修訂紀錄Revision Log

版次 Ver.	修訂人員Prepared by		修訂原因/章節 Modify chart / Reason	權責主管 Approved by	變更日期 Last modified date
	權責部門 Dept	姓名 Name			
01	系統資訊管理處 W000	葉育仁	新建立 Create New Document	林尚璋 Edward	2024.03.19
02	系統資訊管理處 W000	葉育仁	新增 項次4.2.13 ~ 4.2.18、6.5.8、8. Add items 4.2.13 ~ 4.2.18, 6.5.8, 8. 修改 項次6.2、6.4 Modify items 6.2 and 6.4	林尚璋 Edward	2024.04.09
03	系統資訊管理處 W000	葉育仁	新增項次4.4 Add items 4.4 新增項次5.2 Add items 5.2 新增項次6.8 Add items 6.8 修改項次4.2.7 Modify item 4.2.7	林尚璋 Edward	2024.07.16
04	系統資訊管理處 W000	鍾永廷	新增5.3「資訊安全管理組織架構圖」 Add 5.3 Information Security Management Organizational Chart	林尚璋 Edward	2025.02.18

目錄Table of contents

1. 目的PURPOSE

上詮光纖因應資訊安全管理系統的要求，對於流程制度、法令遵循、人員訓練及科技運用，強化資料、資訊系統、設備及網路通訊之安全及防護能力，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，以確保對股東、客戶的承諾，達到保證公司業務持續營運之目的。

In response to the requirements of the information security management system, Shangquan Optical Fiber has strengthened the security and protection capabilities of data, information systems, equipment and network communications in terms of process systems, legal compliance, personnel training and technology application, effectively reducing the risk of human negligence, intentional or natural Risks such as theft, improper use, leakage, tampering or destruction of information assets caused by disasters, etc., to ensure the commitment to shareholders and customers, and to achieve the purpose of ensuring the company's continued business operations.

2. 範圍SCOPE

2.1. 公司資訊安全管理制度（ISMS）Company Information Security Management System (ISMS):

所涵蓋範圍皆適用之。This applies to all areas covered.

2.2. 資訊安全管理涵蓋14項管理事項Information security management covers 14 management matters:

避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對公司帶來各種可能之風險及危害。管理事項如下

Avoid improper use, leakage, tampering, destruction, etc. of data due to factors such as human negligence, intentionality, or natural disasters, which may bring various possible risks and harms to the company. Management matters are as follows：

2.2.1. 資通安全政策之制定及評估
Formulation and evaluation of information security policies

2.2.2. 資訊安全組織之職責與分工
Responsibilities and division of labor of information security organizations

2.2.3. 人力資源安全HR security

2.2.4. 資訊資產管理Information asset management

2.2.5. 存取控制Access control

2.2.6. 密碼措施Cryptographic measures

2.2.7. 實體與環境安全Physical and Environmental Security

2.2.8. 資訊作業安全Information job security

2.2.9. 通訊安全Communication security

2.2.10. 資訊系統獲取、開發及維護
Information system acquisition, development and maintenance

2.2.11. 供應商關係Supplier relations

2.2.12. 資通安全事故管理Information security incident management

2.2.13. 營運持續管理之資訊安全層面
Information Security Aspects of Operational Continuity Management

2.2.14. 遵循性Compliance

3. 權責RESPONSIBILITY

3.1. 系統資訊管理處部門 System Information Management Office

資訊安全政策、計畫及技術規範之研議、建置及評估等事項與資料及資訊系統之安全需求研議、使用管理及保護等事項負責重要資訊系統管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。並加強資訊安全管理人力之培訓，提升全公司同仁資訊安全管理能力。

Personnel responsible for the management, maintenance, design and operation of important information systems, such as the research, establishment and evaluation of information security policies, plans and technical specifications, and the research, use management and protection of data and information system security requirements, etc. There should be an appropriate division of labor, decentralized powers and responsibilities, and a checks and balances mechanism should be established as necessary, staff rotation should be implemented, and a manpower backup system should be established. We also strengthen the training of information security management personnel to enhance the information security management capabilities of all colleagues in the company.

3.2. 系統資訊管理處主管 Head of System Information Management Office

需與公司各部門協調及推動資訊安全管理事項，負責督導所屬員工之資訊作業安全，防範不法或不當行為。

Need to coordinate and promote information security management matters with various departments of the company, be responsible for supervising the information security of employees, and prevent illegal or inappropriate behaviors.

4. 名詞定義DEFINITION

4.1. 資訊安全政策Information Security Policy

為保護上詮光纖公司的產品與服務之資訊，避免有未經授權之存取、修改、使用及揭露，以及天然災害所引起之損失，並適時提供完整與可用之資訊，致力於上詮資訊安全管理，以確保上詮重要資訊財產之機密性(確保被授權之人員才可使用資訊)、完整性(確保使用之資訊正確無誤、未遭竄改)及可用性(確保被授權之人員能取得所需資訊)，並符合相關法令法規之要求，進而獲得客戶信賴、達到對股東的承諾，保證公司重要業務持續運作。

In order to protect the information of Shangquan Optical Fiber Company's products and services from unauthorized access, modification, use and disclosure, as well as losses caused by natural disasters, and to provide complete and usable information in a timely manner, we are committed to Shangquan Information Security management to ensure the confidentiality of Shanghua's important information assets (to ensure that only authorized personnel can use the information), integrity (to ensure that the information used is correct and has not been tampered with) and availability (to ensure that authorized personnel can obtain all information) information required), and comply with the requirements of relevant laws and regulations, thereby gaining the trust of customers, achieving commitments to shareholders, and ensuring the continued operation of the company's important businesses.

4.2. 資通安全政策內容Information security policy content

4.2.1. 公司各項資訊安全管理規定必須遵守政府相關法規（如：資通安全管理法、刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等）之規定。

The company's various information security management regulations must comply with relevant government regulations (such as: Information Security Management Law, Criminal Law, State Secrets Protection Law, Patent Law, Trademark Law, Copyright Law, Personal Data Protection Law, etc.).

