1. Purpose

D-Link Corporation (the "Company") has established this policy in order to strengthen the management of Information Security and to ensure that critical information assets are protected from internal and external, intentional or accidental threats in order to maintain the confidentiality, integrity and availability of information.

2. Operational Basis

This policy is based on the ISO27001:2022 International Standard for Information Security Management Systems.

3. Information Security Slogan

Make Confidentiality Leak Your Last Concern by Placing Information Security First.

4. Information Security Goals

The management objective of D-Link Information Security is to protect the confidentiality, integrity and availability of information assets

- Confidentiality: Ensure that only authorized employees have access to information.
- Integrity: Protect the correctness and integrity of information and processing methods.
- Availability: Ensure that authorized users can obtain information and use relevant equipment when needed.

5. Information Security Organization

To ensure robust information and communication security, the company has adopted the ISO/IEC 27001:2022 international standard for Information Security Management Systems (ISMS), as well as the Guidelines for Establishing Internal Control Systems for Public Companies. The Information Technology and Security Department serves as the dedicated unit for information security management and has established the Information Security Management Committee. The committee is convened by the CEO, with the head of the Information Technology and Security Department acting as the Information Security Management Representative. Relevant departments (e.g., product, personal data, privacy)

appoint Information Security Representatives. Regular information security management meetings are held to discuss related policies and other major security issues. The General Manager regularly reports the status of information security governance to the Board of Directors, ensuring comprehensive oversight and governance of information security.

6. Periodic Review

The policy should be evaluated at least annually to reflect government mandates, information technology, external threats, business needs and the latest development to ensure the effectiveness of Information Security practice.

7. Information Security Management Principles The management principles of this policy are mainly formulated in accordance with the key provisions of ISO 27001:2022.

7.1 Asset Management

In order to protect the security of the company's information assets, an inventory of information assets as well as the principles of information asset categorization, classification, and control measures should be established.

7.2 Security Related to Personnel

In order to reduce the impact of human factors on the Company's Information Security, appropriate information security education, training and publicity should be implemented as necessary to improve personnel's awareness of Information Security.

7.3 Physical and Environmental Security

In order to ensure the security of the computer room and related equipment, the computer room access control, equipment inspection and management principles and general information equipment use, management and scrapping principles should be established.

7.4 Communication and Operation Management

In order to ensure the correct and safe operation of information equipment, information equipment and network usage specifications should be formulated, and a prevention

mechanism for malicious programs, Trojan horses and ransomware should be established. Establish management principles for data backup operations. Establish a network security control mechanism and monitor the system usage to maintain network security.

7.5 Access Control

Establish mechanisms for user passwords, registration, change, deletion, and regular review to ensure access to information systems; establish network security service mechanisms to separate internal networks from external connections, and control the use of remote work and cloud services to maintain network and data security.

7.6 Password and Key Management

In order to ensure the confidentiality of the Company's system operations and various accounts, the Company should properly manage passwords and keys to minimize the risk of leakage and properly protect the company's sensitive information.

7.7 Information System Acquisition, Development and Maintenance

Standard control procedures should be established to ensure the security of application system development management, testing, acceptance, on-line, and maintenance operations.

7.8 Information Security Incident Management

Information Security reporting and processing procedure should be established to reduce the damage caused by Information Security incidents.

7.9 Operational Continuity Management

In order to ensure the continuous operation of the Company's business, a business continuity operation plan for important systems should be established and annual regular drills should be carried out.

8. Supplementary Provisions

8.1 The matters stipulated in this policy are stipulated in accordance with the international

standard ISO27001:2022 for Information Security Management Systems.

8.2 This policy is promulgated and implemented after the resolution of the Board of Directors is passed, and the same applies for revisions.

8.3 This policy was established on February 22, 2022.

8.4 This policy was revised on November 13, 2024.

8.5 This policy was revised on August 13, 2025.