OOOO 公司

通訊與作業管理作業程序

ISMS-B-006

版本 1.0

中華民國 105 年 MM 月 DD 日

1. 目的

OO 公司（以下簡稱本公司）為確保遵循通訊與操作作業之相關安全管理規定，以及確保正確與安全的操作資訊處理設施以降低人為錯誤的風險。。

2. 範圍

適用於本公司資訊安全管理制度範圍內之所有任何形式的資訊傳輸、通訊及處理設施操作等活動。

3. 權責

3.1 資訊設備與系統負責人

資訊設備與系統維護、管理、備份規劃與回復測試等作業。

3.2 防毒系統負責人

3.2.1 定期確認病毒碼為最新版本。

3.2.2 追蹤主機及個人電腦是否安裝最新病毒碼。

3.2.3 處理電腦病毒問題。

3.3 備份系統負責人

3.3.1 規劃、排程與控管備份作業及相關備份軟硬體設備之購置。

3.3.2 提供備份服務並協助確認備份作業內容及還原測試。

3.3.3 執行備份作業及檢查備份資料。

3.3.4 備份作業異常處理。

3.4 網路安全負責人

應用適當工具或方法以確保網路正常運作。

4. 定義

4.1 資訊設備

指電腦設備(如筆記型電腦、個人電腦、大型主機)、資訊週邊設備(如印表機、磁帶機、條碼機)、網路通訊設備(如路由器、交換器、傳真機)、電信通訊設備(如交換機、電話) 等。

4.2 可攜式設備

指可攜帶且具備運算處理、資料擷取功能或儲存媒體之電子設備，包括筆記型電腦、PDA、照相機、攝影機、燒錄器、智慧型手機、電子通訊設備、外接式(含抽取式、移動式)硬碟、外接式光碟燒錄機、USB 相關設施、快閃存取記憶體(卡)、隨身碟、數位相機記憶卡及 MP3 player 等。

4.3 系統

泛指自行開發或套裝應用系統。

4.4 媒體

資料儲存媒介，例如：紙本文件、電腦媒體（磁片、磁帶、記憶卡與光碟片）。

5. **作業內容**

5.1 通訊與作業安全管理

5.1.1 維運作業之專案管理安全要求

5.1.1.1. 應將資訊安全要求整合納入專案需求與其管理作業，以確保將識別並處理資訊安全風險作為專案之一部份。例如：核心業務流程、資訊系統、設施管理與其他支援流程之維運作業。

5.1.1.2. 應將資訊安全政策要求或資訊安全目標，依專案特性適度的納入專案管理目標內。

5.1.1.3. 應對專案作業人員，界定其角色與配置其相關之資訊安全責任。

5.1.2 系統文件管理

5.1.2.1. 原廠提供之各項資訊設備與系統，應依據該系統文件及應用特性要求，以供系統管理者與使用者正確操作與使用資訊設備與系統。

5.1.2.2. 資訊設備與系統之系統文件包含系統管理文件、系統使用文件等等，系統文件應標示其版次與更新日期，並依據【資訊資產管理作業程序】分級處置原則，提供授權人員使用。

5.1.2.3. 應用系統之系統文件管理，依據【資訊系統獲取、開發及維護管理作業程序】辦理。

5.1.3 變更管理

5.1.3.1. 進行資訊設備安裝、變更與維護作業，應於「資訊設備安裝維護申請紀錄單」填寫工作紀錄，並經權責主管同意後再進行變更。變更執行前應對各應用系統或服務所可能導致之影響進行評估，並視需要進行備份。

