TP-Link Statement – EU NIS2 Directive

September 2025

TP-Link Systems Inc. affirms its commitment to cybersecurity and regulatory compliance through the implementation of industry standard governance, risk management, and technical controls. 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)**

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

Based on official guidance from ENISA(NIS2 Technical Implementation Guidance | ENISA), this certification demonstrates TP-Link's alignment with the **security measures** outlined in **Article 21 of the NIS2 Directive**.

2. Mapping to NIS2 Directive Article 21

Specific Feature	Mapped NIS2 Article 21 Clause
VLAN-based Network Isolation	(g)basic cyber hygiene practices and cybersecurity training (i)Human resources security, access control policies, and asset management
Guest Network Separation	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
Controller Access Control	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
2-Factor Authentication & SAML SSO	(j)The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate
RBAC with custom role support	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
IP Access Rules	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
Time-based access controls	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management

Client Access Control	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
LDAP integration	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
WPA3 Enhanced Security	Policies and procedures regarding the use of cryptography and, where appropriate, encryption
RADIUS integration	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
MAC address filtering	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
Time-based access controls	(g) basic cyber hygiene practices and cybersecurity training (i) Human resources security, access control policies, and asset management
Intrusion Detection and Prevention (IDS/IPS)	(a) policies on risk analysis and information system security; (b) Incident handling
DDoS protection	(a) policies on risk analysis and information system security; (b) Incident handling
Firewall rules and policies	(a) policies on risk analysis and information system security; (b) Incident handling
VPN connectivity	(a) policies on risk analysis and information system security; (b) Incident handling
Real-time network traffic analysis	(a) policies on risk analysis and information system security; (b) Incident handling
Device connectivity monitoring	(a) policies on risk analysis and information system security; (b) Incident handling
Bandwidth utilization tracking	(a) policies on risk analysis and information system security; (b) Incident handling
Event Logging & Audit Log	(a) policies on risk analysis and information system security; (b) Incident handling (c) business continuity, such as backup management and disaster recovery, and crisis management;