資訊網路管理辦法

第一章：總　則

1.1 目　的：

為使本企業整體資訊網路之規劃、使用、安全、保密及監控管理等工作有所遵循，並確保整體資訊網路正常運作與資訊傳輸效率，特訂定本管理辦法。

1.2 資訊安全政策：

為確保企業整體的資訊使用安全，及建立可信賴的資訊使用環境，故本企業資訊安全政策如下：

⑴遵守法規要求，普及資安意識。

⑵重視風險管理，保護資料安全。

⑶要求全員參與，追求持續改善。

1.3 適用範圍：

凡本企業各部門之個人電腦、工作站、主機、伺服器、電腦區域網路及電腦主機網路，欲與企業內其他電腦區域網路或企業廣域網路連結成企業整體資訊網路者，均適用本管理辦法。

1.4 管理部門與權責：

⑴總管理處資訊部（以下稱本部）得設專人處理：

A. 全企業廣域資訊網路主幹及網路設備之規劃、設置、測試與驗收。

B. 全企業廣域資訊網路主幹之網路管理與異常排除。

C. 提供網路使用部門技術諮詢及網路規劃服務。

⑵本部各運轉組，其所負責之廠區電腦課得指派專人處理：

A. 各廠區資訊網路主幹及網路設備之規劃、設置、測試與驗收。

B. 各廠區資訊網路之網路管理與異常排除。

C. 網路連結之申請審查。

⑶各公司（總）經理室得指派專人審核各使用部門電腦區域網路設立與連結之需要性。

⑷各使用部門得指派專人管理該部門內區域網路之日常運轉工作及該部門區域網路之異常排除。

第二章：資訊安全管理

2.1 網路安全管理：

網路安全管理包括內部安全管理及防範外部入侵，內部安全管理

包括系統存取權管理(如密碼保護、身份驗證、存取控制)、存取記錄及網路資料傳遞的保密性;防範外部入侵則為防止內部的資訊或資源可能被駭客(Hacker)侵入而遭破壞,企業資訊網路與製程網路、網際網路、非企業內公司、無線網路、遠端連線時,都需在界接的連接點上,建立防火牆(Firewall)機制來阻隔外來的入侵,並考量系統安全需求,評估增設入侵防禦、防毒、網路弱點掃描及安全稽核等防範系統之可行性。

⑴防火牆(Firewall)功能架構建置原則:

A. 供員工上網、電子郵件及網路安全隔離使用之防火牆,採用單層式架構規劃,並以 Juniper、Fortinet、Cisco、Palo Alto 等技術領導廠牌為主。針對原廠已停止支援之防火牆,於維護合約期滿日前一年另購置防火牆替換,汰換下之防火牆做為備機使用,無備機可更換使用之防火牆簽訂 7x24 維護合約,有備機可更換之防火牆不簽訂維護合約。

B. 供電子商務環境使用(如 WWW 網站、FTP 站、電子商務應用)之防火牆,因需防護 Internet 網路駭客入侵及病毒、蠕蟲…等惡意程式攻擊並保護企業內部網路之安全,採用業界較為安全之雙層式防火牆架構,並規劃專屬資料庫網段供應用伺服器存取使用,除以 Juniper、Fortinet、Cisco、Palo Alto 等技術領導廠牌為主外,第一層防火牆及第二層防火牆需為不同廠牌,另為避免任一層單一台防火牆故障影響企業電子商務之營運,擬建置一台防火牆故障,可由另一台防火牆立即接手之 HA 機制,並簽訂 5x8 維護合約。針對原廠已停止支援之防火牆,於維護合約期滿日前一年購置新的防火牆替換,汰換下之防火牆擬做為其他員工上網及安全隔離環境之周轉品使用。

⑵檔案安全:

A. 透過網路設備提供之存取控制功能:

a. 位址表格(Address Table)限制法

b. 通訊埠表格(Port Table)限制法

c. 橋接過濾法(Bridge Filtering)達到防止非法擷取、竄改檔案的目的。B. 各公司總經理室於使用部門申請網路連線時,應確實審核「網路連線申請單」上之 "用途說明" 欄位所示之必要性與妥適性。

