Category：Cyber Security
Writer：Frank Chen
Division： General

資訊安全政策

Information Security Policy

Doc. No.：IM-002
Version： A2
Initial Date：2024/05/23

一、目的 Purpose

1.1 為使研華股份有限公司（以下簡稱本公司）資訊作業相關人員、資料、資訊系統、設備及網路安全運作，並符合相關法規之要求，特訂定資訊安全政策（以下簡稱本政策）作為最高指導原則。

1.1 In order to ensure the safe operation of personnel, data, systems, equipment and networks related to information operations of Advantech Co., Ltd. (hereinafter referred to as the company), and to comply with the requirements of relevant laws and regulations, an information security policy (hereinafter referred to as this policy) has been formulated as the highest guiding principle.

二、範圍 Scope

2.1 適用於本公司資訊資產之安全管理，涵蓋其機密性、完整性和可用性。

2.1 It is applicable to the security management of the company's information assets, covering its confidentiality, integrity and availability.

2.2 涉及本公司資訊作業或資料使用之全體員工、承包商、顧問、臨時雇員、客戶、第三方人員，皆應遵循本政策。

2.2 All employees, contractors, consultants, temporary employees, customers, and third-party personnel involved in the company's information operations or data use should follow this policy.

三、定義 Definition

無

None

四、作業內容及步驟 Operation Content and Procedure

4.1 資訊安全系統及組織

4.1 Information Security System and Organization:

4.1.1 建立資訊安全組織並明訂其權責，以推動及維持資安管理、執行與查核等工作。

4.1.1 Establish an information security organization and specify its rights and responsibilities to promote and maintain related management, execution, and inspection tasks.

4.1.2 訂定資安管理相關辦法及程序，以保護人員、資料、資訊系統、設備及網路等之機密性、完整性及可用性。

4.1.2 Formulate information security management related methods and procedures to protect the confidentiality, integrity and availability of personnel, data, systems, equipment and networks.

4.1.3 定期召開資安管理會議，檢視內外部風險、科技及業務需求等最新發展，以採取因應措施。

4.1.3 Convene information security management meetings on a regular basis to review the latest status in internal and external risks, technology and business needs, and take corresponding measures.

4.1.4 依照資安、個資保護相關法規之規定，謹慎處理與保護資料及系統的安全性。

4.1.4 Handle and protect data and system security cautiously in accordance with relevant regulations on information security and personal data protection.

4.2 存取控制：

4.2 Access Control:

4.2.1 限制對資訊及資訊處理設施之存取。

4.2.1 Restrict access to information and information processing facilities.

4.2.2 確保授權使用者得以存取，並避免系統及服務的未授權存取。

4.2.2 Ensure authorized users can access the system and services while preventing unauthorized access.

4.2.3 令使用者對保全其鑑別資訊負責。

4.2.3 Hold users responsible for securing their authentication information.

4.2.4 系統及資料之使用須經授權，且存取權限之授予應以業務所需之最小範圍為原則。

4.2.4 System and data usage must be authorized, and access permissions should be granted based on the principle of minimum necessary scope for business needs.

4.3 實體及環境安全：

4.3 Physical and Environmental Security:

4.3.1 防止組織資訊及資訊處理設施遭未經授權之實體存取、損害及干擾。

4.3.1 Prevent unauthorized physical access, damage, and interference to organizational information and information processing facilities.

4.3.2 防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。

4.3.2 Prevent loss, damage, theft, or compromise of assets and ensure continuity of organizational operations.

4.4 資產管理：

4.4 Asset Management:

4.4.1 識別組織之資產並定義適切之保護責任。

4.4.1 Identify organizational assets and define appropriate protection responsibilities.

4.4.2 確保所有資產依其對組織之重要性，受到適切等級的保護。

4.4.2 Ensure all assets are protected at an appropriate level based on their importance to the organization.

4.4.3 防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。

4.4.3 Prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

4.5 資料傳送：

4.5 Data Transmission:

4.5.1 確保資料傳送可追溯性及不可否認性 。

4.5.1 Ensure traceability and non-repudiation of data transmission.

4.5.2 維持傳送作業之可靠性及可用性。

4.5.2 Maintain the reliability and availability of transmission operations.

4.5.3 實體傳送使用破壞存跡或抗破壞之控制措施。

4.5.3 Use tamper-evident or tamper-resistant control measures for physical transmission.

4.5.4 使用規定之電子傳輸媒體傳遞資料，不可因貪圖方便而任意使用非法與不當之傳輸媒體。

4.5.4 Use prescribed electronic transmission media for data transfer, avoiding the use of illegal or improper transmission media for convenience.