4.2.2. 成立資訊安全管理組織負責資訊安全制度之建立及推動事宜。

Establish an information security management organization to be responsible for the establishment and promotion of information security systems.

4.2.3. 定期實施資通安全教育訓練，宣導資訊安全政策及相關實施規定。

Regularly implement information security education and training, and promote information security policies and related implementation regulations.

4.2.4. 建立主機及網路使用之管理機制，以統籌分配、運用資源。

Establish a management mechanism for host and network usage to coordinate the allocation and utilization of resources.

4.2.5. 新設備建置前，須將風險、安全因素納入考量，防範危害系統安全之情況發生。

Before constructing new equipment, risk and safety factors must be taken into consideration to prevent situations that may endanger system security.

4.2.6. 明確規範網路系統之使用權限，防止未經授權之存取動作。

Clearly regulate the usage rights of network systems to prevent unauthorized access.

4.2.7. 依據內部稽核流程進行，定期檢視公司推行資訊安全管理制度範圍內所有人員及設備使用情形，依稽核報告擬訂及執行矯正預防措施。

In accordance with the internal audit process, regularly review the use of all personnel and equipment within the scope of the company's information security management system, and formulate and implement corrective and preventive measures based on the audit report.

4.2.8. 公司所有人員負有維持資通安全之責任，且應遵守相關之資通安全管理規範。

All company personnel are responsible for maintaining information security and should abide by relevant information security management regulations.

4.2.9. 資訊安全管理制度文件應有明確之管理規範。

Information security management system documents should have clear management specifications.

4.2.10. 委外廠商在執行公司委外業務時若有複委託之需求，應評估複委託業務相關之資安風險。並要求委外廠商依資訊安全管理制度(ISMS)等相關規定對複委託廠商進行適當之監督與管理。

If the outsourced manufacturer needs to re-entrust the company's outsourced business, it should evaluate the information security risks related to the re-entrusted business. It also requires outsourced vendors to conduct appropriate supervision and management of subcontracted vendors in accordance with the Information Security Management System (ISMS) and other relevant regulations.

4.2.11. 對內部及外部專案管理的過程中，應明訂及陳述與專案相關之各項資訊安全要求，並由風險評鑑之結果用以決定及實作資訊安全控制措施，確保內部及外部專案資訊之機密性、完整性及可用性，降低機敏資訊(含個人資料)外洩及違反法令之風險。

In the process of internal and external project management, various information security requirements related to the project should be clearly defined and stated, and the results of the risk assessment should be used to determine and implement information security control measures to ensure the security of internal and external project information. Confidentiality, integrity and availability reduce the risk of leakage of sensitive information (including personal data) and violation of laws.

4.2.12. 應制定可攜式資訊設備(包含智慧型移動裝置)及可攜式儲存媒體之管理程序，要求同仁落實執行，並定期針對可攜式資訊設備(包含智慧型移動裝置)及可攜式儲存媒體進行風險評鑑，依據風險評鑑之結果選擇適切之控制措施，定期對同仁執行查核作業，確保使用可攜式資訊設備及儲存媒體之風險受到監控，降低機密資料外洩之風險。

Management procedures for portable information equipment (including smart mobile devices) and portable storage media should be formulated, requiring colleagues to implement them, and regularly monitoring portable information equipment (including smart mobile devices) and portable storage media. Conduct a risk assessment, select appropriate control measures based on the results of the risk assessment, and conduct regular audits on colleagues to ensure that the risks of using portable information equipment and storage media are monitored and to reduce the risk of leakage of confidential information.

4.2.13. 重要主機或系統需異地備援籍資料備份機制，並定期進行還原測試驗證。

Important restoration of hosts or systems requires an off-site backup data backup mechanism and regular testing and verification.

4.2.14. 需根據資料分類定義備份策略如資料庫及檔案庫，定期安排備份。

It is necessary to define backup strategies based on data classification, such as databases and archives, and schedule backups regularly.

4.2.15. 需定義安全威脅指標或可疑行為以進行辨識。

Security threat indicators or suspicious behaviors need to be defined for identification.

4.2.16. 軟體授權管理準則，可追蹤資產授權，並確保所有相關協議、法律和法規。

Software licensing management guidelines to track asset licensing and ensure all relevant agreements, laws and regulations.

4.2.17. 因應資訊安全政策需建置資訊安全防護演練紀錄表

In accordance with the information security policy, an information security protection Scenario record sheet needs to be established(依照 A-A-ISO-24-004-01)

