OOOO 公司

存取控制管理作業程序

ISMS-B-007

版本 1.0

中華民國 105 年 MM 月 DD 日

文件編號	ISMS-B-007	存取控制管理作業程序	文件類別	限閱
版　　次	V1.0		發布日期	105/MM/DD

1. 目的

OO 公司（以下簡稱本公司）為確保確保對資訊資產的存取權限經適當的授權、分配及維護，以防止不當存取。

2. 範圍

適用於本公司所有資訊安全制度範圍內設備與提供服務所需之內部作業相關，資訊實體設備、系統與網路等資訊資產，包括作業平台、資料庫、應用系統、企業網路、遠距存取服務、門禁服務、交換機及各種網路設備，如：路由器、防火牆及交換器等之帳號、權限管理。。

3. 權責

3.1 資訊設備與系統管理者

3.1.1 負責資訊設備與系統管理作業。

3.1.2 定期審查資訊設備與系統使用者存取權限。

3.2 權責主管

3.2.1 指派人員職務。

3.2.2 使用者帳號申請及註銷之審查。

3.3 系統使用者

3.3.1 若需使用系統管理權限時，依帳號申請要求執行申請作業。

3.3.2 妥善使用系統。

4. 定義

無

5. 作業內容

5.1 存取控制管理原則

5.1.1 資訊資產之使用須經授權，資訊資產存取權限之設定並應以作業所需知之最小權限為原則或採原則禁止，例外開放之原則，例外開放之帳號存取權限須另行列管並留存相關紀錄。

5.1.2 對於具有相同權限之使用者，應建立適當之角色或群組，並對該角色或群組設定存取權限。

5.2 使用者存取管理

5.2.1 系統使用者帳號管理

5.2.1.1. 各內部使用之應用系統，應由本公司資訊單位、承辦組或委外廠商依系統特性設計應用系統服務申請單，格式可參考「系統服務申請單」，內容至少應含申請日期、申請單位、申請人員、聯絡電話、E-MAIL 帳號、異動原因、申請角色或權限及簽核欄等，並以本公司現有之

服務申請單為優先。

5.2.1.2. 各應用系統使用者（含內部員工、合作廠商）應視業務需求，以「系統服務申請單」申請適當角色或權限，並經該單位主管依據「應用系統角色對應表」審核後，交由應用系統管理者建置相關資料，職務異動之權限調整亦同，人員離職之帳號移除作業，依據【人力資源安全管理作業程序】規範辦理。使用者帳號申請及註銷應保留紀錄。

5.2.1.3. 避免使用共用帳號，如需使用共用帳號，須經權責主管同意。

5.2.1.4. 通行碼設定時系統應主動辨識，其長度應為 8 碼（含 8 碼）以上，且必須包含數字、英文字母、大小寫與特殊字元之組合。

5.2.1.5. 使用者通行碼如由系統或應用系統管理者預設，應告知使用者於首次使用系統時進行變更，或由系統強制執行。

5.2.1.6. 通行碼更改時新通行碼不得與前兩次重複，且通行碼應至少每三個月更換一次。

5.2.2 系統管理者帳號管理

5.2.2.1. 本公司內部管理用途之應用系統帳號，除應用程式使用及特殊需求之帳號外，通行碼應至少每三個月更換一次。

5.2.2.2. 若需使用應用系統管理員帳號（或高作業權限帳號）的需求，應填寫「應用系統維護紀錄表」或「資訊設備安裝維護申請紀錄單」，經權責主管核可後始得開放。

5.2.2.3. 若因應作業需求，須由委外廠商持有系統管理員帳號，系統承辦人應考量操作系統之安全需求，對委外廠商執行之作業採取適當審核與確認。

5.2.3 權限審查

5.2.3.1. 權責主管應管制系統管理人員帳號數量，僅授予合法管理者及代理人，並每半年定期審查，註銷不適切之權限。

5.2.3.2. 置於本公司管理維護之各系統需備有列舉系統使用者帳號與權限報表功能，並定期提供現行系統中之使用者帳號與權限清冊，以供各使用者單位確認帳號權限之適當性，使用者帳號與權限清冊格式可參考「系統使用者帳號清單」 。

5.2.3.3. 置於本公司管理維護之各系統，若無法提供列舉系統使用者帳號與權限報表功能，應由帳號申請審核單位自行

確認帳號權限之適當性。

5.3 使用者責任

5.3.1 使用者之通行碼應妥善保管以避免他人知悉。

5.3.2 放置於工作區域之無人看管設備，應依據工作區域特性，採取實體妥善安置或上鎖，設置適當系統存取控制，並標示管理權責單位與適當警語。

5.3.3 個人電腦或筆記型電腦於下班後，若無使用應確實關機；離開座位時，應將電腦鎖定或設定螢幕保護程式，並啟動密碼以保護電腦資料安全，啟動螢幕保護程式的時間設定不應超過 15 分鐘。