5.1.3.2. 若為緊急變更，可由承辦人先口頭告知權責主管，經核可後進行變更，變更完成後補填「資訊設備安裝維護申請紀錄單」。

5.1.3.3. 進行資訊設備安裝、變更與維護作業，如異動資訊機房機櫃配置，應更新「資訊機房設備資訊表」。

5.1.4 職責區隔管理

5.1.4.1. 資訊機房維運相關人員其職務，須考量適當的權責區隔，各項工作應訂定工作職務代理人。

5.1.4.2. 權責主管指派人員擔任適當職務時，考量職務權責區分與獨立審查要求，記錄於「職務權責區分表」，對兼任

職務所產生之風險，宜有適當監控與審查機制。

5.1.5 資訊系統服務發展與測試管理

5.1.5.1. 發展、測試環境應與線上環境區隔，資訊系統服務發展與測試作業管理，依據【資訊系統獲取、開發及維護管理作業程序】辦理。

5.1.5.2. 資訊機房維運人員確認申請資訊系統服務發展與測試作業相關表單已由權責主管核准並且備妥相關佐證資訊後，依據申請項目配合其作業需求。

5.1.6 委外服務監控與管理

5.1.6.1. 依據【資訊安全組織管理作業程序】與【資訊系統獲取、開發及維護管理作業程序】及【業務委外作業程序】辦理。

5.2 系統容量與驗收管理

5.2.1 系統容量管理

5.2.1.1. 機房人員應對資訊系統、資訊設備之資源使用狀況進行檢查，並依據【實體與環境安全管理作業程序】紀錄於之「資訊機房管理紀錄表」中。

5.2.1.2. 依據現行資訊設備與系統之資源使用狀況及資訊系統資源容量之需求，適時進行系統調整與系統容量擴充之前瞻性的規劃，以獲得必要之系統作業資源。

5.2.1.3. 於評估與規劃系統容量擴充之可行性時，需注意廠商硬體設備及軟體系統版本更新、使用與維護之生命週期，及硬軟體系統運作相容性之管理。

5.2.2 資訊系統驗收管理，資訊設備變動，應確保其符合資訊安全管理制度相關規範要求，應用系統異動應依據【資訊系統獲取、開發及維護管理作業程序】辦理。

5.3 防範惡意碼與行動碼管理

5.3.1 作業系統均需安裝防毒軟體，且病毒碼應自動更新至最新版本；未安裝防毒軟體應輔以其他控制。

5.3.2 安裝防毒軟體後應啟動即時病毒防範機制，並依排程週期執行完整掃描。

5.3.3 應避免開啟來路不明及與業務無關之電子郵件，以避免惡意程式或病毒感染；同時郵件收發軟體應設定停用郵件自動預覽功能與「自動開啟下一封」之功能，關閉或適當限制電子郵件軟體執行 ActiveX、Java applets、Active Scripting 之功能。

5.3.4 如發生電腦病毒感染情形，應需立即採取相關措施，防止病毒繼續擴散，並依據【資訊安全事故管理作業程序】通報處

理。

5.3.5 防毒系統負責人應定期檢查防毒軟體控制台病毒碼更新與病毒偵測紀錄，並彙整「資訊安全事故報告單」中病毒處理統計供資訊安全推動組備查，並依據資訊安全趨勢定期宣導，以提昇使用者資訊安全認知。

5.3.6 如需使用外來的可攜式設備、媒體、檔案或電腦媒體，應確認未遭受病毒感染。

5.3.7 使用瀏覽器瀏覽網站時，將瀏覽器安全性設定為「中高」以上，以限制執行非信任網站之行動碼並對下載的每一檔案做病毒或惡意內容的掃描，以防範惡意行動程式碼(Mobile Code)，並在確認安全情況下，才可執行 ActiveX 或主動式程式之執行。

5.4 備份管理

5.4.1 備份安全管理

5.4.1.1. 備份作業應依據資訊設備或系統需求，擬定「備份媒體管理表」，執行備份作業。

5.4.1.2. 備份媒體保管方式應視其資料內容依據【資訊資產管理作業程序】分級，按其機密等級進行控管，並列入「備份媒體管理表」。

5.4.1.3. 資料備份應依各應用系統資料安全要求，考慮是否異地存放，以增加資料安全性。

5.4.2 備份作業之異常處理

備份作業過程中發生異常狀況，備份系統負責人應通知資訊設備與系統負責人，並依據【實體與環境安全管理作業程序】填寫「資訊機房管理紀錄表」，備份作業規劃人員應將備份異常原因、處理方法及結果，交由權責主管覆核。

5.4.3 備份資料復原測試

應定期執行備份與回復測試或依據【業務持續管理作業程序】所展開的業務持續計畫，規劃備份資料復原測試作業。

5.5 伺服器管理

5.5.1 伺服器相關設備應放置於機架或安全區域內，並適時或依廠商建議安裝相關防護軟體，如防毒軟體，隨時更新病毒碼。

5.5.2 應分離區隔開發測試及正式環境，以降低正式作業因意外造成損害或中斷之機率。

5.5.3 伺服器之屬性為檔案伺服器者，應依分享資料夾用途賦予適當的權限。

5.5.4 應定期執行設備維護作業，留下相關紀錄並記錄於機房工作日誌。

5.5.5 伺服器相關設備(如硬碟、CPU、記憶體與通訊流量等)之使用量須加以監控，若超出警戒值時，管理人員應立即處理，並記錄於機房工作日誌。

5.5.6 重要設備或系統之日誌紀錄(Log)應至少每週查看，結果填寫並記錄於機房工作日誌。

5.5.7 重要設備或系統應定期執行備份。

5.5.8 應識別資訊系統可用性之營運要求。若無法使用現有系統架構保證可用性，應考慮複式組件或架構(redundant)。若可行，應測試複式資訊系統以確保從組件到另一組件之失敗接管如預期之有用並達到效果。