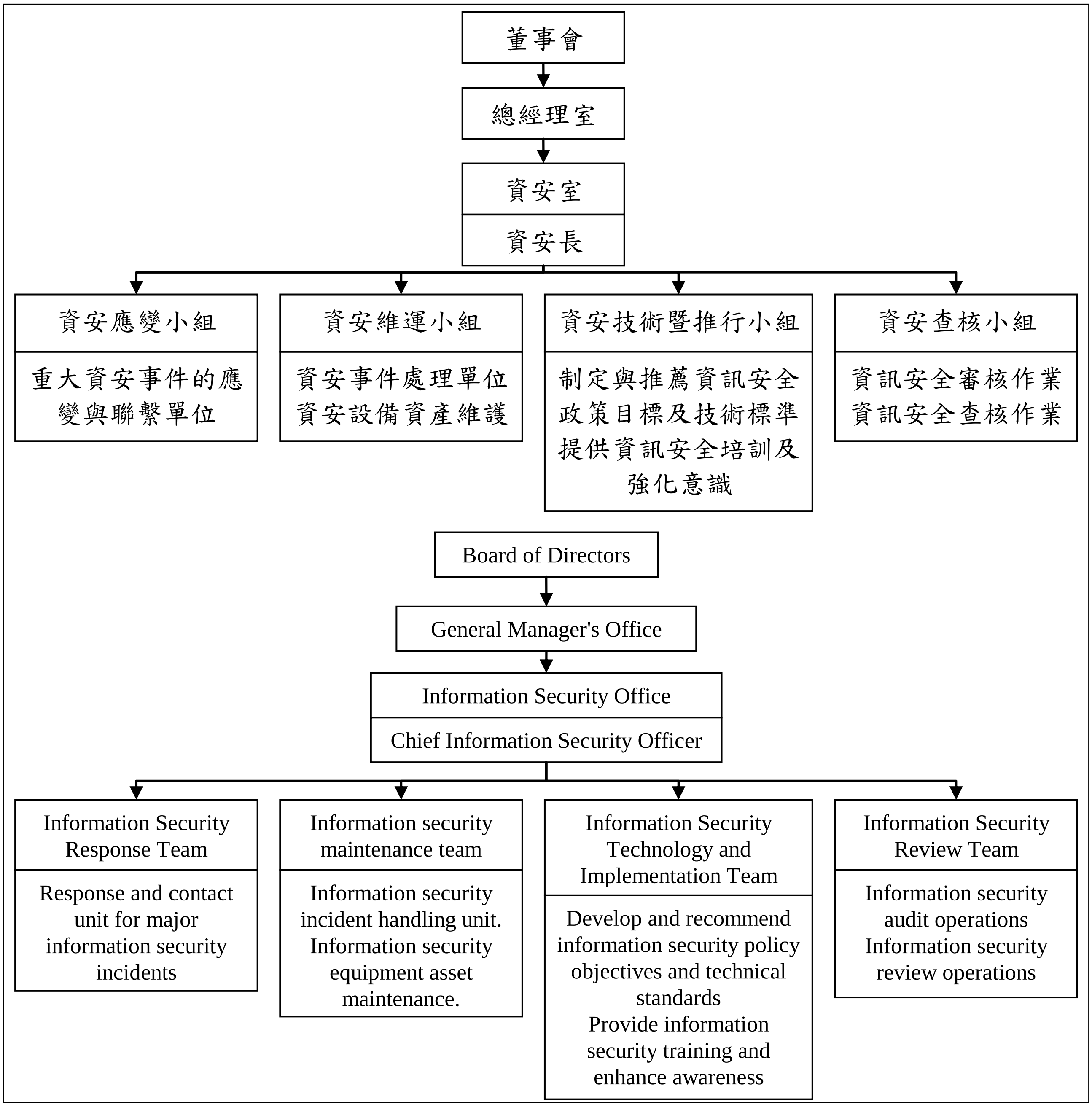
4.2.18. 程式更新及開發，需遵循資訊管理處系統分析模板進行。

Program updates and development must follow the System Analysis Template of the Information Management Office.(依照 A-A-ISO-24-004-02)

4.3. 資安室組織架構Information Security Office Organizational Structure

資安室每二個月召開一次(視需求調整會議頻率)，報告相關執行狀況。會議議程包括資安事件處理報告，各報告組內事務的推動情形，需各單位配合之事項，其他相關建議或臨時動議。管理代表需跟總經理報告資訊安全執行情況。

The Information Security Office holds meetings every two months (additional meetings may be held as appropriate) to report on relevant implementation status. The agenda of the meeting includes information security incident handling reports, the progress of affairs within each reporting group, matters requiring cooperation from each unit, and other relevant suggestions or temporary motions. Management representatives need to report information security implementation status to the general manager.



董事會

總經理室

資安室

資安長

資安應變小組：重大資安事件的應變與聯繫單位

資安維運小組：資安事件處理單位 資安設備資產維護

資安技術暨推行小組：制定與推薦資訊安全政策目標及技術標準 提供資訊安全培訓及強化意識

資安查核小組：資訊安全審核作業 資訊安全查核作業

Board of Directors

General Manager's Office

Information Security Office

Chief Information Security Officer

Information Security Response Team: Response and contact unit for major information security incidents

Information security maintenance team: Information security incident handling unit. Information security equipment asset maintenance.

Information Security Technology and Implementation Team: Develop and recommend information security policy objectives and technical standards Provide information security training and enhance awareness

Information Security Review Team: Information security audit operations Information security review operations

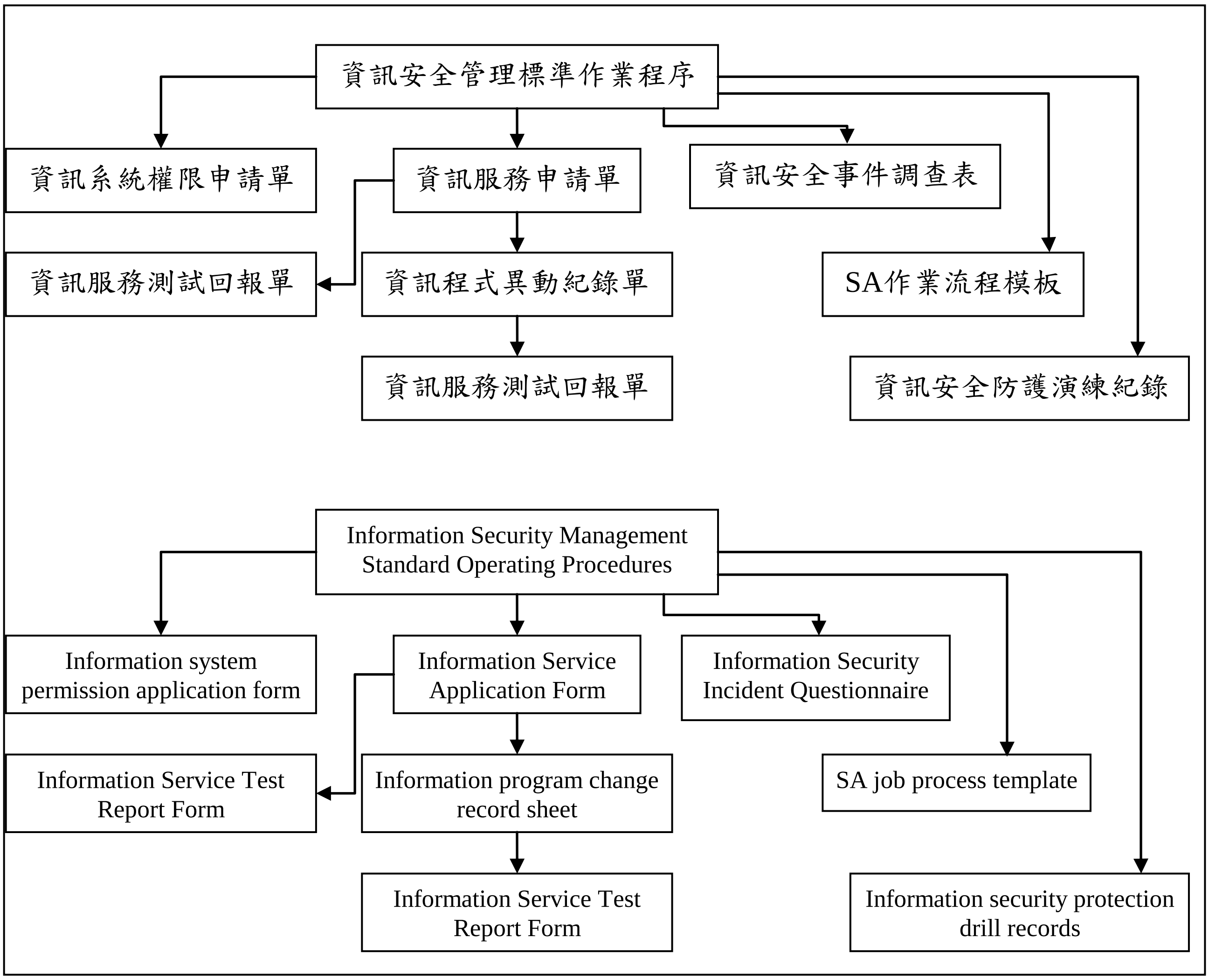
4.4. 攝影器材資料提取作業Photographic Equipment Data Extraction Work Instructions:

為了確保公司內所有攝影器材在遵守資訊安全規範的前提下，能夠安全地提取資料，並實現簡潔便利。

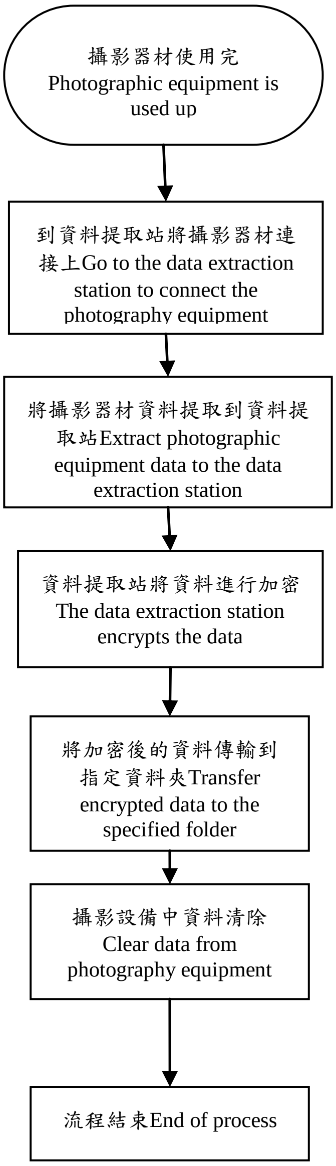
In order to ensure that all photographic equipment in the company can extract data safely and achieve simplicity and convenience while complying with information security regulations.

5. 架構圖Architecture diagram

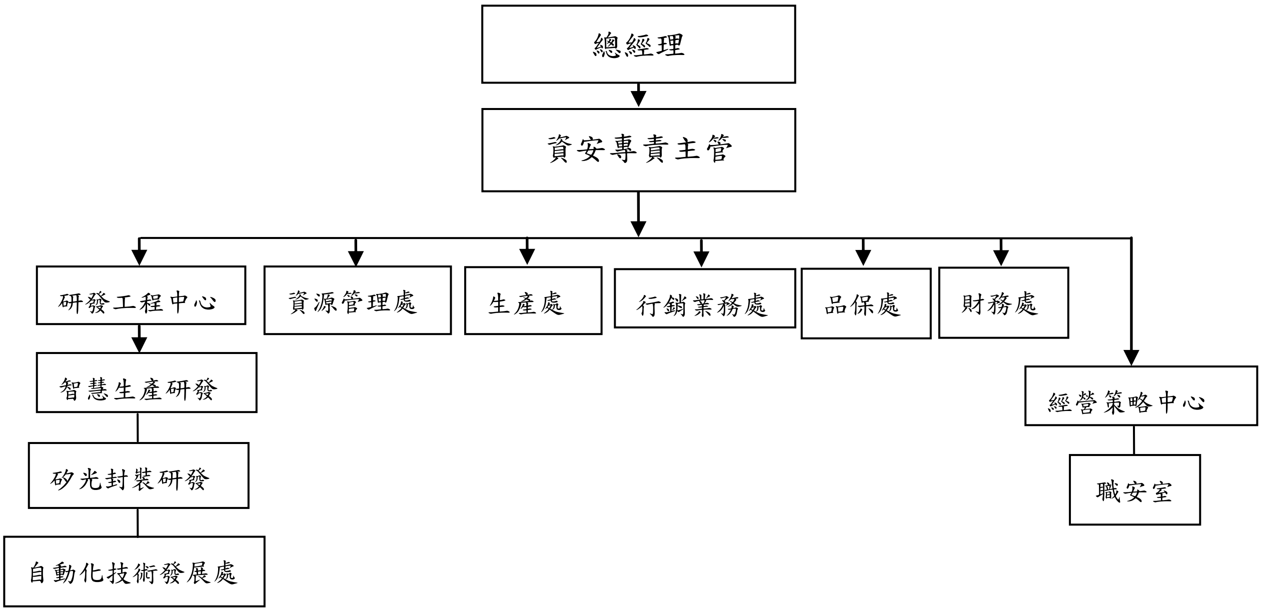
5.1. 資訊安全管理標準作業程序流程圖 Information security management standard operating procedure flow chart

