# OOOO 公司

# 實體與環境安全管理作業程序

ISMS-B-005

版本 1.0

中華民國 105 年 MM 月 DD 日

| 文件編號 | ISMS-B-005 | 實體與環境安全管理<br>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）為維護資訊資產及員工之作業場所遭受未經授權的存取、損害及干擾，以提昇實體與環境之管理、安全、品質，確保資訊資產的安全。

## 2. 範圍

適用於本公司資訊安全管理制度範圍內相關工作區域。

## 3. 權責

3.1 資訊安全推動組

督導實體安全管理並核准相關作業。

3.2 實體安全權責單位

3.2.1 管制資訊機房門禁之權限。

3.2.2 定期覆核人員進出資訊機房紀錄。

3.3 機房維運人員

3.3.1 檢查與維護資訊機房之消防、空調、電力設施及資訊設備等，以確保資訊機房設備與設施正常運作。

3.3.2 管制人員進出資訊機房及作業情形。

3.4 員工

3.4.1 確認外部人員來訪目的，聯繫受訪人員。

3.4.2 保持警覺，留意周遭環境陌生人員出入狀況。

3.5 外部人員

應配合本公司門禁安全管制及資訊安全相關規定。

## 4. 定義

4.1 辦公區域

泛指本公司資訊機房區域外之辦公作業環境。

4.2 機房區域

泛指本公司資訊機房區域。

4.3 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。

4.4 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。

## 5. **作業內容**

5.1 辦公區域安全管制

5.1.1 應明確界定或區隔辦公區域及機房之實體安全邊界，並於出入口設置門禁，以保護實體與環境之安全。

5.1.2 應確保只有經授權的人員方可進入辦公區域及機房。

5.1.3 辦公區域之重要出入口，應設置警衛、門禁管制、保全系統或監視錄影系統，並應保持正常狀態並定期維護，保持正常運作狀態。

5.1.4 本公司同仁於辦公區域活動時，需佩掛本公司之職員證或工作證，並不得擅自轉借他人使用。

5.1.5 本公司同仁應保持警覺，留意陌生人員進出辦公區域。

5.1.6 主管辦公室應宣導下班時上鎖。

5.1.7 相關專責人員應特別注意門禁出入口，並不定期巡視各出入口，以防範不當人員出入，非上班時間更應嚴加控管。

5.1.8 外部人員進入本公司辦公區域前，應連絡接洽人員。

5.1.9 訪客及非本公司員工進出本公司辦公區，應依訪客接待程序辦理相關事宜，於登記於訪客登記表或相關控管表單後進入。

5.1.10 訪客僅於公共區域活動，若於其它區域活動需有專人陪同。

5.2 資訊機房門禁管制

5.2.1 本公司資訊機房門禁之進出帳號權限應設控管，申請時應經資訊機房權責主管同意，並列冊備查。

5.2.2 外部人員進入資訊機房時，應先填寫「資訊機房管理紀錄表」。外部人員進入資訊機房前應完成登記，並由受訪人員簽章確認，若必要時由業務承辦人員陪同與監督。外部人員離去時亦應登記離開時間。