C. 各使用部門應指定專人,對該部門網路檔案伺服器之檔案,自行設定資料擷取權限,防止不當使用電腦檔案,使用者

密碼需包含文數字及符號，不可使用字典查得到的單字及與身份相關資料，並定期更改與重複使用相同密碼，及限定最短長度與啟動連線記錄。

⑶備援處理：

A.資料備份：

使用燒錄機或磁帶機處理網管資料檔案的備份工作，以備硬體故障時回復之用。

B.網路替代線路：

網路主幹線路部份，應有不同迴路備援的規劃與設計，以便線路中斷時，有替代通路可使用。

⑷網路設備安全控管機制：

A.網路設備均不得保留出廠時之預設密碼，且登入帳號之命名不應與職務功能的描述有關(例如：Admin、root、system)。

B.所有網路設備密碼由控管專人每三個月變更一次，不可重複使用，長度需大於八個字元(含)以上，包含文數字及符號，且不能與帳號相同，帳號長度需大於六個字元(含)以上。

C.網路設備不需要使用之功能及未使用之連接埠均需關閉，並　至少保留 3 個連接埠備用。

D.網路設備機櫃需將機櫃輪子及下方腳架固定避免地震時滑動移位。

E.T1 多工機、路由器及網路中樞器等重要網路設備之系統記錄檔除設備內有記錄外，另傳送一份至系統記錄檔收集電腦集中備存，以保護網路設備之系統記錄檔避免被修改或刪除，並每日稽核記錄內容。

F.路由器及網路中樞器等重要網路設備應啟動 broadcast、multicast、icmp、arp、unknow-unicast、cpu 等使用門檻限制，以確保網路設備之穩定性。

G.網路設備之 STP(Spanning Tree Protocol)功能是在防止網路設備互連時 Loop 的發生，網路中樞器及交換式集線器連接主機或伺服器(非網路設備)之埠，應將 STP 功能關閉，避免誤判造成異常。

H.網路設備之預設 community 應取消，並限制可以 SNMP 網管協定存取之機台 IP 位址及存取權限。

I.無線網路基地台應取消 SSID 廣播，並鎖定電腦網路卡 MAC 位址，避免非法電腦連線，並應啟動 WPA 等無線加密協定，避免經由無線傳輸之資料被不當擷取，並需使用防火牆進

行隔離，並對進入企業內部網路使用資源的行為進行控管。

J. 應設置防火牆建立機制管制上網，以維護網路安全，如有異常則自動通知資訊人員，資訊人員並每日確認有無異常狀況，如有異常則由資訊人員確認並排除。

K. 防火牆之系統、連線及資安等記錄均需保存三個月以上，防火牆設定異動時，系統需能主動通知網路管理者異動內容。

L. 防火牆政策(Policy)應每年定期檢視一次。

⑸伺服器負載平衡機制：

A. 為提昇電腦作業穩定性及安全性，針對需要網路分流及作業分工功能之應用作業伺服器建置硬體式的伺服器負載平衡器。

B. 提供企業內電子郵件、員工上網、多國語言版 ERP、圖文管理系統及網路教學等作業的伺服器負載平衡機制。

C. 作業連線總人數達 700 人(含)以上的廠區規劃二台伺服器負載平衡器(二組線上互為備援)，並簽訂 5x8 維護合約。

D. 廠區僅建置一台伺服器負載平衡器者，則需要簽訂 7x24 維護合約。

⑹遠端連線維護管理：

A. 企業員工需透過網際網路連線進入企業網路維護或使用企業資訊系統資源時，需以辦公室自動化系統填寫「VPN 申請單」後，再透過發放之企業電子憑證及 AD 帳號進行驗證後，方可連線使用。

B. 企業資訊系統有開放維護廠商連線維護需求時，需以「管理制度改善意見反應單」申請開放，網路設備安全政策需鎖定維護廠商連線之 IP 位址。企業員工使用 VPN 連線作業時需保留連線記錄及畫面，並每日將連線記錄彙總呈送單位主管查核確認連線原因，連線記錄應保存三個月以上。

C. 企業員工使用 VPN 連線需管制檔案傳送功能，以避免企業資料檔案外流。

2.2 資訊系統安全管理：

⑴應依據登入電腦網域的人員帳號，設定登入人員使用電腦資源的權限範圍，其權限範圍包含使用者的上網、郵件帳號、ERP 系統、檔案伺服器中相關資訊的取得及權限等進行管理。