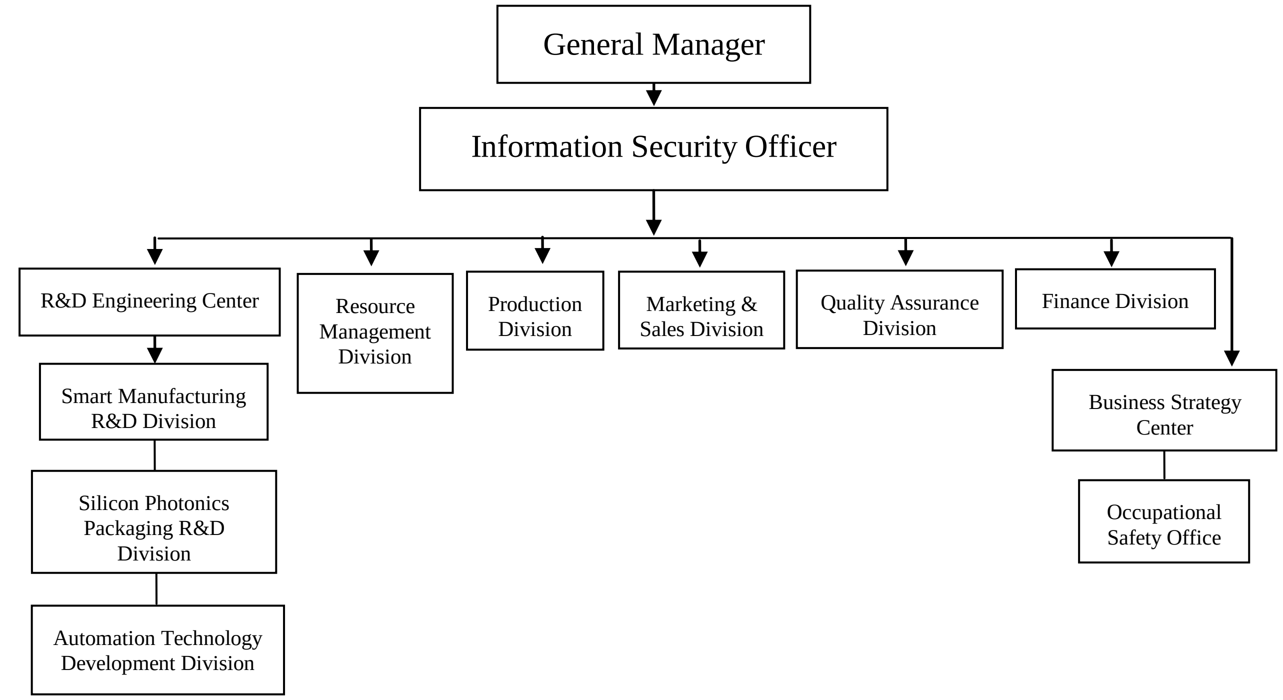

資訊安全管理標準作業程序
資訊系統權限申請單
資訊服務申請單
資訊安全事件調查表
資訊服務測試回報單
資訊程式異動紀錄單
SA作業流程模板
資訊服務測試回報單
資訊安全防護演練紀錄
Information Security Management Standard Operating Procedures
Information system permission application form
Information Service Application Form
Information Security Incident Questionnaire
Information Service Test Report Form
Information program change record sheet
SA job process template
Information Service Test Report Form
Information security protection drill records

5.2. 攝影器材資料提取作業流程圖Photographic equipment data extraction operation flow chart

作業流程Work process	權責單位 Responsible unit
 攝影器材使用完 Photographic equipment is used up 到資料提取站將攝影器材連接上Go to the data extraction station to connect the photography equipment 將攝影器材資料提取到資料提取站Extract photographic equipment data to the data extraction station 資料提取站將資料進行加密 The data extraction station encrypts the data 將加密後的資料傳輸到指定資料夾Transfer encrypted data to the specified folder 攝影設備中資料清除 Clear data from photography equipment 流程結束End of process	攝影器材使用人 Photographic equipment users

5.3. 資訊安全管理組織架構圖 (Information Security Management Organizational Chart)




General Manager
Information Security Officer
R&D Engineering Center
Resource Management Division
Production Division
Marketing & Sales Division
Quality Assurance Division
Finance Division
Smart Manufacturing R&D Division
Business Strategy Center
Silicon Photonics Packaging R&D Division
Occupational Safety Office
Automation Technology Development Division

更新日期 2025.02.18

5.4. 辨識資訊安全管理制度之相關利害團體 Identify relevant stakeholder groups of information security management systems:

定期確認利害關係團體對於資訊安全管理制度之需求（包含客戶對資安的要求）社交工程演練及員工資安教育訓練，以全面性的提升同仁資安意識
Regularly confirm the needs of stakeholder groups for information security management systems (including customer requirements for information security), conduct social engineering drills, and employee security education and training to comprehensively enhance colleagues’ information security awareness.

5.4.1. 制定完整規範及明確之作業流程，讓資安管理制度化地運行
Develop complete, standardized and clear operating procedures to allow information security management to operate in an institutionalized manner

5.4.2. 定期執行風險評鑑，以識別出高風險項目並投入適當資源予以降低或移轉
Conduct risk assessments regularly to identify high-risk projects and invest appropriate resources to reduce or transfer them

5.4.3. 透過各項工具、技術運用做到及時有效的辨識、保護、偵測、回應及復原
Achieve timely and effective identification, protection, detection, response and recovery through the use of various tools and technologies

5.4.4. 建立資安異常事件應變及復原作業流程，以期能迅速對資訊安全事件隔離、排除威脅，降低影響範圍及程度
Establish an information security abnormal incident response and recovery operation process, with a view to quickly isolating information security incidents, eliminating threats, and reducing the scope and degree of impact.

5.4.5. 定期執行關鍵應用系統災難復原演練，以確保其有效性
Regularly perform disaster recovery drills for critical application systems to ensure their effectiveness

5.4.6. 每年定期執行內外部稽核，檢視整個管理系統，確保正常運作並持續改善
Conduct internal and external audits regularly every year to review the entire management system to ensure normal operation and continuous improvement

5.4.7. 持續關注新的資安資訊、技術，將防禦或管理手法與時俱進，以有效阻擋新型態的資安威脅，降低營運的風險
Continue to pay attention to new information security information and technologies, and keep defense or management methods up to date to effectively block new types of information security threats and reduce operational risks.

