

視陽光學股份有限公司

資通安全管理準則

第一條：目的

本公司為確保資通安全管理制度能持續有效運作，建立安全可靠之電腦化作業環境，確保電腦資料、系統、設備及網路安全，以符合相關法令規定，並保障公司權益及永續經營。

第二條：適用範圍

本公司所有正式員工、約聘員工、派遣人員等公司所聘用之人員及外來的訪客和廠商等。

第三條：資通安全目標

- 一、確保本公司資訊資產之機密性，落實資料存取控制，資訊需經授權人員方可存取。
- 二、確保本公司資訊作業管理之完整，避免未經授權之修改。
- 三、確保本公司資訊作業之持續運作，符合營運服務水準。
- 四、確保本公司資訊作業均符合相關法令規定要求。

第四條：資通安全管理架構

本公司為落實資通安全目標，故成立資通安全管理小組，負責資通安全管理制度規劃、建立、實施、維護、審查與持續改善，並定期召開管理審查會議，召集人由總經理擔任。小組相關作業的工作要點如下：

- 一、管制技術：外部技術處理，資訊安全維運，資訊安全工具提供、監控及規劃，資訊安全規範遵循，負責資訊安全事件蒐集調查。
- 二、教育訓練：資訊安全文化形塑、新人資訊安全教育、內外資訊安全訓練與講座。
- 三、稽核風管：資訊安全管理制度內部查核與資訊風險管控。
- 四、文件管制：文件資訊安全管制、分類及保存管理。
- 五、法律合規：資通安全管理、營業秘密管理、個人資料管理等法規遵循。

第五條：資通安全管理方案

本公司資通安全主要採取以下管理措施，詳細作法訂定於「資通安全管理辦法」。此外，並會隨時注意最新資安管理發展，導入相對應的資安措施，逐步建構完整的資安體系，以確保公司健全的運作。

- 一、員工安全管理及教育訓練：員工依其工作職掌，給予適當的系統與資料存

取權限，並進行資訊安全教育及訓練。

二、電腦主機安全管理：各項電腦主機及伺服器設備均指定專人管理與維護，並設密碼保護與定時更換，嚴禁使用非經授權及來路不明之軟硬體。

三、資料安全管理：資料保存定時備份，並分機密等級管理資料檔案與權限，以防止遺失、毀壞、被偽造或竄改。

四、系統開發維護安全管理：新發展的資訊系統，或是現有系統功能之強化，應考量資訊安全的需求與評估，並要求納入系統功能中。

五、網路安全管理：網路設備須有專人管理，隨時監測網路的狀況，並設置防火牆對內外網路進行安全控管。

六、網路存取之安全控制：使用者依其權限限制其連線作業能力，並應遵守相關安全規定；如有違反，依相關法規處理，並取消其網路資源存取權限。

七、系統與網路入侵之處理：隨時檢討網路安全措施及修正防火牆的設定，以防禦網路的入侵與攻擊。

八、設備安全管理：重要資訊設備應安置在適當的地點並予保護，以減少環境不安全引發的危險，及未經授權存取系統的機會。

九、實體環境安全管理：實體環境應以事前劃定的各項資訊設施為基礎，設置必要的障礙（例如：使用身分識別卡之安全門），達成安全控管的目的。電腦機房應考量火災、水災、地震等災害的實體安全防護措施，並考量鄰近空間的可能安全威脅。

十、業務永續經營運作計畫管理：為因應各種人為及天然災害造成業務運作受影響，須確實做好各項備份工作。各部門應依業務性質研擬緊急應變計畫，使各項業務得以永續運作。

十一、資通安全應變措施：於發生重大資通安全事件或其他災害涉及資通安全事件時，應立即「資通安全管理辦法」所載之分級方式處理。

十二、備份作業：應落實定期備份作業之規定，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

第六條：年度審查

本管理辦法每年至少審查一次，以符合相關法令規定及資訊業務最新發展現況，並於必要時修正之。

第六條：罰則

本公司員工違反本管理規定者，其主管應要求限期改善，如限期未見改善或案

件情節重大者，由當事人所屬單位部門主管、人力資源部及其他相關單位研議獎懲內容後，依本公司獎懲辦法之規定，報請權責主管核定後予以議處。與本公司有業務往來之廠商違反本管理規定者，應依雙方訂定之合約或約定辦理。

第七條：實施及修正

本作業程序訂立於民國一一一年六月一日。