

Device password checklist: UK PSTI, EU and US rules

One password design that meets the UK PSTI rules, ETSI EN 303 645 provision 5.1-1, the EN 18031 restriction on optional passwords, and the California and Oregon connected device laws.

- ☐ No universal default password shared by every unit, on any interface.
- ☐ Either a password unique to each device, or the user must set one before first use.
- ☐ Unique passwords not based on incremental counters, public information or an easy derivation of an identifier such as the serial number or MAC address.
- ☐ No option to skip setting a password at setup.
- ☐ No hard-coded credentials or backdoor accounts in the firmware, including the chip vendor's SDK.
- ☐ No account without a password, including root, telnet and the serial console.
- ☐ Passwords stored with a strong salted hash, never in clear text in configuration files.
- ☐ The same rule applied to every way in: the web interface, the app, telnet, SSH, the serial console and video protocols.

Sources

- GOV.UK, The UK PSTI (Product Security) regime: <https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime>
- Commission Implementing Decision (EU) 2025/138 citing EN 18031: https://eur-lex.europa.eu/eli/dec_impl/2025/138/oj/eng
- Oregon Revised Statutes 646A.813: https://oregon.public.law/statutes/ors_646A.813

A guide to where the evidence is, not legal advice or certification. Your lab, notified body or regulator makes the final call.
magdox.io/blog/uk-psti-for-device-makers/