5.4.8. 強化員工資安意識:為了落實資訊安全觀念至每一位員工，公司每季進行社交工程演練，模擬駭客的釣魚郵件，檢測員工資安風險意識，輔以資安宣導及教育訓練。每月發布資安電子報，包含最新資 安趨勢與近期國內外重大資安事件，藉此提升同仁對於資安的意識及警覺性。同時，對於員工違反資訊 安全政策時，給予懲處並做為績效管理之參考依據，以降低資訊安全之 風險，與對公司

營運衝擊。

Strengthen employee security awareness: In order to implement the concept of information security to every employee, the company conducts social engineering drills every quarter, simulates phishing emails from hackers, and tests employees' awareness of security risks, supplemented by information security promotion and education training. Information security e-newsletters are released monthly, including the latest information security trends and recent major domestic and international information security incidents, to enhance colleagues' awareness and vigilance of information security. At the same time, when employees violate information security policies, they will be punished and used as a reference for performance management to reduce information security risks and the impact on company operations.

5.4.9. 網路及系統的弱點偵測:為保護公司及個人資訊，以及對內對外通訊系統避免因洩漏、竊取、破壞等人為因素，或天然災害所引起的損失，除了每季內部的弱點掃描，每年定期委託第三方專業單位進行網路及系統的滲透測試，降低 人為因素或自然因素之影響對公司營運所造成的衝擊。其目的為瞭解、評估組織網路環境及系統安全狀況，驗證目前資安防護的安全等級與成效，做為漏洞補強、改善方法、加強系統的安全性。

Network and system vulnerability detection: In order to protect company and personal information, as well as internal and external communication systems from losses caused by human factors such as leakage, theft, destruction, or natural disasters, in addition to quarterly internal vulnerability scans, annual Regularly entrust third-party professional units to conduct network and system penetration tests to reduce the impact of human factors or natural factors on the company's operations. Its purpose is to understand and evaluate the organization's network environment and system security status, verify the security level and effectiveness of the current information security protection, and use it as a method to reinforce loopholes, improve methods, and enhance system security.

5.5. 軟體開發安全Software Development Security

為提早控管軟體開發生命週期（Software development lifecycle，SDLC）的安全，達成測試左移（Shift Left）安全性，以降低應用系統資安維運成本，並須遵循設計和開發安全指引和確認清單，公司導入了 DevSecOps（Development, Security and Operations）機制，並強化了開發團隊、維運團隊及資安團隊的協同合作。同時將軟體組 成分析（Software Composition Analysis，SCA）技術加入開發作業流程中，以提昇軟體的安全品質，系統應用程式上線前有執行程式碼安全掃描並於上線前修復漏洞。

In order to control the security of the software development lifecycle (SDLC) in advance, achieve test shift left (Shift Left) security, and reduce the cost of application system information security and maintenance, and must follow design and development safety guidelines and confirmation checklists, the company introduced DevSecOps (Development, Security and Operations) mechanism, and strengthened the collaborative cooperation between the development team, maintenance team and information security team. At the same time, Software Composition Analysis (SCA) technology is added to the development process to improve the safety quality of software, Before system applications go online, code security scans are performed and vulnerabilities are fixed before going online..

5.6. 資安警訊通報與事件管理Information security alert notification and incident management:

根據資安事件管理規範，確保公司資訊安全事件通報、分類、分級、處理、統計及追蹤之作業制度化並 系統化。當資訊安全事件發生時，迅速通報及應變處理，並在最短時間內回復，以確保各項業務之正常 運作 導入進階持續性威脅 （ATP）監控與資安監控中心（SOC）的運作機制，偕同外部資安專家 的資源，資安維運與應變小組人員迅速掌握資安警訊通報及情資事件，強化並加速偵測與回應機制。

In accordance with the information security incident management specifications, ensure that the reporting, classification, grading, processing, statistics and tracking of company information security incidents are institutionalized and systematic. When an information security incident occurs, we will quickly report and respond to it, and respond within the shortest time to ensure the normal operation of all businesses. Introduce the operation mechanism of Advanced Persistent Threat (ATP) monitoring and Security Control Center (SOC). Together with the resources of external security experts, the staff of the security maintenance and response team quickly grasped security alert notifications and intelligence incidents, and strengthened and accelerated the detection and response mechanism.

5.7. 災難復原演練Disaster recovery drill:

為確保營運與重要業務的永續運作，避免重要資訊系統因重大災難事件而導致服務無法持續的風險，公司每半年至少進行一次測試或書面演練資訊業務營運持續計畫或資安事故緊急應變計畫， 確保公司在關鍵時刻發揮災難應變能力以災害復原機制快速回復至企業正常或可接受的營運水準，以達到關鍵應用系統能持續運作並確保企業的營運不中斷。此外電腦中心的備份管理人員每年至少一次 選取部份備份儲存媒體或備援設備，進行備份資料之回存測試，以確認備份資料之可讀性、儲存媒體之可用性與重要資產回存測試步驟的可行性，以確保有效之備份作業，能夠在恢復操作步驟分配的時間內完成。

In order to ensure the sustainable operation of operations and important businesses and avoid the risk of unsustainable services for important information systems due to major disaster events, the company conducts tests or written drills at least once every six months on the information business operations continuation plan or information security incident emergency response plan. To ensure that the company exerts its disaster response capabilities at critical moments and uses the disaster recovery mechanism to quickly return to the company's normal or acceptable operating levels, so that key application systems can continue to operate and ensure that the company's operations are not interrupted. In addition, the computer center's backup managers select some backup storage media or backup devices at least once a year to conduct a backup data restore test to confirm the readability of the backup data, the availability of the storage media, and the test procedures for restoring important assets. Feasibility to ensure that effective backup operations can be completed within the time allocated for recovery operation steps.

