

Australia Voluntary Code of Practice for Securing the Internet of Things v1.0 (2020)

Australia IoT Code of Practice is a voluntary framework providing guidance to secure consumer IoT devices and protect end-user data.

What it is

Australia IoT Code of Practice is a voluntary cybersecurity framework that helps organizations strengthen the security and privacy of consumer Internet of Things (IoT) devices and related services. Its primary purpose is to provide practical guidance on protecting connected devices against cyber threats and safeguarding end-user data.

Published by the Australian Government, the Code is targeted at manufacturers, service providers, and developers involved in designing, developing, or supplying IoT devices for the Australian market. It addresses key areas such as secure device configuration, vulnerability management, data protection, access controls, and privacy governance, aligning its principles with international security standards.

At a glance

PUBLISHER

Office of the Australian Information Commissioner (OAIC)

TYPE

Framework

VERSION

Voluntary Code of Practice for Securing the Internet of Things

EFFECTIVE
2019

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Australia

ADOPTION MODEL
Security Baseline

IMPLEMENTATION COMPLEXITY
Moderate

Source: <https://www.oaic.gov.au/privacy/australian-privacy-principles>

Why it matters

- **Strengthen risk management for IoT** Support identification and mitigation of unique cyber risks associated with connected devices and service ecosystems.
- **Enhance compliance with privacy standards** Enable alignment with privacy laws and regulations through practical data protection and governance measures.
- **Improve incident response readiness** Facilitate faster detection, reporting, and mitigation of IoT-specific security incidents, reducing potential impact on users and systems.
- **Promote secure product development** Encourage the integration of security principles throughout product design and supply chain processes for safer device offerings.



Australian Government
Australian Signals Directorate

How SmartSuite supports Australia IoT Code

IoT Security Principles Framework

Structure the 13 IoT security principles with ownership and implementation tracking.

Secure Design and Development Governance

Track secure development practices, default configurations, and vulnerability disclosure processes.

Device Identity and Access Management

Manage authentication, credential handling, and secure access controls for IoT devices.

Firmware and Device Lifecycle Maintenance

Track firmware updates, vulnerability remediation, and device lifecycle maintenance.

IoT Data Collection and Transmission Safeguards

Manage data collection, storage, and transmission safeguards for IoT environments.

IoT Device Security Posture and Readiness Reporting

Provide dashboards showing control adoption, device risk posture, and security readiness.

Common framework mappings

- CIS Controls v8.1
- 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](https://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

What is the Australia IoT Code of Practice used for?

The Australia IoT Code of Practice provides guidance to organizations on securing consumer Internet of Things (IoT) devices and services to protect against cyber threats and enhance data privacy. It establishes best-practice principles for risk management, secure device configuration, vulnerability handling, and privacy protection throughout the IoT device lifecycle.

Is compliance with the Australia IoT Code of Practice mandatory?

Compliance with the Australia IoT Code of Practice is voluntary and not legally mandated. However, adopting the Code can support organizations in meeting broader regulatory expectations, addressing emerging threats, and aligning with international IoT security standards.

Who does the Australia IoT Code of Practice apply to?

The Code is intended for manufacturers, developers, and service providers involved in the design, development, supply, or operation of consumer IoT devices sold in the Australian market. It encompasses a broad range of connected products, including smart home devices, wearables, and connected appliances.

What key concepts and requirements are outlined in the Australia IoT Code of Practice?

Key requirements include secure-by-design principles, strong default settings, vulnerability disclosure processes, secure patching, data protection, and user privacy governance. The Code encourages organizations to develop baseline security controls, implement supply chain risk mitigation, and document incident response protocols.

How is the Australia IoT Code of Practice implemented in practice?

Organizations integrate the Code's principles into product development processes, conducting risk assessments for each IoT device, and embedding security requirements into vendor management and procurement. It also involves ongoing monitoring, vulnerability management, and periodic review of security controls across the device lifecycle.

How does the Australia IoT Code of Practice relate to other frameworks or standards?

The Code aligns with international IoT security and privacy standards, such as ETSI EN 303 645, and complements regulatory requirements like the Australian Privacy Principles. It offers outcomes-based guidance that can be mapped to internal controls and global best practices for broader compliance programs.

What are the ongoing compliance requirements for the Australia IoT Code of Practice?

Ongoing compliance involves regularly reviewing and updating security controls, maintaining vulnerability and risk registers, establishing incident response plans, and ensuring that supply chain and vendor processes remain aligned with the Code. Evidence of continuous improvement and monitoring is also expected.

How would SmartSuite support Australia IoT Code of Practice?

SmartSuite can help organizations operationalize the Australia IoT Code of Practice by providing tools for importing mapped control libraries, tracking device risks, and managing control implementation. It enables evidence collection, compliance status monitoring, and remediation workflows, as well as supporting audit readiness and reporting through dashboards and integrations.

License included / downloadable: Yes The IoT Code of Practice is published by the Australian Government and is publicly available through official government cybersecurity resources.

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