CONSUMER IOT AND CONNECTED PRODUCTS

A MANUFACTURERS CHECKLIST FOR SMART DEVICE SECURITY

bsi.

As UK government announce their intention to move forward with the proposal for regulation on consumer IoT products, what do manufacturers need to do to ensure their products meet the cybersecurity laws?

The Government's Code of Practice for Consumer IoT Security outlines 13 principles to ensure that products are secure by design. Principles 1 to 3 will form part of the new legislation. This guide looks at them all.

CONSUMER IOT SECURITY SPECIFICATION

1

NO DEFAULT PASSWORDS

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

2

IMPLEMENT A VULNERABILITY DISCLOSURE POLICY

All companies that provide internet-connected devices/ services **shall provide a public point of contact** where potential vulnerabilities are disclosed. These vulnerabilities should be acted on in a timely manner.

3

KEEP SOFTWARE UPDATED

IoT software components should be **securely and easily updatable** without impacting the device's function. These updates should be timely, **based on an end-of-life policy** that explicitly states a minimum length of time for which the device will receive updates, and the reasons why. Updates should be made clear to consumers, and any devices that cannot physically be updated should be **isolatable and replaceable**.

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**.

5

COMMUNICATE SECURELY

All **security-sensitive data** should be **encrypted in transit**, appropriate to the properties of the technologies and usage. All keys should be managed securely.

bsi.

6 MINIMIZE EXPOSED ATTACK SURFACES

All devices and services should operate on the '**principle of least privilege**'; unused ports should be closed, hardware not available when not used and code minimized to the necessary functionality.

7 ENSURE SOFTWARE INTEGRITY

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

8 ENSURE THAT PERSONAL DATA IS PROTECTED

Where devices and services process personal data they shall do so in accordance with applicable data protection law, such as **GDPR**. Manufacturers and service providers should **provide transparent information** about **how customers data will be used**, applying also to any third parties that may be involved. Customers' consent must be **validly and lawfully obtained**.

9 MAKE SYSTEMS RESILIENT TO OUTAGES

Resilience should be built into IoT devices and services, taking into account the **possibility of outages to data networks or power**. As far as reasonably possible, devices should be able to **return to network in a sensible state** and an orderly fashion.

10 MONITOR SYSTEM TELEMETRY

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

11 MAKE IT EASY FOR CONSUMERS TO DELETE PERSONAL DATA

Devices and services should be configured so that **personal data can easily be removed** from them for a transfer of ownership, when the customer wishes to delete it or when they are disposing of it. Customers should be **given clear instructions** as to how to do this.

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**. Customers should be given guidance on securely setting up their device.

13 VALIDATE INPUT DATA

Data input via **user interfaces** and **transferred via APIs** or **between networks** in services and devices **should be validated**.


bsi.
The consumer IoT and connected devices market is at a precipice of change. Manufacturers have guidance, and what will soon be regulation to ensure they deliver products that are safe and secure.
To find out how BSI can help build trust in your consumer IoT and connected products - whether 'on market' or at design stage - through foundation testing to Kitemark, visit bsigroup.com/Internet-of-Things