5.3.4 一般事務機器管理

5.3.4.1. 傳真機使用管理

5.3.4.1.1. 內部使用等級以上之資料以傳真機傳送時，於傳送前及傳送完成後，均應通知資料接收單位，並妥善保管原始資料。

5.3.4.1.2. 請對方傳真內部使用(含)以上有關資料時，需與對方聯繫，傳真接收後立即取走。

5.3.4.1.3. 傳送或接收完成之文件，需依據【資訊資產管理作業程序】進行後續處理。

5.3.4.1.4. 未註明收件人員之傳真資料，若無人認領則由各設備管理者於次一工作日執行銷毀。

5.3.4.1.5. 接收之傳真明細盡可能啓動記錄功能，若需要記錄時，則向各設備管理者提出申請調閱。

5.3.4.2. 印表機、影印機使用管理

5.3.4.2.1. 列印、影印資料後，應立即將原始文件及相關資料取走。

5.3.4.2.2. 屬內部使用(含)以上的資料，禁止當回收紙重覆使用。

5.3.4.2.3. 無人領取之列印、影印資料，若無人認領則由該設備管理者於次一工作日執行銷毀。

5.3.5 使用者離開電腦設備時，應退出使用環境或電腦螢幕鎖定，以確保資料之安全。若超過 15 分鐘未使用電腦，需設定螢幕通行碼保護或強制登出措施。

5.3.6 使用者離開辦公區域時作業區域存放資料，依據【資訊資產管理作業程序】規範辦理。

5.3.7 密碼管理

5.3.7.1. 電腦及資訊設備之密碼長度應為 8 碼(含)以上，密碼應以包含英文大寫、小寫、數字及特殊符號等之強式密碼

為原則。

5.3.7.2. 員工及廠商應負保護密碼之責，應避免將密碼記錄在書面上或張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。

5.3.7.3. 帳號及密碼，嚴禁轉知他人，若已為他人知悉者應立即更新。

5.3.7.4. 避免使用與個人有關資料（如生日、身份證字號、單位簡稱、電話號碼等）做為密碼。

5.3.7.5. 禁止盜用他人帳號及密碼使用網路資源，或將個人帳號及密碼借予他人使用。

5.3.8 電子郵件使用規範

5.3.8.1. 不開啟或轉寄來路不明的電子郵件及其附件檔案或連結。

5.3.8.2. 不開啟來路不明的圖檔及執行檔。

5.3.8.3. 不利用電子郵件寄送未加密之機敏資料。

5.3.8.4. 未經授權，禁止對外發送機敏文件。

5.3.8.5. 禁止散播或轉發不當消息之電子郵件。

5.3.8.6. 禁止互傳夾帶大量（外部傳遞不得超過 10M /內部傳遞不得超過 10M）附加檔案之電子郵件。

5.3.8.7. 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。

5.3.9 電腦防毒及惡意軟體侵入保護

5.3.9.1. 電腦應安裝防毒軟體，使用人或管理者應注意病毒碼更新狀況。

5.3.9.2. 電腦使用人應定期（至少每週掃瞄一次）執行個人電腦、筆記型電腦病毒掃描。

5.3.9.3. 與其他外部電腦、筆記型電腦及可攜式媒體交換資料時，電腦使用人應先經過掃毒。

5.3.9.4. 電腦使用人或管理者應定期更新作業系統及其它應用程式之弱點修補程式。

5.3.9.5. 不隨意下載或使用不明資料或檔案，以防被植入後門或木馬程式。

5.3.9.6. 嚴禁安裝非公務使用之軟體。

5.3.10 資料保護

5.3.10.1. 不隨意在網站留下公務或個人隱私資料。

5.3.10.2. 儲存設備核准報廢後，須將機敏性資料及授權軟體予以移除，實施安全性覆寫(如硬碟低階格式化或做硬碟

複寫)或實體破壞。

5.3.10.3. 本公司人員應落實辦公桌面/螢幕淨空政策，以避免機敏文件或光碟等資料遭未經授權使用、遺失或破壞。

5.3.11 網路連線規範

5.3.11.1. 依據【通訊與作業管理程序】之防範惡意碼與行動碼管理規範辦理。

5.3.11.2. 禁止利用本公司網路散布機敏或違法資料及檔案。

5.3.11.3. 受著作權法保護之著作或軟體禁止違法下載、拷貝、安裝。

5.3.11.4. 禁止連線色情、暴力等非公務網站。

5.3.11.5. 禁止使用點對點(Peer to Peer, P2P)類型的傳輸軟體(如：Messenger、ezPeer、KURO、FOXY、e-Donkey、BT…等類型軟體)。

