TP-Link Systems strengthens public telecommunications security in alignment with the Telecommunications (Security) Act 2021.

July 2026

TP-Link Systems Inc. affirms its commitment to strengthening the security and resilience of telecommunications networks within the UK telecoms sector through the implementation of the Telecommunications (Security) Act 2021 (TSA) security framework. TP-Link follows all three core components of TSA by aligning with its overarching security duties, required security measures, and supporting technical guidance.

As part of this commitment, TP-Link is certified under **ISO/IEC 27001:2022** (ISO/IEC 27001:2022), the internationally recognized standard for Information Security Management Systems (ISMS) and has adopted a **Secure Product Development Lifecycle (SPDL)** to embed security throughout product design, development, and maintenance.

1. ISO/IEC 27001:2022 Certification

TP-Link's ISMS is certified under ISO/IEC 27001:2022, which requires:

- Policies on risk analysis and information system security
- Incident and vulnerability management
- Supply Chain security controls
- Secure Product Development Lifecycle
- Continuous monitoring and improvement of mechanisms

With official guidance from the UK Department for Science, Innovation, & Technology (Telecommunications Security Code of Practice version 1.1) TP-Link ensures that its product development practices meet established security and regulatory standards, enabling the creation of resilient and high-quality networking products.

TP-Link Systems Inc.'s commentary on Section 3: Technical Guidance Measures (M1.01-M21.07) may be provided upon request, pending appropriate authorization and legal department approval.

2. Mapping to TSA Principles

Specific Feature	Mapped TSA Principle	Security Rationale
V-LAN based Network Isolation	Network Architecture, Protection of data and network function, Prevention of unauthorized access or interference	Prevents unauthorized lateral movement and protects critical functions by limiting the spread of compromise.
Guest network separation	Network Architecture, Prevention of unauthorized access or interference	Separating guest traffic from production network reduces risk from untrusted devices and prevents interference with core network functions.

Controller (admin) access control	Prevention of unauthorized Access or Interference, Monitoring and analysis	Strong administrative access controls ensure only authorized personnel can modify critical settings, reducing risk of misuse or malicious changes
2-Factor Authentication & Security Assertion Markup Language (SAML) Single Sign On (SSO)	Prevention of unauthorized Access or Interference, Governance	Multi-factor authentication lowers the risk of unauthorized access by ensuring only verified users can reach sensitive tools.
Role Based Access Control (RBAC) with custom role support	Prevention of unauthorized access of interference, Governance, Reviews	RBAC limit sensitive operations to those who need them and support access review requirements.
Internet Protocol (IP) Access Rules/ Allowlist	Network Architecture, Prevention of unauthorized Access or Interference	Restricting access to trusted IPs reduces attack surfaces and prevents exposure to sensitive services.
Time-based Access Control	Prevention of unauthorized Access or Interference, Governance	Time-limited access reduced standing privilege and opportunity for unauthorized attempts.
Client Access Control	Protection of Data and Network, Functions Prevention of unauthorized Access or Interference	Ensuring only authorized devices connect reduces compromise risk from unmanaged endpoints.
Lightweight Directory Access Protocol (LDAP) Integration	Prevention of unauthorized Access or Interference, Governance, Reviews	Central identity management enforces consistent authentication and improves auditability.
Wi-Fi Protected Access 3 (WPA3) Enhanced Security	Protection of Data and Network, Prevention of unauthorized access or interference	WPA3 ensures stronger cryptographic protection for wireless communication.
Remote Authentication Dail-In User Service (RADIUS) Integration	Protection of Data and Network, Prevention of Unauthorized Access or Interference	RADIUS centralizes authentication and logging, improving traceability and access control.
Media Access Control (MAC) Address Filtering	Prevention of unauthorized Access or Interference	Limiting network access to recognized devices reduces the change of unauthorized connection attempts.
Intrusion Detection and Prevention (IDS/IPS)	Monitoring and Analysis, Remediation and Recovery	IDS/IPS detects and blocks threats in real time, supporting early detection and containment.
Distributed Denial of Service (DDoS) Protection	Protection of Data and Network Functions, Monitoring and Analysis, Remediation and Recovery	DDoS protection maintains service availability by detecting and mitigating network-level attacks.
Firewall Rules & Policies	Network Architecture Prevention of unauthorized Access or Interference	Firewalls enforce secure boundaries and prevent untrusted traffic from entering sensitive areas.
Virtual Private Network (VPN) Connectivity	Protection of Data and Network, Prevention of unauthorized access or interference	VPNs encrypt and secure mote access, reducing risks from external connections.
Real-Time Network Traffic Analysis	Monitoring and Analysis	Real-time monitoring identifies anomalies quickly, supporting early detection and response.
Device Connectivity Monitoring	Monitoring and Analysis, Governance	Monitoring devices help detect unauthorized connections and suspicious behavior.
Bandwidth Utilization Tracking	Monitoring and Analysis	Tracking bandwidth use helps detect abnormal spikes indicating attacks or data exfiltration
Event Logging and Audit Logs	Monitoring and Analysis, Governance, Review	Logging provides visibility for investigations, oversight, and regulatory compliance.
Backup and Disaster Recovery	Remediation and Recovery, Governance	Backups and DR processes ensure service continuity and minimize downtime after incidents.