4.5.5 不得利用任何傳輸媒介透過資料傳遞、訊息傳送、發言或視訊等方式透露機密或敏感性資訊給其他組織或人員。

4.5.5 Do not disclose confidential or sensitive information to other organizations or personnel through any transmission medium, such as data transfer, messaging, speech, or video.

4.5.6 內部資訊網站須依權責及工作需求核發適當權限，以管制相關文件之存取。

4.5.6 Internal information websites must grant appropriate access permissions based on authority and job requirements to control access to related documents.

4.6 端點裝置之安全組態及處置：

4.6 Security Configuration and Handling of Endpoint Devices:

4.6.1 對使用者端點裝置分發及回收 。

4.6.1 Distribution and retrieval of user endpoint devices.

4.6.2 對使用者端點裝置軟體安裝進行控制。

4.6.2 Control software installation on user endpoint devices.

4.6.3 對使用者端點裝置進行安全性更新。

4.6.3 Perform security updates on user endpoint devices.

4.6.4 使用者端點裝置經登入程序使用。

4.6.4 Use user endpoint devices through a login process.

4.6.5 防範惡意軟體對使用者端點裝置危害。

4.6.5 Prevent malware from compromising user endpoint devices.

4.6.6 管制自攜裝置對 server farm 存取，避免自攜裝置影響公司內部資訊系統、設備運作。

4.6.6 Control access to server farms from BYOD (Bring Your Own Device) to prevent

BYOD from affecting internal information systems and equipment operations.

4.7 網路安全：

4.7 Network Security:

4.7.1 網路使用者經授權後，只能在授權範圍內存取網路資源。

4.7.1 Network users can only access network resources within the authorized scope after authorization.

4.7.2 對使用網路系統的電腦連接線路，應適當加以控制，以減少未經授權之系統存取或電腦設施的風險。

4.7.2 Appropriate controls should be applied to computer connections using the network system to reduce the risk of unauthorized system access or computer facility compromise.

4.7.3 設定網路區隔之規劃，應遵循內外網路實體區隔規定，並應禁止個人無線網路裝置破壞內外網路實體區隔之安全機制。

4.7.3 The planning of network segmentation should follow the rules of physical separation between internal and external networks, and the use of personal wireless network devices that compromise the security mechanisms of this separation should be prohibited.

4.7.4 非經授權嚴禁使用無線網路及私有有線設備與網路介接。

4.7.4 Unauthorized use of wireless networks and private wired equipment to interface with the network is strictly prohibited.

4.8 資訊安全事故管理：

4.8 Information Security Incident Management:

4.8.1 確保對資訊安全事故之管理的一致及有效作法，包括對安全事件及弱點之傳達。

4.8.1 Ensure consistent and effective practices for managing information security incidents, including the communication of security events and vulnerabilities.

4.8.2 建立資安事件的回應及通報程序，提昇內部人員面對突發狀況之應對與協調能力。

4.8.2 Establish response and reporting procedures for information security incidents to enhance the ability of internal personnel to respond to and coordinate in the face of emergencies.

4.9 資訊系統備援與備份：

4.9 Information System Backup and Redundancy:

4.9.1 依照資訊之可用性及完整性需求，制定個資訊備份週期、方式及保存期限，並測試其有效性。

4.9.1 Develop backup cycles, methods, and retention periods for information based on availability and integrity requirements, and test their effectiveness.

4.9.2 依照備份資料之機密性需求加以防護，避免衍生之其他資安事件。

4.9.2 Protect backup data according to confidentiality requirements to prevent additional security incidents.

4.9.3 資訊系統建置適當之備援及備份機制並進行應變演練，強化資訊服務在面對威脅時之韌性。

4.9.3 Implement appropriate redundancy and backup mechanisms for information systems and conduct contingency drills to enhance the resilience of information services against threats.

