UK PSTI Compliance Service

Applus+ Laboratories, a global leader in cybersecurity evaluations, is excited to announce a new service designed specifically for manufacturers and distributors seeking compliance with Schedule 1 of the UK Product Security and Telecommunications Infrastructure (UK-PSTI) regulation.

UK PSTI, a new UK regulation for connected products

While the UK's New Cybersecurity Regulation for Connected Consumer Devices relies on vendor self-compliance, **obtaining a third-party certificate remains a prudent choice.** Applus+ Laboratories provides various options for vendors seeking independent proof of compliance.

What is UK PSTI (Product Security and Telecommunications Infrastructure)?

The UK Product Security and Telecommunications Infrastructure (PSTI) Product Security Regime is a legal framework aimed at mandating security requirements for ioT products sold in the United Kingdom (UK).

The PSTI legal framework is made of two parts which are summarised here:

On 29 April 2024, Product Security and Telecommunications Infrastructure Act Regulations **came into force into immediate effect** and there is no provision in the regime that excludes products that are already placed on the UK market.

What products are affected by UK PSTI and which requirements are in scope?

The UK PSTI regime casts a wide net, covering an extensive array of products. From smart thermostats to fitness trackers, everyday devices are now integral to the security conversation. For some IT companies, this level of cybersecurity is old hat—they've long surpassed it. But for others, it's uncharted territory, necessitating a thorough assessment of their current practices and identifying necessary changes to ensure compliance.

Manufacturers shall implement the minimum-security measures defined in Schedule 1 and the regulation relies on self-assessment approach. They are related to three main items:

Passwords

Manufacturers must ensure that passwords for products have minimum security such as unique per device or set by the user, avoiding guessable patterns and publicly available information.

Information on how to report security issues

Manufacturers must provide clear contact points for users to report security concerns, with assurances of acknowledgment and status updates, accessible without personal data requirements.

Information on minimum security update periods

Manufacturers must publish defined support periods for security updates, ensuring accessibility and transparency, without prior request, in understandable language, and without personal information requests.

Self-compliance and third-party certification for UK PSTI

Under this new regulation, there are no mandatory certification bodies actively verifying compliance. The responsibility now squarely rests on the vendors' shoulders. However, obtaining a proof of compliance issued by a third-party remains a prudent choice. Independent validation by third-party experts adds credibility.

For manufacturers without in-house cybersecurity teams, third-party certification simplifies the process. Smaller companies can navigate complexity more effectively.

Moreover, displaying a certificate signals commitment to security, instilling consumer confidence. When consumers see that independent assessments have validated a product, trust is bolstered.

As other countries follow suit with similar regulations, this proactive approach becomes essential for vendors selling products in the global market.

Applus+ Laboratories service solutions for UK PSTI compliance

Applus+ Laboratories have offer a number of service solutions for UK PSTI compliance:

PSTI-Focused Certificate

Applus+ Laboratories will review and analyse the provided documentation and issue a report that will bring the confidence to the manufacturer to claim a self-compliance to the regulation. Optionally, Applus+ Laboratories can also provide a Certificate of Compliance (CoC), which will strengthen the confidence of the client in case they need to prove to a third party the compliance of this regulation. This will allow clients to demonstrate compliance but also to identify potential gaps, assisting them on their path to meet UK-PSTI security requirements. Our impartial analysis, conducted by top experts in current cybersecurity regulations, ensures thorough and accurate assessment.

Our specialised service provides a **comprehensive assessment** of the security requirements outlined in Schedule 1 of the UK-PSTI regulation. This assessment ensures that manufacturers can confidently use the results as evidence to demonstrate compliance with the security requirements set forth in the UK-PSTI regulation. With Applus+ Laboratories, manufacturers and distributors can assess their key regulatory areas efficiently and effectively by an experienced third party entity, which will lead to know their status and possible gaps ahead of schedule.

Full ETSI EN 303 645 Evaluation

For those aiming higher, evaluating against the entire ETSI EN 303 645 standard is an option. Note that if your product is already compliant with ETSI 303 645, it is deemed to be compliant to UK-PSTI cybersecurity regulations. Applus+ Laboratories holds accreditation of ISO/IEC 17025 with ETSI 303 645 as Evaluation Laboratory.

PSA Certified Level 1 Scheme

PSA Certified is an industry-led certification scheme for IoT cybersecurity. Level 1 mark aligns with major global guidelines for connected consumer devices security, mapping requirements from various standards, including ETSI EN 303 645, NIST 8259A, PSTI, California State Law SB-327, Matter and ioXt.

Contact Us to Ensure Compliance to already in force PSTI regulation!

Trust Applus+ Laboratories to guide you through the UK-PSTI cybersecurity landscape, providing the expertise needed to help you meet your compliance goals seamlessly.

Contact us today to safeguard your consumer devices and build trust in the connected world or request a quote!