FACTSHEET

Security standards for smart devices

The *Cyber Security Act 2024* (the Act) established the power to prescribe security standards for smart devices, otherwise known as Internet of Things (IoT) devices, under ministerial rules.

The Act, and any rules made under these provisions, place obligations on entities to ensure that the products they manufacture or supply to the Australian market meet requirements in the specified security standards relevant to that product.

Cyber Security (Security Standards for Smart Devices) Rules 2025

The Cyber Security (Security Standards for Smart Devices) Rules 2025 (the Rules) are the first set of rules under the secure technology framework and mandate standards to uplift the cyber security of most types of **consumer grade smart devices**, which aligns with existing international approaches.

Under Schedule 1, the Rules mandate:

- **No universal default passwords** – passwords must be unique per product or defined by the user of the product for a smart device's hardware or pre-installed software used in any state other than factory default, and where software is required to be installed for the product's intended usage.
- **Manufacturers publish a means to report security issues** – allowing security issues to be reported to the manufacturer, with status updates on the resolution of these issues.
- **Manufacturers publish information about how long the device will be supported for** – providing transparency to consumers about the period, including an end date, that the product will receive security updates.

The security standards closely follow the first three principles of the ETSI EN 303 645 standard and the United Kingdom's Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (UK), under the Product Security and Telecommunications Infrastructure Act 2022 (UK).

Scope of the security standards for consumer grade smart devices

The security standards cover products that consumers use every day, such as smart TVs, smart watches, home assistants, baby monitors, and consumer energy resources.

The standards apply to any smart device that:

- Meets the definition of a **relevant connectable product** (as defined in the Act);
- Will be acquired, or could reasonably be expected to be acquired, in Australia by a **consumer**, as defined in section 3 of the Australian Consumer Law; and
- Is intended by the manufacturer to be used, or likely to be used, for personal, domestic or household use or consumption.

The security standards apply to all in-scope products manufactured **on and from 4 March 2026**.

There are some specific exemptions that apply to the standards. The following types of products are excluded under section 8 of the Rules:

- A desktop computer or a laptop;
- A tablet computer;
- A smartphone;
- Therapeutic goods within the meaning of the *Therapeutic Goods Act 1989*;
- A road vehicle within the meaning of the *Road Vehicle Standards Act 2018*; and
- A road vehicle component within the meaning of the *Road Vehicle Standards Act 2018*.

Requirements for statements of compliance

Under the Act, manufacturers and suppliers have obligations to provide **statements of compliance** with the security standard:

- Manufacturers must provide statements of compliance for supply of in-scope products, where the manufacturer is aware, or could reasonably be expected to be aware, that the product will be acquired by a consumer in Australia.
- Suppliers must supply in-scope products with a statement of compliance, where the supplier is aware, or could reasonably be expected to be aware, that the product will be acquired by a consumer in Australia.

Division 3 of Part 2 of the Rules specifies the **requirements for statements of compliance** for in-scope products. An example statement of compliance template is available on the Department of Home Affairs website.

While not a requirement under the Act or the Rules, manufacturers may wish to publish the statement on their website to provide transparency to consumers and to make it easier to pass information onto suppliers.

Manufacturers and suppliers must **retain the statement of compliance for five years**.

Enforcement and regulation

The enforcement framework established in the Act is designed to encourage engagement with manufacturers and suppliers of smart devices and uplift industry best practice. The Act allows the Secretary of the Department of Home Affairs to undertake enforcement action to ensure entities comply with their obligations under the Act. This action includes issuing compliance notices, stop notices and recall notices. The Secretary may engage experts to examine a product or statement of compliance. The Secretary may also request a statement of compliance from the manufacturer or supplier to ensure the entity has met their obligations under the Act and the Rules.

If an entity fails to comply with a recall notice, the identity of the entity, the details of the product and non-compliance, and the risks posed by the product may be published on the website of the Department of Home Affairs.

Regulatory support will be provided from within the Department of Home Affairs to assist the Secretary in monitoring compliance with the Rules and the Act. The below flow chart illustrates how the regulatory and enforcement framework may function.