NIKO-SEM 尼克森微電子股份有限公司		編號	NKS-MIS-02
MIS 管理辦法		頁次	1/3
主題	資通安全管理辦法	□管制文件 ■非管制文件	

一、目的：

依『金融監督管理委員會』之『內部控制制度處理準則』第九條第十項規定『資通安全檢查之控制』制定本程序，以確保本公司資訊處理、傳送、儲存及流通之安全作有效之管制。

二、範圍：

本公司有關資通安全管理事務均屬之。

三、權責單位：

由資訊單位負責規劃，管理資通安全相關事務。

四、程序/方法：

(一)資訊安全政策訂定：

1.所訂定之資訊安全管理政策，以書面、電子或其他方式告知本公司所屬各單位員工、連線作業之相關單位及提供資訊服務之廠商共同遵行。

2.資訊安全管理政策實施後，資訊單位須定期評估，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

(二)建立資訊安全組織：

1.資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。

2.資料及資訊系統之安全需求研議、使用管理及保護等事項，由各單位負責辦理。

3.資通安全相關稽核事宜，由稽核單位會同相關單位負責辦理。

(三)人員安全與管理：

1.對資訊相關職務及工作人員，應進行安全評估，並依其任務之適任性進行必要之考核。

2.對可存取機密性與敏感性資訊或系統之人員，及因工作需要須配賦系統管理權限之人員，應加強評估及考核。

3.資訊單位得依業務及資訊等不同工作類別，視實際需要辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升機關資訊安全水準。

4.資訊單位應加強資訊安全管理人力之培訓，提升資訊安全管理能力。

5.對負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並視需要建立人力備援制度。

6.各級單位主管，須負責督導所屬員工之資訊作業安全，防範不法及不當行為。

(四)資產分類與控管：

1.重要資訊資產應指定保管人及指定專人定期檢測。

2.重要資訊資產應列冊管制並隨時更新。

(五) 實體及環境安全管理：

1.資訊單位就系統伺服器主機設備安置於主機房，並由資訊單位專責管理，並管制非相關人員隨意進出。

2.主機房須設置空調恆溫控制，並配置適量之化學消防設施。

3.若非資訊單位人員或維修人員，不得自行拆卸電腦機殼及更換內部零組件。

4.為防斷電時造成系統毀損或資料流失，主機房須配置不斷電系統因應斷電時有足夠時間做存檔與正常關機。

5.須設置防火牆設施以防外界的不當入侵。

(六)通訊與操作管理：

1.各系統伺服器與外界網路連接之網點，須透過防火牆的控管，始可進行外界與內部網路之資料傳輸及資源存取，必要時應以代理伺服器等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。

2.各單位使用電子郵件傳輸公務文件及資料須加密碼保護。

3.開放外界連線作業，須由資訊單位事前與連線單位簽訂契約或協定，限制系統可運作之權限，並明定應遵守之資訊安全規定、程序及應負之責任。

(七)存取控制：

1.登入各作業系統時，依各級人員執行公司規定任務所必要之系統存取權限，由資訊單位系統管理人員設定應賦予權限之帳號與密碼，並於三個月內須更換一次。

2.對離（休）職人員，須取消使用各項資訊資源所有權限，並列入人員離（休）職之必要手續。

3.對公司內外擁有系統存取特別權限之人員，由資訊單位建立使用人員名冊，加強安全控管。

4.各單位之重要資料如需委外建檔者，不論在公司內外執行，應與委外廠商簽訂適當之安全管制合約，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

5.個人筆記型電腦攜入公司使用時，仍須遵守公司制訂之安全管理政策，對於可能造成資通安全的軟體及常駐程式，資訊人員得強制移除，使用者不得拒絕，否則公司有權限制使用者在公司內使用該設備。

6.對於在公司內使用之私人電腦設備或外來電腦設備，基於資安考量，公司有權逕行佈署安全監控套件，以利資訊單位監控可能發生的資安問題。

(八)系統開發與維護：

1.各單位自行開發或委外發展系統，須在系統開發初期階段，即將資訊安全入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

2.對委外廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁資訊單位核發長期性之系統辨識碼及通行密碼。

3.對委外廠商或系統維護人員基於實際作業需要，資訊單位得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。但使用完畢後應立即取消其使用權限。

4.各單位委託廠商建置及維護重要軟硬體設施時，應在各單位系統管理人員與資訊單位人員監督及陪同下始得為之。

(九)永續經營管理：

1.為因應各種人為及天然災害造成業務運作受影響，資訊單位須定期進行資料備份。

2.各單位在發生資訊安全事件時，應立即向權責主管通報，由資訊單位聯繫檢警調單位協助偵查。

3.為保障企業營運秘密安全，資訊單位得對電子資料通訊做必要的監控與資料保存。

(十)電腦報廢管理：

1.電腦報廢時須先通知資訊人員進行報廢檢測，由資訊人員於檢測完成後填寫「資訊設備報廢檢測紀錄」，如確認報廢則將該紀錄以附件方式進行固定資產報廢程序。

2.報廢之零組件中包含內接式或外接式硬碟等儲存裝置時，堪用品整理完成後納入備品管理，唯無論判定為堪用品或報廢品，為避免內部資料外洩皆需由資訊人員進行格式化等資料清除方式，以確保資料完全清除已無法回復或無法讀取。

3.報廢品之廢棄物清運委由資源回收公司處理，或配合總務年度相關計畫統一處理。

(十一)個人資料保護：

1.為避免洩漏個人資料，傳送包含個人資料之電子郵件，資料檔應加密碼保護，密碼需另外通知對方不可使用相同郵件告知密碼。

2.處理個人資料之資訊設備，需設置使用者帳號及密碼，如需離開工作崗位時應登出帳號或螢幕保護鎖定。

3.為避免個人資料被竊取、竄改，儲存個人資料之資訊設備應放置於設有門禁控管之實體安全區域，網路通訊需設置防火牆及防毒軟體，避免有心人士或非授權人員存取。

4.儲存個人資料之電腦或設備如需報廢或轉移他用時，資訊單位應確實刪除該設備所儲存之個人資料檔案。

5.處理個人資料檔案人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員應重置相關系統密碼及使用者帳號識別。

6.為避免資料毀損、滅失，儲存個人資料之電腦主機應建立備援機制。備援儲存裝置報廢請參照電腦報廢管理程序，以確保資料無法讀取及回復。

(十二)內部稽核及其他：

1.資通安全檢查項目，另定「資通安全檢查表」。

2.相關查核記錄應妥善保存。

3.資通安全稽核人員應由具相關專業能力或經適當訓練，並獨立於日常資安工作且能客觀評估者擔任。

五、本辦法經呈董事會通過後實施，修正時亦同。