5.6 網路通訊設備管理

5.6.1 網路通訊設備須置於機房或安全場所，非經主管授權不得任意移動設備或更改設定。

5.6.2 網路通訊設備系統登入被拒絕後，應立即中斷登入程序，結束連線，並不得給予任何的協助訊息與畫面。

5.6.3 網路通訊設備安裝完成後，應立即刪除系統預設帳號或修正廠商預設密碼。

5.6.4 網路通訊設備系統登入方式，應依據 【存取控制管理作業程序】之相關規範進行管理，以防止網路監聽、竊取帳號密碼。

5.6.5 重要網路通訊設備應啟動系統紀錄（Log），至少記錄登入、登出之成功或失敗紀錄；網路通訊設備系統紀錄應定期檢視與備份。

5.6.6 應識別營運資訊系統之可用性是否符合營運作業要求。若無法使用現有系統架構保證可用性，應考慮複式組件或架構(redundant)。若可行，應測試複式資訊系統以確保從組件到另一組件之失敗接管如預期之有用並達到效果。

5.7 可攜式媒體及行動裝置設備管理

5.7.1 應依據【存取控制管理作業程序】及本程序之規範使用可攜式媒體或行動裝置設備。

5.7.2 因需求而需攜入可攜式媒體或行動裝置設備至機房或敏感區域內使用時，應先經單位主管核准後方可攜入使用。

5.7.3 機房內使用可攜式媒體或行動裝置設備儲存、複製或傳遞資料時，應切實遵守相關法令、法規及資訊安全管理相關規定。

5.7.4 存放於可攜式媒體或行動裝置設備之檔案，應經壓縮（可使用 winzip、winrar、7-zip、ultimate zip 等軟體）並設密碼或檔案加密之保護，並於使用完畢後立即刪除，以避免資料外洩。

5.7.5 如需使用外來的行動裝置設備或可攜式媒體之檔案，應先使用防毒軟體掃描可攜式媒體內儲存之資料，確認其未遭受病毒感染後，方可使用。

5.8 媒體安全管理

5.8.1 媒體之使用、傳遞與報廢，應依其內含資訊等級，遵循【資訊資產管理作業程序】分級處置原則，進行標示與處理。

5.8.2 媒體若需攜出時，遵循【資訊資產管理作業程序】分級處置原則，進行適當保護，以保護敏感資訊避免未經授權的揭露、修改與複製。

5.8.3 媒體交換宜使用可靠的運輸工具或快遞送服務。

5.9 私密金鑰之管理：

5.9.1 私密金鑰應有明確的啟動與止動管理，並於可用期間，保護其不被修改、遺失和破壞。

5.9.2 私密金鑰之使用與存取，應限於私密金鑰之管理者，不可由其他人員任意存取。

5.9.3 私密金鑰，應指定管理員專責保管並鎖於安全之處所。

5.9.4 對於私密金鑰之使用、啟動、止動及備份，皆應留存相關之稽核紀錄。

5.10 網路安全管理

5.10.1 網路服務安全管理

5.10.1.1. 本公司只開放必須的網路服務功能與通訊協定，如需異動應依據【存取控制管理作業程序】辦理。

5.10.1.2. 為確保網際網路的服務持續暢通，本公司網路與外界網路的連接，應建立備援線路或服務持續協議，並確保備援線路受到安全管控。

5.10.2 網路使用者安全管理

5.10.2.1. 需經授權並賦予相關存取權限後，始得使用網路資源。

5.10.2.2. 禁止以任何儀器設備或軟體工具竊聽網路上的通訊。

5.10.2.3. 不得以任何手段蓄意干擾或妨害網路系統的正常運作。

5.10.2.4. 禁止濫用網路系統，若影響網路正常運作者，得暫停其使用權利。

5.10.3 網路入侵偵測/防禦安全管理

5.10.3.1. 應於網路重要區段或是節點，佈署網路入侵偵測/防禦系統，進行入侵偵測與防禦。

5.10.3.2. 應配合資訊安全政策及規定，隨時檢討及調整網路入侵偵測/防禦系統的設定，以反應最新的狀況。

5.10.3.3. 如發現疑似網路入侵情形，依據【資訊安全事故管理

作業程序】辦理。

5.10.4 防火牆管理原則

5.10.4.1. 網路應建置防火牆以連接 Internet，保障網路主機及內部使用者之網路安全，重要網路服務主機群應以防火牆連接網路，限制存取服務。

5.10.4.2. 防火牆規則應以正面表列，開放對外服務通訊埠，並避免不當範圍之群組設定，包含連線來源、目標位址與通訊協定。

5.10.4.3. 申請網路服務開放應填寫「資訊設備安裝維護申請紀錄單」提出異動需求，網路安全負責人須於權責主管核可後方可執行相關異動作業。

5.10.4.4. 防火牆配置與異動時應予以紀錄，建立或更改安全規則時，應對規則加註識別與更新註釋並保留設備之備份檔為最新狀態，異動規則前應測試推演以確認可行性，並考量是否可與其他規則整併。

