# 資通安全風險管理

一 資通安全管理策略與架構

1 資通安全風險管理架構：

本公司組織結構設有資訊室，由總經理兼任資安長，另配置資安專責主管一人及資安專責人員一人，負責推動、協調監督及審查資通安全管理事項。每年至少一次向董事會報告投入資通安全管理之資源及運作情形。

2 資通安全政策：

本公司已制定資通安全政策與資訊安全管理目標，詳如「ISMS-L1-01資訊安全管理手冊」。

3 具體管理方案：

本公司具體管理方案如下：

| 類別 | 採行措施/作法 | |
|---|---|---|
| 網路安全 | 網路服務使用原則 | ✓ 本公司基礎網路架構區分為內部區域網路、外部網路與對外提供服務之非軍事區(DMZ)網路。<br>✓ 為確保內部區域網路私密性，本公司內部網路實體連線應進行識別。<br>✓ 外部網路除網路基礎設備外，以不提供服務為原則，如設置服務者，應有足夠之安全措施。<br>✓ 對外提供服務之非軍事區(DMZ)網路應考量網路服務之安全性進行管控。 |
| | 網路設備安裝、維護作業 | ✓ 網路連結設備與網路安全設備之安裝，應依據「ISMS-L3-04設備保護管理工作指導書」之要求辦理。<br>✓ 網路連結設備與網路安全設備於安裝、維護前須與本公司之資訊單位進行安裝前協調，以充分了解該項維護之影響層面與作業風險。<br>✓ 網路連結設備與網路安全設備安裝、維護時，設備密碼，除網路管理人員外，不得交予其他人員，更改設定時如須輸入密碼，應由網路管理人員輸入，並應於安裝及維護作業完成後，視需要變更設備內設密碼。<br>✓ 網路連結設備與網路安全設備之密碼，應依據「ISMS-L2-13身份和存取管理程序書」之要求辦理。<br>✓ 網路連結設備與網路安全設備之安裝應考慮裝置場地之安全性，應設置於有人員管制之地點，並考慮通風散熱問題。 |
| | 網路線路設置 | ✓ 網路連結設備與網路安全設備於安裝時，應注意機房之電力與通訊線路架構，以避免產生線路間之電磁干擾與網路設備電源負載問題。<br>✓ 光纖線路設施應加以特別標示警告，應避免彎折與刮傷，以有效降低因工程裝設而影響網路正常運作之風險。<br>✓ 線路之鋪設應避免電磁干擾，並儘可能不要與電力線路共存，以 |

| | | |
|---|---|---|
| | | 防止線路遭電磁干擾、破壞或損毀。<br>✓ 網路設備應於安裝設置完成後，更新「ISMS-L4-30網路架構圖」。 |
| | 網路連線作業 | ✓ 本公司對外網路連結及區域網路，由資訊室統一規劃。<br>✓ 本公司各部門不得以未經申請許可之方式，私行架設與外部網路連結設施或使用非本公司同意之通訊方式進行網路連線。<br>✓ 本公司區域網路位址，均採用固定式IP位址。<br>✓ 本公司同仁原則上採一人一機方式，以同仁專屬帳號登入所屬個人電腦。若實際情況不許可一人一機作業，或有共用帳號之情形，須先經由權責主管核准，並對此設備進行監視作業。<br>✓ 遠距工作作業，應依據「ISMS-L3-09遠距工作指導書」之要求辦理。 |
| | 網路安全管理作業 | ✓ 防火牆管理<br>■ 本公司與網際網路連結，應以防火牆區隔。防火牆之管理，應依據「ISMS-L3-10防火牆工作指導書」之要求辦理。<br>■ 應每年檢核防火牆存取規則以及版本更新資訊，以維護系統安全。<br>■ 本公司應識別惡意外部網站，並記錄於「ISMS-L4-31惡意網站清單」。於清單內之網站，應使用防火牆之設定，阻止本公司同仁進行存取。<br>✓ 本公司同仁使用電子郵件，應依據「ISMS-L3-14電子郵件工作指導書」辦理。<br>✓ 即時通訊軟體僅作為文字或語音訊息溝通使用，不得傳送檔案。<br>✓ 為確保網路安全性及避免浪費網路頻寬之考量，除公務所需外，禁止使用點對點分享軟體(Peer-to-Peer, P2P)。 |
| | 無線網路安全 | ✓ 若須架設無線網路需經核准後方能設置。<br>✓ 外部人員採用獨立無線網路設備，且不能介接本公司內部網路。 |
| 電腦安全 | 電腦系統與實體設備保護 | ✓各式電腦的系統應及時進行安全修補。<br>✓各式電腦軟體及版權，集中由資訊單位管理。<br>✓資訊設備如：使用者端點設備、伺服器應設定螢幕密碼保護程式，螢幕保護程式啓動時間應設定不超過15分鐘，並啟動密碼保護措施，防止他人未經授權使用電腦。<br>✓使用者端點設備、伺服器之作業系統桌面，不應存放敏感性文件。<br>✓使用者離開座位或辦公區域，應隨手將使用者端點設備、伺服器之作業環境登出或鎖定電腦。<br>✓注意使用任何電腦設備時，其電源使用不可超過電源負載量。 |
| | 防毒軟體 | ✓公司所有電腦系統均安裝防毒軟體，實施並自動更新病毒庫，並定期執行病毒掃描。<br>✓資訊室應定期確認本公司之個人電腦、筆記型電腦、各伺服器均已安裝防毒軟體，並維持正常啟動狀態。若有無法安裝防毒軟體之情形，應經由資安~~全~~長核准，並有其他之控制措施。<br>✓區隔辦公環境與現場設備的網路管理，進行分割VLAN方式管理不同場域應用。 |