5.3.11.6. 一般設備、筆記型電腦或其他行動裝置設備於使用無線網路、GPRS 無線網路(3G / 3.5G/4G)連線上網時，應先啟動設備之個人防火牆及防毒軟體，並禁止同時使用一般設備、筆記型電腦或其他行動裝置設備之實體網路連線，串接本公司之內部網路(Intranet)。

5.3.11.7. 一般設備、筆記型電腦或其他行動裝置設備於使用公司無線網路時，應先經申請核准並只能在授權權限範圍內存取網路資源。

5.3.11.8. 在外地或家裡以各式裝置使用網際網路資源存取公司資訊系統，應先經申請核准並遵循公司所定的規範。

5.3.11.9. 為確保網際網路資源正常運作與防範不當使用，監督、記錄與定期稽查，公司保有存取每一位同仁的帳號與業務連繫資訊的權利，必要時，得將個人的資料提供給第三者，如法院、檢調等部門。

5.3.11.10. 禁止使用非法軟體，不得使用來路不明之軟體，亦不得測試來路不明之軟體。

5.3.11.11. 禁止使用任何儀器設備或軟體工具竊聽網路上的通訊。

5.4 網路存取控制

5.4.1 網路服務申請及規範

5.4.1.1. 為確保資訊傳輸的安全，禁止使用未經授權之網路設備，若有違反規定之行為，則依本公司相關規定進行懲處。

5.4.1.2. 各單位若有使用網路服務之需求，由申請人填寫資訊系統需求申請單，並經權責主管核准後交承辦組辦理。

5.4.1.3. 若有內部網路使用需求，申請人填寫資訊系統需求申請單且經核准後，透過網路認證機制使用本公司內部網路。

5.4.1.4. 公司外人員使用公司內網路(含無線網路)之申請，應填寫資訊系統需求申請單，由相關單位代為申請，使用完畢後停用帳號。

5.4.2 網路區隔

5.4.2.1. 為便於管理，防止不當網路存取行為與流量散佈，應區分主機與使用者工作內容，賦予適當網路區段，以協助網路存取控制管理。

5.4.2.2. 應將對外網際網路連線服務予以適當存取控制，防止機敏資料外洩。

5.4.2.3. 禁止同仁私有網路設備與本公司內部網路界接。

5.4.2.4. 定期利用無線網路搜尋工具檢查，是否有非法使用之無線網路設備。

5.4.3 網路選路與頻寬管理

5.4.3.1. 公司內與各公司間網路存取行為應透過本公司網路設備與專屬線路，對外網路存取行為須經由本公司對外專屬線路，並受到相關資訊安全管控機制監控與管理。

5.4.3.2. 應進行網路流量之監控，保障網路頻寬之正常使用。

5.4.3.3. 如發現流量異常，應立即採取適當措施後，分析網路異常原因。如果為使用者非法使用或是電腦中毒，依據【資訊安全事故管理作業程序】進行通報，並通知相關人員進行後續處理。

5.4.4 網路連線設備安全

5.4.4.1. 依照每個網路介面用途及通訊協定，設定存取控制清單，以便進行存取控制。

5.4.4.2. 需使用遠端方式管理網路連接設備時，應於網路連接設備中設定適當之存取控制清單，限制遠端管理之來源位置。

5.4.4.3. 永久有效之網路服務申請，應每年定期覆核。

5.4.4.4. 關閉網路設備不必要之服務與通訊協定，避免網路刺探攻擊。

5.4.4.5. 網路線路異動應依據【通訊與作業管理作業程序】之「資訊設備安裝維護申請紀錄單」提出申請。

5.5 作業系統存取控制

5.5.1 調整系統安全設定，以滿足使用者存取管理要求。

5.5.2 使用者帳號應具有唯一鑑識性，並應避免共用帳號。

5.5.3 取消、停用匿名權限帳戶。

5.5.4 刪除多餘不用之帳號與群組。

5.5.5 將容易被猜測之群組名稱重新命名。

5.5.6 使用安全的檔案系統。

5.5.7 依各資料夾（目錄）之用途，設定適當使用權限。

5.5.8 移除所有非必要之資源分享與網路服務。

5.5.9 啟用稽核原則（例如登入失敗之稽核），保留稽核紀錄。

5.5.10 依據系統特性設定會談期逾時（Session Time Out）時間。

5.5.11 登入較具機密性之應用系統後，若超過時限無任何動作時，系統須設定將其帳號鎖定或登出。

5.5.12 依據使用者或管理者使用需求設定連線時間或連線能力。

5.5.13 本公司公用程式個人電腦部份由軟體管理單位統一控管，軟體安裝管理，依據【遵循性管理作業流程序】規範辦理，各應用系統主機使用之公用程式，由各系統承辦人列冊管理。