5.10.4.5. 為求落實安全管理，於防火牆安全規則建置後，應每半年由網路安全負責人、權責主管會同相關人員審查規則適用性，並予以檢討修正，避免因時間或業務變更而不符現狀。

5.11 資訊交換管理

5.11.1 資料取得

5.11.1.1. 資訊單位向外單位申請資料，應經過權責主管同意，以請辦單或公文方式向外單位提出申請。

5.11.1.2. 資訊單位資料取得後，應依據【資訊資產管理作業程序】妥善處理，並僅得使用於申請目的之範圍，禁止移作他用。

5.11.2 資料提供

5.11.2.1. 外單位向資訊單位提出資料需求時，原則應填寫「資料申請單」。

5.11.2.2. 資訊單位提供資料時，應依據【資訊資產管理作業程序】辦理。

5.11.3 電子通訊管理

5.11.3.1. 使用網路通訊服務時，依據【資訊資產管理作業程序】不同等級的資訊類資訊資產控管要求，進行傳遞。

5.11.3.2. 禁止使用網路通訊服務傳遞任何違法及違反本公司規定之資訊。

5.11.4 營運資訊系統

營運資訊系統資料相互流通時應保護，避免非授權人員取

得機密性資料，依據【資訊資產管理作業程序】與【存取控制管理作業程序】對不同等級的資訊建立存取控制管理原則，並據以執行。

5.12 網頁資訊管理

5.12.1 中英文網站公告事項變更

5.12.1.1. 中英文網站網頁內容如需變更，如不牽涉程式修改，由申請業務單位填寫資訊系統需求申請單，向本公司提出申請，經權責主管核准後，由上架人員進行網頁內容之新增或修改。

5.12.1.2. 中英文網站網頁內容如需變更，如牽涉程式修改，應依據【資訊系統獲取、開發及維護管理作業程序】辦理。

5.12.2 公司內網路公告事項變更

5.12.2.1. 公司內網路內容如需變更，如不牽涉程式修改，由申請業務單位填寫資訊系統需求申請單向公司資訊單位提出申請，經權責主管核准後，由承辦人指派上架人員進行網頁內容之新增或修改。

5.12.2.2. 公司內網路內容如需變更，如牽涉程式修改，應依據【資訊系統獲取、開發及維護管理作業程序】辦理。

5.13 監控管理

5.13.1 紀錄管理

5.13.1.1. 資訊設備與系統若提供資訊存取、管理者與操作者稽核紀錄功能且具有追蹤分析價值，在不影響正常運作效能之前提下，應予以啟動並定期予以審查。

5.13.1.2. 資訊設備與系統之紀錄保留至少三個月，若無法線上保存，則將紀錄匯出存檔備查。

5.13.2 紀錄保護

應監控紀錄檔容量，以避免紀錄檔儲存空間不足，導致無法記錄事件或覆蓋以往紀錄。須留存之紀錄應以唯讀方式存放。

5.13.3 紀錄審查

5.13.3.1. 相關權責主管需定期審查系統紀錄（例如系統資源使用狀態、系統漏洞與修補程式安裝情形）。

5.13.3.2. 針對錯誤日誌應分析原因與釐清權責人員，若造成資訊安全事件，則依據【資訊安全事故管理作業程序】通報。

5.13.4 應建置對時機制，所有資訊設備(伺服器主機、網路設備、電信設備及個人電腦等資訊資產)應定期至少每月與對時

主機(Time server)進行時鐘同步更新，以確保系統時間的一致性。若有其他設備，無法與對時主機(Time server)進行時鐘同步更新時，應定期(至少每月一次) 進行人工時鐘同步更新，以確保系統時間的一致性。

6. 相關資料

6.1【資訊資產管理作業程序】

6.2【實體與環境安全管理作業程序】

6.3【資訊系統獲取、開發及維護管理作業程序】

6.4【資訊安全組織管理作業程序】

6.5【資訊安全事故管理作業程序】

6.6【業務委外作業程序】

7. 附件

7.1 資訊設備安裝維護申請紀錄單

7.2 職務權責區分表

7.3 備份媒體管理表

7.4 資料申請單