2022 年全球電腦中心針對 7 大功能系統與資料庫，選取了 30 份備份儲存媒體，成功完成備份資料 之回存測試。年度全球電腦中心災難復原演練結果顯示，災難事故發生時最大可容忍資料遺失時間，還需要制定安全要求的實現方式、安全人員角色。（RPO）=0.9 小時，災難事故發生後，最大可容忍資訊服務復原時間 （RTO）=18.83 小時。

Computer Center selected 30 backup storage media for 7 major functional systems and databases, and successfully completed the backup data restore test. The results of the annual global computer center disaster recovery drill show that the maximum tolerable data loss time when a disaster occurs, and the implementation of security requirements and the roles of security personnel also need to be formulated. (RPO) = 0.9 hours. After a disaster, the maximum tolerable information service recovery time (RTO) = 18.83 hours.

5.8. 雲服務評估Cloud service evaluation:

5.8.1. 審查雲端業者的資質，確保其具有提供雲端服務的能力和經驗。
Review the qualifications of cloud providers to ensure they have the ability and experience to provide cloud services.

5.8.2. 簽訂雲端服務合約，明確雙方的權利義務
Sign a cloud service contract to clarify the rights and obligations of both parties

5.8.3. 定期對雲端業者進行稽核，以確保其符合相關規定
Regularly audit cloud providers to ensure they comply with relevant regulations

5.8.4. 定期查核雲端服務的資安控管措施是否有效
Regularly check whether the information security control measures of cloud services are effective

5.8.5. 定期查核雲端服務的使用是否符合相關規定
Regularly check whether the use of cloud services complies with relevant regulations

5.8.6. 定期查核雲端服務的營運是否穩定可靠
Regularly check whether the operation of cloud services is stable and reliable

5.8.7. 雲端服務業者重大事件通報及緊急應變處理
Notification of major incidents and emergency response for cloud service providers

5.8.8. 制定雲服務供應商的資安管理政策與辦法。
Develop information security management policies and methods for cloud service providers.

5.9. 資安政策之評估與審查Evaluation and review of information security policies:

本政策應至少每年評估及審查一次，以反映政府資通安全管理政策、法令、技術及公司業務等之最新發展現況，確保公司資訊安全管理制度的可行性及有效性，以維持營運和提供適當服務的能力

Evaluation and review of information security policy: This policy should be evaluated and reviewed at least once a year to reflect the latest developments in government information security management policies, laws, technology and company business, etc., to ensure the feasibility and effectiveness of the company's information security management system. effectiveness to maintain operations and the ability to provide appropriate services

5.10. 網路安全框架Cybersecurity Framework2.0

NIST CSF旨在提供高層次的框架，並且可以擴展至任何組織，但可能導致CSF的子類別想要呈現的意圖難以理解。對於網路安全框架CSF 2.0版，NIST將用更為「簡單明確與行動導向」的流程呈現，並使用範例，讓組織可具體瞭解如何實現子類別的預期結果，以確保其對於各種組織的規模與靈活性都能適用。期望通過CSF 六大功能分別為識別、防禦、偵測、回應、恢復，以及新增的「治理」，透過利用與連接全球公認的標準與指南，但不取代它們的方式，產生組織所其期望資訊安全的價值。

The NIST CSF is intended to provide a high-level framework and can be extended to any organization, but may make it difficult to understand the intent of the CSF's subcategories. For the Cybersecurity Framework CSF version 2.0, NIST will present it in a more "simple, clear and action-oriented" process and use examples to allow organizations to understand specifically how to achieve the expected results of the subcategories to ensure that it is relevant to various organizations. Both scale and flexibility apply. It is expected that through the six major functions of CSF, namely identification, defense, detection, response, recovery, and the newly added "governance", by utilizing and connecting globally recognized standards and guidelines, but not replacing them, the organization can achieve its goals. Expect the value of information security.

5.10.1. 識別Identify:

發展組織有關系統、資產、資料、能力的網路安全風險管理的認知。

Develop the organization's understanding of cybersecurity risk management related to systems, assets, data, and capabilities.

(a) 資產管理（ID.AM）：識別出可讓組織達成其商業目的資料、人員、設備、系統及設施，依照這些在商業目標上的相對重要性，以及組織的風險策略，對上述資產進行管理。

Identify the data, personnel, equipment, systems and facilities that enable the organization to achieve its business objectives, and manage the above assets according to their relative importance to the business objectives and the organization's risk strategy.

(b) 商業環境（ID.BE）：瞭解組織的使命、目標、利益相關者以及活動，並且

排先後順序。此一資訊可以用來告知在網路安全的角色、責任以及風險管理的決策。

Understand and prioritize the organization's mission, goals, stakeholders, and activities. This information can be used to inform decisions about cybersecurity roles, responsibilities, and risk management.

(c)治理（ID.GV）：瞭解組織用來管控監理單位、法令、風險、環境及運作等需求的政策、程序以及流程，並且告知網路安全風險的管理。

Understand the policies, procedures, and processes used by the organization to control regulatory, regulatory, risk, environmental, and operational needs and inform the management of cybersecurity risks.

(d)風險評估（ID.RA）：組織瞭解有關組織營運（包括使命、功能、形象及聲譽）、組織資產以及人員的網路安全風險。

The organization understands the cybersecurity risks related to the organization's operations (including mission, functions, image and reputation), organizational assets and people.

(e)風險管理策略（ID.RM）：組織建立有關營運風險決策的優先順序、限制、允許風險以及假設。

The organization establishes priorities, limits, allowable risks, and assumptions for decisions regarding operational risks.

(f)供應鏈風險管理（ID.SC）：組織建立有關供應鏈風險管理決策的優先順序、限制、允許風險以及假設。組織也已有識別、評估及管理供應鏈風險的流程。

The organization establishes priorities, limits, allowable risks, and assumptions regarding supply chain risk management decisions. The organization also has processes in place to identify, assess and manage supply chain risks.

5.10.2. 防護Protection:

發展及實施適當的安全措施，確保關鍵基礎服務以及正常運作。

Develop and implement appropriate security measures to ensure the normal operation of critical infrastructure services.

(a)存取控制（PR.AC）：只允許有授權的人員、流程或是設備才可以存取資產及相關設施，並且其活動或交易也要經過授權。

Only authorized personnel, processes or equipment are allowed to access assets and related facilities, and their activities or transactions must also be authorized.

