1.作業程序

1.1.網路安全管理服務之控制

1.1.1.公司對外網路之節點，設置防火牆區隔內、外網路，以控管內部網路與外部網路之資料傳輸及資源存取。

1.1.2.防火牆管制及安全管理規則：

1.1.2.1.外部網路不得直接連線進入內部網路。

1.1.2.2.內部網路通往外部網路只開啟 HTTP,HTTPS,SMTP,POP3,PPTP,L2TP, SSH,DSN 等必要服務通道。

1.1.2.3.對外服務器置於 DMZ 並只開啟相關之服務通道 DNS,FTP,HTTP,HTTPS, SMTP,POP3,DCC)。

1.1.2.4.資訊單位應負責製發帳號，供授權的人員使用。

1.1.2.5.離職人員應依資訊安全規定及程序，取銷其存取網路之權利。

1.1.2.6.資訊單位需定期檢閱系統之日誌檔是否有異常現象，並檢查系統是否有更新檔並加以更新，以維持系統之穩定性及安全性。

1.1.2.7.應遵守智慧財產權相關規定。

1.1.2.8.使用者如須其它網路服務，提出申請經單位主管及總經理核准後，由資訊單位開放申請者使用。

1.1.2.9.使用者如須由遠端登入管理資訊系統，提出申請經單位主管及總經理核准後，由資訊單位開放申請者使用。

1.1.3.電腦病毒及惡意軟體之防範

1.1.3.1.資料經由電子郵件傳送或接收時，應於電腦系統設置防毒軟體，以防止駭客或電腦病毒之侵害。

1.1.3.2.公司員工應避免透過公司網路收發或下載與業務無關之郵件或軟體，以避免佔用公司之網路資源，及增加電腦病毒感染機會。

1.1.3.3.電腦病毒防制軟體應定期自動偵測病毒。

1.1.3.4 .建立軟體管理政策，規定使用者應遵守軟體授權規定，嚴禁使用未取得授權的軟體。

1.2.人員教育訓練

1.2.1.公司員工非經權責主管授權，禁止將公司相關資訊經由電子郵件對外傳送。

1.2.2.定期對員工進行資訊安全教育訓練。

1.3.系統與網路入侵之處理

1.3.1.應全面檢討網路安全措施及修正防火牆的設定，以防禦類似的入侵與功擊。

1.3.2.對於入侵者的追查，除利用稽核檔案提供的資料，可使用系統指令執行反向查詢，並連結相關配合單位(如外包網路服務公司)，追蹤入侵者。

1.3.3. 若入侵者之行為觸犯法律規定，構成犯罪事實，應立即告之檢警調單位，協助處理犯罪事實之調查。

1.4. 電腦作業之安全管制

1.4.1. 電腦作業環境如溫度、濕度及電源供應之品質等，應隨時監測，必要時採取補救措施。

1.4.2. 應有足夠的備援設施，定期執行必要性的資料及軟體備份之備援功能，防止災害發生或儲存媒體失效時，可迅速回復正常作業。

1.4.3. 系統作業發生錯誤時，應詳細紀錄並提報權責主管，立即採取必要性的更正作業。

1.5. 電腦報廢管制程序

1.5.1. 資訊人員應確實將硬碟資料銷毀且確定永遠無法恢復讀取，避免公司資料外洩，並依「不動產廠房及設備循環」之處分程序辦理。

1.6. 與委外廠商或第三方簽訂合約中，須包括符合公司資訊安全政策規範及法律要求。

2. 控制要點

2.1. 公司郵件伺服器是否裝設防火牆及防毒軟體以隔絕外來侵害。

2.2. 資訊人員是否定期檢視伺服器上郵件收發情形，若有異常狀況應呈報權責主管處理。

2.3. 報廢電腦時資訊人員應確實將硬碟資料銷毀且確定永遠無法恢復讀取，避免公司資料外洩，並依「不動產廠房及設備循環」之處分程序辦理。

3. 實施與修正

本辦法經董事會通過後實施，修改時亦同。