⑵應依據「ERP 電腦作業登入及權限控管電腦作業」之規定，

ERP 系統依據登入 ERP 系統的使用者帳號，設定 ERP 內各項作業模組之使用權限及 ERP 資料之新增、修改、刪除的權限等進行管理。使用者進入 ERP 系統及修改 ERP 系統內之重要資料皆留有記錄，以供事後查證。

⑶針對存放機密性及敏感性資料之主機或伺服器，除作業系統既有的安全設定外，對於敏感性資料，應透過 ERP 系統或表單來管制存取權限。

⑷安裝主機及伺服器的作業系統或應用程式時，不需要使用之功能不得安裝，另安裝完成後，需將不需要使用之服務關閉。

⑸主機及伺服器的系統管理員帳號(如 Administrator、Root)應設定密碼，並以紙本彌封交由專人保管，供緊急狀況時使用，且使用後應立即變更密碼，並再次重新彌封交由專人保管。

⑹共享文件夾應依部門或使用者權限設定權限管理，各共享文件夾的使用權限均應填寫「部門內便簽」提出申請。

⑺具機密性及敏感性資料或文件，不得存放在對外開放的資訊系統中。開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

⑻離職及調職人員，資訊部人員應依人事規定作業，針對離職人員，系統於離職當日自動刪除各項權限和帳號；另針對調職人員，系統於人員調職後自動以辦公室自動化系統表單通知原單位主管，審核是否刪除或保留該人員之各項權限和帳號。

⑼辦公室自動化系統超過 90 天未使用的使用者帳號，系統應主動以「NOTES 帳號三個月未使用確認提示表」通知該使用者的主管，以確認要保留或註銷該使用者帳號。

⑽每日應執行 ERP、辦公室自動化系統及電子商務系統備份，備份於磁帶中，並建置系統異地備援機制，每日夜間於台北、麥寮兩個電腦中心，進行系統資料的異地備援。

⑾機房應設置門禁刷卡管制並記錄，以維護電腦設備安全，相關人員應填寫「電腦機房人員進出申請單」並經申請核可後，才能以員工識別證刷卡進入，非經許可不得擅自進入。廠商維修人員欲進入電腦機房，應由資訊部相關人員陪同，並於「機房門禁管制記錄表」登記事由及進出時間，進出機房皆應留有記錄，以利事後追蹤。

⑿應設置入侵偵測系統，監測 DMZ 網段的主機或伺服器是否遭受網路攻擊，並即時通知系統管理者進行處理。

⒀應設置網站滲透測試工具，模擬各種駭客攻擊手法，定期檢測網站應用程式的安全性漏洞。

⒁應設置系統及網路弱點掃描系統，定期掃描資訊系統是否存在系統及網路上的弱點，並即時通知系統管理者進行處理。

⒂公司內部人員若發生侵犯系統等違規行為，則依「人事管理規則」進行懲處。若廠商與外部人員發生侵犯系統等違規行為，則依「出入廠管理規則」、「廠商違反出入廠管理規定扣款標準」進行處分，如涉及不法者則逕予報警移送法辦。

⒃每年針對員工，應由資訊部門於六月底前編訂資訊安全訓練教材，並由各公司相關部門排定企業知識庫指定閱讀文件作業及追蹤、記錄執行情形，以確保員工皆已完成資訊安全訓練

2.3 個人電腦安全管理：

⑴個人電腦及 ERP 系統之登入密碼長度應為 6 碼以上，密碼可包含英文、數字及特殊符號，且英文區分大小寫，有效期為 90 天，且新設定之密碼不可與前 4 次相同，另針對員工新申請的帳號，需於員工首次登入時，強制要求變更密碼。

⑵使用者登入網域時，輸入密碼錯誤達 30 次後，系統將主動鎖定登入使用者的帳號,被鎖定的使用者帳號系統會於15分鐘後自動解除鎖定，未解除鎖定前，將無法登入或使用系統功能。