5.2.3 非上班時間若外部人員需進入資訊機房時，機房維運人員應先向業務承辦人員確認，必要時並陪同與監督。

5.2.4 資訊機房出入口及機房內應設 24 小時監控，監控範圍應包含出入口與重要資訊設備，監控紀錄應至少可追溯前一個月。

5.2.5 資訊機房門禁系統進出紀錄應至少可追溯前一個月。

5.2.6

5.3 辦公區域管理

5.3.1 下班時應關閉個人電腦及相關週邊設備，並啟動辦公室門禁管制。

5.3.2 辦公區域內應置放適當之消防設備及緊急照明設備，以確保

其可用性，並定期檢測。

5.3.3 辦公區域內不同等級的資訊類資訊資產，應依據【資訊資產管理作業程序】規範辦理。

5.4 資訊設備與媒體進出與使用管理

5.4.1 資訊機房入口應設置物品卸載區，進出資訊機房設備應進行安全檢查，以確保符合安全管理要求。

5.4.2 人員攜帶可攜式資訊設備與媒體進出機房時，須於「資訊機房管理紀錄表」註明。

5.4.3 辦公區域之資訊設備攜出入，應記錄於「資訊設備管理紀錄表」)，並依據 5.10 資訊設備攜出入管理之規範管理。

5.4.4 若有資訊機房設備變動，須填寫「資訊機房設備資訊表」，更新資訊機房設備資訊。

5.4.5 資訊設備與儲存媒體在汰除或重複使用前，應經核准後進行相關處理作業並將儲存的資料徹底清除。

5.4.6 伺服器或個人電腦應設定啟動螢幕保護與密碼保護機制及對時機制。

5.5 資訊機房環境管理

5.5.1 資訊機房內應保持整齊清潔，並禁止吸煙及飲食。

5.5.2 資訊機房內禁止攜入或堆置易燃物。

5.5.3 資訊機房溫度應維持在 20℃至 30℃，相對溼度維持在 40 度至 65 度，如有系統監控，告警值應滿足規範要求。

5.5.4 空調設備應 24 小時運轉，並設置備援機制。

5.5.5 資訊機房內應設置停電緊急照明設備。

5.5.6 資訊機房應設置專用之消防系統與搭配設置不斷電設備，並定期檢測。

5.5.7 資訊機房設備、線路等應有適當標示。

5.5.8 應設置緊急照明設備，以利消防逃生。

5.6 佈線安全管理

5.6.1 網路通訊設備於安裝時，應注意機房之電力線路架構，以避免產生線路間之干擾問題。

5.6.2 光纖或是易遭受破壞之線路設施應妥善保護，以免因其他工程裝設而影響網路之運作。

5.6.3 線路採用天花板高架或佈建於高架地板下，以防止線路遭破壞或損毀。

5.6.4 線路配置需注意維護安全與方便。

5.6.5 應使用配線圖以降低錯誤可能性。

5.6.6 網路纜線佈線時，應使用導管或其他安全措施，以防止未經授權的竊聽或損害，同時應與電力纜線予以隔離，以避免通

訊干擾;上述規範若屬功能限制或機房設施老舊無法提供此功能，需規劃於更新時改善之。

5.7 資訊機房維運管理

5.7.1 機房維運人員應每日檢查資訊機房設施及設備並填寫「資訊機房管理紀錄表」，如發現異常，應即時處理並通知業務承辦人員、權責主管或維護廠商；處理結果須記載於「資訊機房管理紀錄表」。

5.7.2 維護廠商作業完成後需提供維護處理紀錄表單，交由機房維運人員保管。

5.7.3 資訊機房設施或重要資訊設備應定期實施保養與妥善維護。

5.7.4 機房維運人員進行機架設備清查並更新標示。

5.7.5 機櫃應上鎖並獨立管理。

5.8 資訊設備維修

5.8.1 新購置之資訊設備，如無法自行維護，應於採購時，洽談維護服務事宜。

5.8.2 設備異常時，由設備系統負責人進行初步研判或處理，能自行解決於確認後結案，若系統負責人無法自行解決則須報請設備維護廠商進行維修。

5.8.3 設備異常嚴重影響應用系統之運作時，系統負責人則依據【資訊安全事故管理作業程序】進行通報。

5.8.4 資訊設備送修時，若非屬儲存媒體損壞，於送修前應進行資料清除或取出儲存媒體，防止資訊外洩。

5.8.5 合約規範之外修作業，修復後發現資訊設備規格不符，則依合約規範處理。

5.9 場所外設備安全

5.9.1 設置場所外設備安全，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以避免人員誤觸，並標示管理權責單位與適當警語。

5.9.2 若因環境限制無法達成上述規範，則應派員加強巡檢，確保資訊設備安全。

5.9.3 設置於本公司外之資訊資產如需與本公司內部網路連線，應透過專屬加密線路，並設置網路存取控制，使用者應遵循本公司相關資訊安全規範。

5.10 資訊設備攜出入管理

5.10.1 資訊設備由保管單位（管理者或使用者）妥善保管且負保管之責，如需攜出入須經保管單位主管同意。

5.10.2 保管單位主管或業務承辦人員應審慎評估資訊設備攜出入需求之必要性，並記錄於「資訊設備管理紀錄表」。

5.10.3 資訊設備於攜出入經核准後，應由檢查人員確認資訊設備與資料安全，申請人不得將設備擅自轉借他人或用於申請目的以外之用途使用。

5.10.4 將機密資料存放於資訊設備時，應採取適當加密處理或保護措施，應謹慎防範資訊洩漏或妨害組織利益等情節發生，保管單位或廠商應盡控管之責，避免遺失時洩漏資訊。

5.11 資訊設備報廢作業

5.11.1 報廢申請應向總務單位提出申請，於核可後方得辦理報廢。

5.11.2 資訊設備與儲存媒體報廢時，由保管單位確認所報廢之資訊資產內之資訊是否已完全清除。

5.11.3「資訊資產清冊」內之資產報廢作業完成後，依據【資訊資產管理作業程序】規範更新「資訊資產清冊」。

5.11.4 實體類資訊資產若無殘值時，應進行實體破壞後，進行資源回收。

5.11.5 資訊資產之儲存媒體必須消磁或利用工具清除資料，如無法進行時則進行實體破壞。報廢磁帶需進行燒毀，確保資料已被銷毀。

5.11.6 儲存媒體由廠商協助銷毀時必須知會保管單位，並在其監督下進行銷毀，必須指派監督人員跟隨。

5.12 資訊設備歸還管理

5.12.1 應依據人事管理辦法及離(調)職程序辦理，盤點離(調)職人員所歸還或移交之資訊設備是否正確無誤，歸還設備如需再使用，應清除不必要之資訊或軟體。

5.12.2 資訊單位應依據人事單位通知，刪除、停用或修改離調職人員之系統權限。

## 6. **相關資料**

6.1【通訊與作業管理作業程序】

6.2【資訊資產管理作業程序】

6.3【資訊安全事故管理作業程序】

## 7. **附件**

7.1 資訊機房管理紀錄表

7.2 資訊設備管理紀錄表

7.3 資訊機房設備資訊表