4.10 密碼學：

4.10 Cryptography:

4.10.1 依照法規、客戶要求及資訊資產風險設置加密機制。

4.10.1 Implement encryption mechanisms according to regulations, customer requirements, and information asset risk assessments.

4.10.2 管制金鑰產生、分派啟用、儲存、更新、廢止到封存和銷毀等作業。

4.10.2 Control operations such as key generation, distribution, activation, storage, update, revocation, archiving, and destruction.

4.11 資訊分類分級及處理：

4.11 Information Classification and Handling:

4.11.1 資訊標示涵蓋所有格式的資訊及其他相關聯資產。

4.11.1 Information labeling should cover all formats of information and other related assets.

4.11.2 使人員及其他關注方認知標示要求。

4.11.2 Ensure that personnel and other concerned parties are aware of labeling requirements.

4.11.3 提供所有人員必要之認知方法，以確保正確標示資訊並進行相對應的處理 。

4.11.3 Provide all personnel with necessary awareness methods to ensure correct information labeling and corresponding handling.

4.12 技術脆弱性管理：

4.12 Technical Vulnerability Management:

4.12.1 定義並建立與技術脆弱性管理相關聯之角色及責任 。

4.12.1 Define and establish roles and responsibilities related to technical vulnerability management.

4.12.2 偵測其資訊資產是否存在脆弱性。

4.12.2 Detect vulnerabilities in information assets.

4.12.3 軟體更新管理過程，以確保對所有獲授權軟體，安裝最新經核可之修補程式及應用程式之更新套件。

4.12.3 Manage software update processes to ensure that all authorized software installs the latest approved patches and application updates.

4.12.4.使用適合所使用技術之弱點掃描工具，以識別脆弱性並查證脆弱性修補是否成功 。

4.12.4 Use appropriate vulnerability scanning tools for the technology in use to identify vulnerabilities and verify the success of vulnerability remediation.

4.12.5 定期辦理各項資訊安全檢測及稽核，以評估資訊環境之風險並進行改善。

4.12.5 Conduct regular information security assessments and audits to evaluate and improve the risk profile of the information environment.

4.13 保全開發政策：

4.13 Secure Development Policy:

4.13.1 確保資訊安全係跨越整個生命週期之整體資訊系統的一部分。此亦包括經由公共網路提供服務之資訊系統的要求事項。

4.13.1 Ensure that information security is part of the overall information system throughout its entire lifecycle. This also includes requirements for information systems that provide services over public networks.

4.13.2 當發展新資訊系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。

4.13.2 When developing new information systems or enhancing the functionality of existing systems, include security requirements in the system functional planning and requirements analysis phase.

4.13.3 在採購軟體時，視其安全需求，進行評估。

4.13.3 Evaluate security requirements when procuring software.

4.13.4 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

4.13.4 The security requirements and controls of the system should be proportional to the value of the information assets and consider the potential damage that insufficient security measures might cause.

4.13.5 資訊系統應保護資料，防止洩漏或被竄改。

4.13.5 Information systems should protect data to prevent leakage or tampering.

4.14 資訊安全政策審查及維護:

4.14 Information Security Policy Review and Maintenance:

4.14.1 本政策應至少每年審查一次，以反映相關法令、技術及本公司業務等最新發展，並予以適當修訂。

4.14.1 This policy should be reviewed at least once a year to reflect the latest developments in relevant laws, technology and the company's business, and be appropriately revised.

4.14.2 本政策修訂由總經理核定後，於公告日施行。且應以公告、書面、電子郵件或其他方式告知利害關係人，如：全體員工、合作廠商、供應商等。

4.14.2 The revision of this policy is approved by the general manager, and become effective on the announcement day. In addition, interested parties, such as all employees, cooperating manufacturers, suppliers, etc., shall be notified by announcement, writing, e-mail or other methods.

4.14.3 訂定資訊安全目標，並考慮關鍵系統與重要設備的機密性、完整性、可用性，且每年至少一次定期量測與審查各指標項目，確保績效指標落實的有效性。

4.14.3 Consider the confidentiality, integrity, and availability of key systems and important equipment to set information security objectives, and regularly measure and review each indicator item at least once a year to ensure the effectiveness of performance.