⑶個人電腦之本機系統管理員帳號(Administrator)應設定密碼並停用，員工使用電腦時，需使用網域帳號登入。

⑷應設置 Windows 安全性更新為自動更新，統一由 SCCM 系統派送 Windows 安全性更新檔案，修補已知漏洞。

⑸各電腦皆應安裝防毒軟體，並設定為自動更新病毒碼及定期掃描(每週執行一次快速掃描、每月執行一次完整掃描)，防止遭受電腦病毒感染，遇有多台電腦中毒之情況，維護廠商應主動發送郵件通知資訊部人員，以進行後續病毒的清除及過濾。

⑹安裝於電腦上之套裝軟體，應為擁有正式授權之合法軟體。

⑺禁止於電腦上使用未經核准之軟體或私自複製套裝軟體使用，避免遭不明程式植入後門或間諜程式。

⑻電腦系統應設定螢幕保護功能，閒置 10 分鐘即啟動，解除螢幕保護應輸入密碼，以防止非該電腦使用者盜用該電腦。

⑼「製程電腦控制室的個人電腦」及「電腦機房的個人電腦」均需設定封鎖 USB PORT。各電腦系統的 USB PORT 皆可依各公司的資訊安全需求進行設定 (唯讀或完全封鎖)，以防止透過 USB 裝置存取公司電子資料，若需使用應填寫「管理制度改善意見反應單」提出申請。

⑽個人電腦中若有具機密性及敏感性的重要檔案或資料夾，企業同仁應透過加密軟體進一步設定密碼保護，以避免資料外洩。

⑾個人電腦或伺服器等資訊設備報廢減損時，應由保管人清空電腦硬碟資料，以避免資料外洩。

⑿報廢電腦設備硬碟繳回處理方式：

A. 留用硬碟：需使用硬碟抹除機進行資料複寫抹除後，轉維修拆解零組件列管供轉用。

B. 報廢硬碟：需使用硬碟破壞機於固態硬碟最少四顆晶片，或磁盤硬碟之碟盤相對位置，執行至少四個打洞破壞後，才可進行後續報廢程序。

2.4 上網安全管理：

⑴應透過上網代理伺服器管制員工上網，並設有黑名單，針對具論壇性質的社群網站、娛樂性網站、博奕網站、情色網站及內含惡意程式的網站，進行封鎖及管制，以防員工存取不當網站。

⑵上網代理伺服器應保留最近 90 天的員工上網記錄。

2.5 郵件安全管理：

⑴為避免同仁收送的電子郵件中含有電腦病毒、木馬程式及間諜軟體等惡意程式，應針對可執行檔、系統參數檔、系統設定檔等附加檔案格式(詳如附表四)，加以管制禁止傳送接收。

⑵針對 Internet 寄送到企業內的電子郵件，應透過郵件防毒軟體進行掃毒，並針對垃圾郵件加以過濾及防堵。

⑶針對同仁透過企業電子郵件伺服器寄送到企業外的電子郵件，應自動加註警語，以提醒收件者對於電子郵件內容予以保密。

⑷應建置郵件歸檔系統，針對同仁與企業外相互寄送的郵件進行完整的備存，並保留 5 年。

⑸為符合「個人資料保護法」之規定，防止違反公司政策的個人資料透過電子郵件或 Web Mail 外寄(如 Gmail 及 Yahoo Mail 等)，應建置 DLP 防範資料外洩系統，針對同仁寄送至企業外的郵件是否含有大量個資進行控管及完整的備存，並保留 5 年，同時管制同仁要寄送大量個資的郵件，需填寫「大量個資外寄郵件申請單」提出申請，經核准後再透過企業的電子郵件系統傳送，不允許使用非本企業的電子郵件系統(如 Gmail 及 Yahoo Mail 等)傳送。

2.6 資訊安全事件管理：

⑴當發生重大資通安全事件時，發生部門應立即向資訊部門通報
(屬 ERP 及辦公室自動化系統應向總管理處資訊部通報，屬製程系統應向各製程系統管理部門通報)。

⑵資訊部門收到發生部門的通報後，應以辦公室自動化系統填寫「資安事件通報單」，將事件的發生地點、時間、類別、

發生經過、處理情形及結果等扼要敘述傳簽。

⑶資訊部門應與發生部門檢討事件發生原因及改善對策，並審視現有的各項系統是否存在相同的資安問題，以避免再次發生。

⑷資訊部門應就曾經發生過的資通安全事件，檢討修訂資訊安全訓練教材，或發佈資通安全公告，提升員工的資安意識。