SmartSuite

Framework / Cybersecurity / Other

Code of Practice: Securing the Internet of Things for Consumers (2020)

Australia's IoT Code of Practice is a voluntary set of 13 principles for consumer internet-connected devices, now alongside mandatory smart device standards that began on 4 March 2026.



What it is

The Code of Practice: Securing the Internet of Things for Consumers (2020) is a voluntary set of 13 principles that the Australian Government recommends as the minimum standard for consumer IoT devices. The Department of Home Affairs developed it with the Australian Signals Directorate's Australian Cyber Security Centre. It is designed for an industry audience: device manufacturers, IoT service providers, mobile application developers, and retailers.

Compliance is encouraged but optional, and an entity may comply with all or some of the principles, stating which ones it meets, for example principles 1, 2, and 3. The government recommends prioritizing the top three principles: no duplicated default or weak passwords, a vulnerability disclosure policy, and securely updated software.

At a glance

PUBLISHER Australian Government Department of Home Affairs, with the Australian Signals Directorate's Australian Cyber Security Centre	TYPE Framework	VERSION Code of Practice: Securing the Internet of Things for Consumers (2020)
EFFECTIVE 2020	DOMAIN Cybersecurity	FAMILY Other
REGION Australia	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

Why it matters

- **Prioritized principles** The government names the top three, default passwords, vulnerability disclosure, and security updates, as the actions with the largest short-term security benefit.
- **Role-specific guidance** Each principle states whether it applies primarily to device manufacturers, IoT service providers, mobile application developers, or retailers.
- **Flexible adoption** An entity may comply with all or some principles and should state which principles it has met.
- **Whole-lifecycle coverage** The principles run from credentials and updates through end-of-life policy to deleting personal data when a device changes hands or is disposed of.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Australia IoT Code

Principle control library

Record each of the 13 principles as a control, with the roles it applies to, an owner, and the product lines in scope.

Vulnerability and update tracking

Track vulnerability reports, remediation, and update releases, including each product's published support end date.

Password and credential checks

Plan tests for unique default passwords, hard-coded credentials, and multi-factor authentication on associated services.

Personal data handling

Link privacy settings, consent, and data deletion procedures to the devices and services that process personal data, using Privacy Management.

Supplier and service provider oversight

Assess the IoT service providers, app developers, and component suppliers behind each product using Third Party Risk Management.

Compliance statements and reporting

Keep the statement of which principles are met, plus statements of compliance for the 2025 Rules, with Enterprise Reporting for status.

Common framework mappings

CIS Controls v8.1 | ETSI EN 303 645 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0

Official resources

IoT Code of Practice – Guidance for Manufacturers

Outlines practical implementation guidance for the 13 principles in Australia's voluntary IoT security Code.

cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20IoT%20Code%20of%20Practice%20%E2%80%93%20Guidance%20for%20Manufacturers%20(October%202021).pdf

Voluntary Code of Practice: Securing the Internet of Things for Consumers

Defines the thirteen foundational cybersecurity principles for consumer IoT devices in Australia.

homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

Frequently asked questions

Is the Australia IoT Code of Practice mandatory?

No. The Code is a voluntary set of principles, and compliance is encouraged but optional. An entity may comply with all or some of the principles and should state which ones. Separate mandatory smart device standards under the Cyber Security Act 2024 began on 4 March 2026.

What are the 13 principles of the IoT Code of Practice?

No duplicated default or weak passwords, implement a vulnerability disclosure policy, keep software securely updated, securely store credentials, ensure personal data is protected, minimize exposed attack surfaces, ensure communication security, ensure software integrity, make systems resilient to outages, monitor system telemetry data, make it easy for consumers to delete personal data, make installation and maintenance easy, and validate input data.

Which principles should be prioritized?

The Australian Government recommends prioritizing the top three: no duplicated default or weak passwords, a vulnerability disclosure policy, and keeping software securely updated. It says action on these will bring the largest security benefits in the short term.

 Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What do the mandatory smart device rules require?

The Cyber Security (Security Standards for Smart Devices) Rules 2025 apply to most smart devices for personal, domestic, or household use manufactured on or after 4 March 2026. They require no universal default passwords, a published means to report security issues, and published information on how long the device will receive security updates, plus statements of compliance.

Who does the Code apply to?

It is designed for device manufacturers, IoT service providers, mobile application developers, and retailers of consumer-grade internet-connected devices and associated applications. Each principle names the roles it applies to primarily. Mobile phones are not its focus.

License included / downloadable: Yes The Department of Home Affairs publishes the Code of Practice under a Creative Commons Attribution 4.0 International license, except for the Commonwealth Coat of Arms. The text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/australia-iot-code-of-practice