5.6 應用系統存取控制

5.6.1 依據【資訊系統獲取、開發及維護管理作業程序】規範辦理，對於限制存取的應用系統，應採取身分認證（例如帳號、密碼）或其他身分鑑別的機制，並隔離敏感性系統。

5.6.2 資訊存取限制

5.6.2.1. 使用應用系統及權限，應向各相關權責單位填寫申請單申請並於核准後依申請單核准之內容進行權限設定。

5.6.2.2. 根據使用者之權限，應用系統之功能只能依其單位及角色權限執行。

5.6.3 敏感性系統隔離

具有機密性或敏感性資料的應用系統，必要時應以網路或實體的方式進行隔離。

5.7 資料庫存取控制

5.7.1 資料庫系統帳號密碼管理

5.7.1.1. 資料庫系統管理員帳號應限制保管人數，並依需求指定代理人。

5.7.1.2. 原則至少 3 個月變更一次密碼，若為特殊使用而不予變更時，應申請並經單位最高主管核定。

5.7.1.3. 密碼管理原則，應依據本程序 5.2 條文規範辦理。

5.7.2 資料庫檔案之目錄存取權限

須限制對資料庫檔案所在目錄之存取，僅有資料庫管理人員、應用系統程式可進行存取。

5.7.3 資料庫資料表存取權限

5.7.3.1. 對於資料庫資料表，應限制僅有應用系統程式可進行存取。

5.7.3.2. 若需由資料庫管理人員直接對資料庫資料表進行存取之作業，須經由單位最高主管及資料庫資料之相關權責主管授權同意。

5.7.4 資料庫公用程式及工具使用權限

限制僅有經授權之人員方可使用資料庫公用程式及工具。

5.7.5 事件紀錄

5.7.5.1. 應啟動資料庫系統事件記錄功能，記錄項目至少包含：

5.7.5.1.1. 登入使用者帳號。

5.7.5.1.2. 系統存取失敗。

5.7.5.1.3. 稽核工具安全管理

5.7.6 未經申請核准不得使用稽核工具（例如：資料庫弱點掃描軟體或程式）以防止被誤用。

5.8 遠端連線存取控制

5.8.1 由本公司外部進行主機維運管理，應依據【通訊與作業管理作業程序】填寫資訊系統需求申請單，經權責主管評估並核准後，始可開放，待作業完畢即關閉連線，若長期開放，應由權責主管定期審查。由本公司內部進行主機維運管理，應考量以加密方式或限制特定來源連線使用。

5.8.2 僅提供必要之網路服務項目、通訊協定、與連線時間，所有行為不得與原有之網路安全相關限制、規定相抵觸。

5.8.3 連線記錄，至少保留半年，網路安全負責人應依據連線申請單不定期抽檢。

5.9 可攜式資訊設備管理

5.9.1 使用可攜式資訊設備時應謹防資訊外洩。

5.9.2 可攜式電腦應確實按規定安裝防毒軟體，若需使用內、外部網路，應先評估網路環境之安全性，並確認檢查作業系統修正程式與更新病毒碼為最新版本。

5.9.3 於公共空間使用時，應注意畫面是否有遭旁人窺視之疑慮。

5.9.4 不可將可攜式設備置於視線以外之處，並隨身攜帶不可托運。

5.10 非本公司可攜式設備管理

5.10.1 訪客攜入可攜式設備需經本公司許可。

5.10.2 處理內部使用等級以上資料之工作區域（例如資訊機房），未經許可禁止使用相關設備進行拍攝或是螢幕畫面捕捉之行為，使用時需有本公司人員在場陪同。

5.10.3 未經授權核可，禁止以設備及媒體執行網路偵測、弱點掃

描、封包收集分析等高危險性軟體。

5.11 遠距工作

公司內同仁由公司外僅能透過 VPN 連線至公司內部網站。

5.12 上述所有規範若屬功能限制或老舊系統無法提供此功能，待版本升級或更新系統時改善。

6. **相關資料**

6.1【資訊資產管理作業程序】

6.2【資訊安全事故管理作業程序】

6.3【資訊系統獲取、開發及維護管理作業程序】

6.4【通訊與作業管理作業程序】

7. **附件**

7.1 系統服務申請單

7.2 應用系統角色對應表

7.3 系統使用者帳號清單