(b)意識和訓練（PR.AT）：組織的人員和上下游廠商都需要有資安意識教育訓練，並且使用可以進行和資料安全相關的責任及義務，和相關的政策、流程以及協議一致。

Organizational personnel and upstream and downstream vendors need to have information security awareness education and training, and be able to carry out their responsibilities and obligations related to data security, consistent with relevant policies, procedures and protocols.

(c) 資料安全（PR.DS）：管理資訊以及紀錄的方式，和組織保護資訊機密性、完整性及可用性的風險策略一致。
Manage information and records in a manner consistent with the organization's risk strategy for protecting the confidentiality, integrity and availability of information.

(d) 資訊保護程序和流程（PR.IP）：組織已有安全政策（其中有提到目的、範圍、角色、責任、管理承諾以及組織間的合作）、流程及程序，用來管理資訊系統及資訊資產的保護。
The organization has security policies (which address purpose, scope, roles, responsibilities, management commitment and inter-organizational cooperation), processes and procedures to manage the protection of information systems and information assets.

(e) 維護（PR.MA）：以和安全政策和流程一致的方式，維護或修理工業控制或是資訊系統的元件。
Maintain or repair components of industrial control or information systems in a manner consistent with security policies and procedures.

(f) 保護技術（PR.PT）：管理技術安全方案，確保系統及資產的安全及強健性，並且和相關的政策、程序及協議一致。
Manage technical security programs to ensure the security and robustness of systems and assets and are consistent with relevant policies, procedures and protocols.

5.10.3. 偵測Detect:

發展及實施可以識別網路安全事件發生的活動。
Develop and implement activities that identify cybersecurity incidents as they occur.

(a) 異常及事件（DE.AE）：可以及時的偵測到異常活動，並且瞭解事件的潛在影響。
Abnormal activities can be detected in a timely manner and the potential impact of the event can be understood.

(b) 安全持續監控（DE.CM）：定期監控資訊系統以及資產，以識別網路安全事件，並且驗證保護措施的效果。
Regularly monitor information systems and assets to identify network security incidents and verify the effectiveness of protective measures.

(c) 偵測流程（DE.DP）：維護偵測流程及程序，並且經過測試，確保可以及時、適當的告知有異常事件。
Maintain detection processes and procedures and test them to ensure that abnormal events can be notified promptly and appropriately.

5.10.4. 回應Respond:

發展及實施活動，針對已偵測到的網路安全事故進行因應。
Develop and implement activities to respond to detected cybersecurity incidents.

(a) 回應計劃（RS.RP）：執行及維護回應流程和程序，確保對偵測到的網路安全事故可以及時回應。
Implement and maintain response processes and procedures to ensure timely response to detected network security incidents.

(b) 溝通（RS.CO）：回應計劃和內部和外部的利益相關者一起進行，若合適的話，也可以包括執法單位的外部支援。
Response planning is conducted with internal and external stakeholders and, if appropriate, may include external support from law enforcement agencies.

(c) 分析（RS.AN）：分析的目的是要確保有進行適當的回應，並且分析也可以支持復原活動。
The purpose of analysis is to ensure that an appropriate response occurs, and analysis can also support recovery activities.

(d) 緩釋（RS.MI）：進行此一活動來避免事件的擴大、緩釋其影響、並且根除該事故。
This activity is carried out to avoid the expansion of the incident, mitigate its impact, and eradicate the incident.

(e) 改進（RS.IM）：透過整合歷來偵測活動或回應活動中累積的經驗教訓，提昇組織的回應活動。
Improve the organization's response activities by integrating lessons learned from past detection activities or response activities.

5.10.5. 復原Recover:

發展及實施活動，維持組織的韌性計劃，復原所有在網路安全事故中受損的能力或是服務。
Develop and implement activities to maintain the organization's resilience plan and restore all capabilities or services damaged by a cybersecurity incident.

(a) 復原計劃（RC.RP）：執行及維護復原流程和程序，確保因網路事件影響的系統或資產可以及時的恢復。
Implement and maintain recovery processes and procedures to ensure that systems or assets affected by network incidents can be recovered in a timely manner.

(b) 改進（RC.IM）：透過整合經驗教訓，提昇復原流程和程序，以因應未來的活動。
Improve recovery processes and procedures by integrating lessons learned to prepare for future activities.

(c) 溝通（RC.CO）：復原計劃和內部和外部的單位一起進行，例如網路危機處理暨協調中心、網路服務提供者、發起攻擊系統的所有者、受害者、其他電腦資安事件應變小組、以及供應商。
Recovery planning is conducted with internal and external parties, such as cyber crisis management and coordination centers, Internet service providers, owners of the systems that initiated the attack, victims, other computer security incident response teams, and vendors.

5.10.6. 治理Govern

組織環境（GV.OC），風險管理策略（GV.RM），角色、責任與權（GV.RR），政策（GV.PO），監督（GV.OV），網路安全供應鏈風險管理（GV.SC）。

5.11. 攝影器材資料提取作業辦法Photographic equipment data extraction work methods

5.11.1. 產線內攝影器材使用完畢
The photography equipment in the production line has been used

5.11.2. 攝影器材使用人到產線內資料提取站
Users of photographic equipment go to the data extraction station in the production line

5.11.3. 將攝影器材內資料取出至資料提取站
Take out the data from the photographic equipment to the data extraction station

5.11.4. 資料提取站取出後的資料電腦會自動進行加密
The data taken out from the data extraction station will be automatically encrypted by the computer.

5.11.5. 從資料提取站中將已加密資料傳輸到攝影器材使用人指定的資料夾
Transfer the encrypted data from the data extraction station to the folder designated by the user of the photographic equipment

5.11.6. 將攝影器材中資料清除 Clear data from photographic equipment

6. 相關文件REFERENCES

1. ISO/IEC 27001:2013 (Information technology — Security techniques — Information security management systems — Requirements)
2. 資通安全管理法Information Security Management Law (https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297)

7. 附件RECORD

1. 資訊安全防護演練紀錄Information security protection Scenario records(A-A-ISO-24-004-01)
2. 資訊管理處系統分析模板Information Management Office System Analysis Template(A-A-ISO-24-004-02)