EU NIS2 Directive Compliance Declaration

Date: May 18, 2026

D-Link Corporation (hereinafter referred to as “D-Link”) affirms its unwavering commitment to robust cybersecurity, meticulous data privacy, and stringent regulatory compliance through the implementation of industry-leading corporate governance, threat risk management, and technical security controls.

1. Information Security Certifications and Governance Framework

To provide verifiable security assurance, D-Link’s core corporate infrastructure and product research environments are fully certified under three globally recognized international standards:

- **ISO/IEC 27001:2022** –Information Security Management Systems (ISMS)
- **IEC 62443-4-1:2018** – Secure Product Development Lifecycle Requirements (SPDL)
- **BS 10012:2017** – Personal Information Management System (PIMS), fully aligned with EU General Data Protection Regulation (GDPR) requirements

Furthermore, through a long-term strategic partnership with the global data privacy authority **TrustArc Inc.**, D-Link’s external service platforms and domains have successfully achieved the **TRUSTe Privacy Certification Label**.

By synthesizing these frameworks into a unified “Plan-Do-Check-Act" (PDCA) operational model, D-Link establishes an institutional defense posture that comprehensively satisfies and exceeds the mandatory risk-management obligations outlined in **Article 21 of the European Union NIS2 Directive**.

2. Mapping to NIS2 Directive Article 21

The following compliance matrix details the specific technical features, policies, and governance structures implemented by D-Link to satisfy each mandatory clause under NIS2 Article 21:

NIS2 Article 21 Core Clauses	D-Link Implementation Measures & Technical Features
(a) policies on risk analysis and information system security	• ISO/IEC 27001 Framework: Implemented Board-approved "Information Security Management Policy" with mandatory annual risk analysis checking asset confidentiality, integrity, and availability.
(b) incident handling	• Enforced “Information Security Incident Reporting and Handling Procedure.” • Real-world executed server isolation, threat containment, and expert-led remediation.
(c) business continuity, such as backup management and disaster	• Comprehensive Business Continuity Plans (BCPs) maintained for all core systems.

recovery, and crisis management	• Mandatory annual disaster recovery simulations and high-availability drills.
(d) supply chain security, including security-related aspects concerning relationships with direct suppliers	• Regular security capability reviews and compliance audits for hardware/EMS partners. • Personal data obligations contractually extended to suppliers under BS 10012. • Automated provisioning of machine-readable Software Bill of Materials (SBOM).
(e) security in network and info systems acquisition, development, maintenance, including vulnerability handling	• Certified under IEC 62443-4-1 with security checkpoints from design to test. • Mandatory automated pre-factory vulnerability scanning for 100% of products. • Guaranteed minimum 5-year security update support compliant with EU CRA.
(f) policies and procedures to assess effectiveness of cyber risk-management measures	• Dedicated internal information security audits integrated into the annual audit plan. • Annual external surveillance audits for ISO 27001 and BS 10012 validity. • Bi-annual product security audits with direct reporting to the Board of Directors.
(g) basic cyber hygiene practices and cybersecurity training	• Global deployment of endpoint protection (EDR), patching, and host firewalls. • Mandatory continuous phishing simulations and employee social engineering training.
(h) policies and procedures regarding the use of cryptography and encryption	• "Secure by Default" protocol: enforced device encryption and disabled insecure legacy protocols. • Full cryptographic transmission across user domains via TRUSTe Privacy standard. • Centralized, strict password key management infrastructure to prevent leaks.
(i) human resources security, access control policies and asset management	• Granular identity governance with mandated password changes every 90 days. • Strict internal network segmentation and encrypted remote work gateway controls. • Zero-tolerance policy for privacy violations with formalized HR disciplinary procedures.
(j) use of multi-factor authentication, secured communications & secured emergency systems	• Full Multi-Factor Authentication (MFA/2FA) enforced across cloud platforms (mydlink/AQUILA PRO AI). • CEO-supervised "Information Security Management Committee" serves as the emergency backbone.