Australian Government

Code of Practice

Securing the Internet of Things for Consumers

Contact us
Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

P - 20-02351

Introduction

The Internet of Things (IoT), which includes everyday smart devices that connect to the internet – such as smart TVs and home assistants – provides significant benefits to Australians; enhancing our convenience, comfort and efficiency. Many of these devices are developed with functionality as a priority, and security features are often absent or an afterthought. By 2030, it is estimated that there will be more than 21 billion IoT devices connected to the internet globally, with the highest estimations predicting over 64 billion devices. It is essential that these devices in our homes and businesses have cyber security provisions that defend against potential threats and malicious cyber activity.

The *Code of Practice: Securing the Internet of Things for Consumers* (Code of Practice) represents a first step in the Australian Government's approach to improve the security of IoT devices in Australia. This Code of Practice is a voluntary set of measures the Australian Government recommends for industry as the minimum standard for IoT devices. The Code of Practice will also help raise awareness of security safeguards associated with IoT devices, build greater consumer confidence in IoT technology and allow Australia to reap the benefits of greater IoT adoption.

The Code of Practice was developed by the Department of Home Affairs, in partnership with the Australian Signals Directorate's Australian Cyber Security Centre, and follows nation-wide engagement with industry and the Australian public. The Code of Practice was recognised as a necessary step to lifting the cyber security of internet-connected devices domestically.

The Code of Practice is designed for an industry audience and comprises 13 principles. The Australian Government recommends industry prioritise the top three principles because action on default passwords, vulnerability disclosure and security updates will bring the largest security benefits in the short term.

In acknowledgement of the global nature of this issue, the Code of Practice aligns with and builds upon guidance provided by the United Kingdom and is consistent with other international standards. The principles will help inform domestic and international manufacturers about the security features expected of devices available in Australia.

Ensuring the security and integrity of IoT devices will enhance the way we live and work. By improving the overall cyber security of these devices, we also deter the risks they pose to Australian families, our economy and national security.

This Code of Practice will be reviewed on a regular basis to ensure it remains fit for purpose.

Application

This Code of Practice constitutes a voluntary set of principles, and compliance with these principles is encouraged but optional. Any entity choosing to comply with the Code of Practice may do so in accordance with all or some of the principles contained in the Code of Practice. Where the Code of Practice has been partially complied with, the entity should state the specific principle that is in compliance. For example, by stating, "Our organisation has complied with principles 1, 2 and 3 of the Code of Practice: Securing the Internet of Things for Consumers".

Principles

Principle	Description
1. No duplicated default or weak passwords	IoT device (and associated backend/cloud account) passwords should be unique, unpredictable, complex and unfeasible to guess, and not resettable to any factory default value that is common to multiple devices. Associated web services should use Multi-Factor Authentication, not provide any unnecessary user information prior to authentication, and any password reset process should appropriately authenticate the user. *Primarily applies to Device Manufacturers.*
2. Implement a vulnerability disclosure policy	IoT device manufacturers, IoT service providers and mobile application developers should provide a public point of contact as part of a vulnerability disclosure policy in order for security researchers and others to report issues. Disclosed vulnerabilities should be acted on in a timely manner. Implementing a bug bounty program encourages and rewards the cyber security community for identifying and reporting vulnerabilities, thereby facilitating the responsible and coordinated disclosure and remediation of vulnerabilities. *Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.*

Principle	Description
3. Keep software securely updated	Software (including firmware) on IoT devices, including third party and open source software, as well as associated web services, should be securely updateable. Updates should be timely and not impact the device's functionality. Updates should also not change user-configured preferences, security or privacy settings without prior approval from the user. The need for each update should be made clear to consumers, and updates should be easy to implement and applied automatically by default. The device should verify that updates are from a trusted source e.g. via use of a trusted digital signature. Updates should be distributed via secure IT infrastructure to mitigate the trusted source being compromised. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable. Where possible, vendors should inform the user when their constrained device is no longer fit for purpose. An end-of-life policy should be clear to the consumer including when they acquire the device, which explicitly states the minimum length of time for which a device will receive software updates, the reasons for this timeframe and a commitment and method to warn consumers when the product will no longer receive updates. If a user interface is available it should clearly display when a device has reached its end-of-life, inform the user of the risk of security updates no longer being available and provide suggestions for mitigating this risk. *Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.*
4. Securely store credentials	Any credentials should be stored securely within devices and on services. Hard-coded credentials (e.g. usernames and passwords) should not be embedded in device software or hardware since they can be discovered via reverse engineering. *Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.*

