on the circumstances:

- Vulnerabilities related to single products or services: the problem should be reported directly to the affected stakeholder (e.g. Device Manufacturer, IoT Service Provider or Mobile Application Developer). The source of these reports may be security researchers or industry peers. If, after making contact with the device manufacturer or other affected stakeholders, they are not acting in a timely manner then it is possible to report an issue directly to the NCSC.

[8] International Organization for Standardization, 2014, 'ISO/IEC 29147 - Vulnerability Disclosure', https://www.iso.org/standard/45170.html

- Systemic vulnerabilities: It may be the case that a stakeholder, such as a Device Manufacturer, discovers a problem that is potentially systemic. Whilst fixing it in the Device Manufacturer's own product is crucial, there is significant benefit to industry and consumers from sharing this information. Similarly, security researchers may also seek to report such systemic vulnerabilities. In this case, a relevant competent industry body can coordinate a wider scale response. The NCSC can provide advice and guidance to the competent industry body in order to deliver the coordinated response.

A 'timely manner' for acting on vulnerabilities varies considerably and is incident specific, however, the de facto standard for the vulnerability process to be completed is to not exceed 90 days. A hardware fix may take considerably longer to address than a software fix. Additionally, a fix that has to be deployed to devices may take time to roll out compared with a server software fix.

Guideline 3 on keeping software updated: Software security updates are one of the most important things a company can do to protect its customers and the wider technical ecosystem. Vulnerabilities often stem from software components that are not considered to be security related. Therefore as a general principle, all software should be kept updated and well maintained. Fixes can be pushed out to devices in a preventative manner, often as part of automatic updates, which can remove security vulnerabilities before it is exploited. Managing this can be complex, especially if there are cloud updates, device updates and other service updates to deal with. Therefore, a clear management and deployment plan is essential, as is transparency to consumers about the current state of update support.

In many cases publishing software updates will involve multiple dependencies on other organisations such as manufacturers of sub-components. This is not a reason to withhold updates – the aim of the Code of Practice is to instigate positive security change throughout the entire software supply chain. There are also some situations where devices cannot be patched. Some ultra-constrained devices will fit in this category and for these a replacement plan needs to be in place which should be clearly communicated to the consumer. This plan should detail a schedule for when technologies will need to be replaced and, where applicable, when support for hardware and software ends.

It may be critical for consumers that a device continues to function. This is why an update should 'not impact on the functioning of a device' where possible. Particularly, devices that fulfil a safety-relevant function should not turn completely off in the case of an update; there should be some minimal system functional capability, for example maintaining the operation of a heating system or a burglar alarm. Manufacturers of these types of devices should also consider moving towards an architecture which is more resilient.

It is important to be aware that software update mechanisms are a vector for attack and attention should be paid to ensuring that they are secured.

Guideline 5 on communicating securely: Appropriateness of security controls and the use of encryption is dependent on many factors including the usage context.[9] As security is ever-evolving it is difficult to give prescriptive advice about encryption measures without the risk of such advice quickly becoming obsolete. Implementers should ensure that their product can meet the needs of users whilst remaining resilient to attacks on encryption.

Guideline 7 on ensuring software integrity: If an IoT device detects something unusual has happened with its software, it needs to be able to inform the right person. In some cases, devices may have the ability to be in administration mode – for example, there may be a user mode for a thermostat in a room that prevents other settings being changed. In these cases, an alert to the administrator is appropriate as that person has the ability to act on the alert.

Guideline 9 on making systems resilient to outages: The aim of this guideline is to ensure that IoT services are kept up and running as the adoption of IoT devices across all aspects of a consumer's life increases, including in functions that are relevant to personal safety. The impact on people's lives could be prevalent if, for example, an internet connection is lost to a connected door and someone is locked outside. Another example is a home heating system that turns off because of a DDoS attack against a cloud service. It is important to note that other safety-related regulations may apply, but the key is to avoid making outages the cause of these problems and to design products and services ready for these challenges.

[9] Guidance is available, for example, by the NCSC at https://www.ncsc.gov.uk/guidance/tls-external-facing-services