Principle	Description
5. Ensure that personal data is protected	Where devices and/or services process personal data, they must do so in accordance with data protection law e.g. the *Privacy Act 1988* and Australian Privacy Principles. Personal data should only be collected if necessary for the operation of the device, and privacy settings on a device should be set to privacy protective by default. Adequate industry-standard encryption, as articulated in the *Australian Government Information Security Manual*, should be applied to personal data in transit and data at rest. Consumers should be provided with clear and transparent information about what data is being used and how, 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 should be validly and lawfully obtained from an adult, with those consumers being given the opportunity to withdraw it at any time. Several other principles in this document are related to protecting personal data, such as installing and securely configuring devices, as well as deleting personal data. *Primarily applies to Device Manufacturers, IoT Service Providers, Mobile Application Developers and Retailers.*
6. Minimise exposed attack surfaces	Devices and services should operate on the 'principle of least privilege'. Unused functionality should be disabled; hardware should not unnecessarily expose access (e.g. unrequired ports should be closed, the web management interface should only be accessible to the local network unless the device needs to be managed remotely via the Internet); functionality should not be available if they are not used; and code should be minimised to the functionality necessary for devices and services to operate. Software should run with appropriate privileges, taking account of both security and functionality. To further reduce the number of vulnerabilities, use a secure software development process and perform penetration testing. *Primarily applies to Device Manufacturers and IoT Service Providers.*
7. Ensure communication security	Data requiring confidentiality or integrity protection, or associated with remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All credentials and certificates should be managed securely. All remote access should be logged, with logs including the date, time and source of access at a minimum. *Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.*

Principle	Description
8. Ensure software integrity	Software (including firmware) 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. *Primarily applies to Device Manufacturers.*
9. Make systems resilient to outages	Resilience should be built into 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 devices should remain operating and locally functional in the case of a loss of network, without compromising security or safety. They 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 all attempt to reconnect at the same time. Implementing redundancy and DDoS mitigation helps ensure that IoT services remain online. Architect IoT devices to continue functioning as much as possible if an associated IoT service becomes unavailable, and disclose upfront to the consumer which features will cease working in this case. IoT service providers should also update data when network connection is restored. *Primarily applies to Device Manufacturers and 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. *Primarily applies to Device Manufacturers and 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 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, including how to reset the device to "factory default" and delete data stored on the device and in associated backend/cloud accounts and mobile applications. *Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.*

Principle	Description
12. Make installation and maintenance of devices easy	Installation and maintenance of IoT devices should employ minimal steps and follow Australian Government best practice on security[1] and usability.[2] Consumers should also be provided with clear and straightforward guidance on how to securely set up their device and maintain it through its lifecycle. Accessibility options on a device should be enabled by default. *Primarily applies to Device Manufacturers, IoT Services Providers and Mobile Application Developers.*
13. Validate input data	Data received via user interfaces, application programming interfaces (APIs) and network interfaces should be validated. Ensure data input is authorised and conforms to expectations. *Primarily applies to Device Manufacturers, IoT Service Providers and Mobile Application Developers.*

[1] Australian Signals Directorate's '*How to implement the Code of Practice: Securing the Internet of Things for Consumers*'.

[2] Digital Transformation Agency's *'Accessibility and Inclusivity Guide'*.

Definitions

Consumer IoT: Consumers may take many forms. Governments, businesses and individuals may all be consumers of IoT devices. This Code of Practice particularly focuses on consumer grade, internet-connected devices and associated applications (e.g. wearable devices, and home appliances such as “smart” televisions and refrigerators). This group of devices does not include mobile phones – as they are considered sophisticated devices and other guidance may more accurately apply.

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