| | | |
|---|---|---|
| | 存取安全 | ✓每位電腦系統使用者，應賦予獨立的通行帳號，且帳號應依業務需求賦予最低能滿足作業的許可權。<br>✓如因特殊需求，需共用帳號時，應先提出申請，並經審核後方能使用。<br>✓職員離職或職位調動時，需立即取消或調整其帳號許可權。<br>✓定期審查帳號及使用權限情況，確保符合現狀。 |
| | 密碼安全管理 | ✓同仁應申請公務所需系統帳號，密碼應妥善保管，並依下列規定設定密碼：<br>■ 禁止使用空白密碼。<br>■ 管理員帳號密碼長度應為8碼(含)以上，使用者帳號密碼長度應為8碼(含)以上。<br>■ 密碼複雜度須為4取3原則：a.英文字母大寫 b.英文字母小寫 c.阿拉伯數字 d.特殊符號。<br>■ 密碼更改時，新密碼不應與前3次密碼相同。<br>■ 密碼應最少每90天更換一次，密碼最短使用期限為1天。<br>■ 密碼須妥善保管避免他人知悉。<br>✓輸入密碼時，電腦螢幕不得明白顯示所輸入之密碼。 |
| 應用系統管理 | 電子郵件使用安全 | ✓人員離職、退休或留職停薪時，電子郵件帳號應立即刪除或停用。若因業務需求，無法刪除或停用，需經權責主管同意後保留此帳號，但應立即變更此帳號之密碼。<br>✓人員於處理公務時，不能使用外部電子郵件服務。若需使用，需經資訊安全長核准同意。<br>✓不得與他人共享電子郵件服務之郵件帳號，或將郵件帳號與密碼洩露與他人。<br>✓對於敏感性資訊，除因主管機關之要求與公務需求外，不得使用電子郵件對外傳送。如須經電子郵件傳送時，須經部門主管同意，並應將資訊加密後傳送。<br>✓內部互傳或對外的郵件皆不允許超過規定之大小限制，並禁止傳送垃圾郵件，以免影響頻寬，浪費網路資源。<br>✓禁止隨意開啟來路不明之電子郵件，以避免惡意程式或病毒感染。<br>✓下載電子郵件附件及檔案前應檢查是否有惡意軟體（含病毒、木馬及後門等程式等）。<br>✓應關閉電子郵件自動預覽及下載圖片之功能。 |
| | 即時通訊軟體使用安全 | ✓安裝與使用即時通訊軟體，須按業務實際需要進行審慎評估，且須採取適當的安全控管措施。<br>✓即時通訊軟體僅作為文字或語音訊息溝通使用，資料機密等級危機密時不得傳送檔案，但有需要時，需以加密方式進行。 |
| | 資料安全與備份 | ✓資訊單位應指派備份管理員負責執行與管理備份作業。<br>✓備份管理員應擬定「ISMS-L4-36備份計畫」，經資訊單位主管核准後，依規劃時程執行備份作業。<br>✓備份作業成功和失敗，均應建立和維持備份紀錄。<br>✓備份管理員應對備份作業失敗之原因，採取處理措施或調整備份計畫，以免再次發生備份失敗之情形。<br>✓備份管理員應依據「備份計畫」中的「還原測試規劃時程」執行備份資料還原測試，以確保備份資料能夠在原來資料發生異常時，進行回 |

| | | |
|---|---|---|
| | | 復作業。<br>✓備份之資料，不應與原來資料存放於同一實體之儲存設備。<br>✓備份資料之保護措施，應與原來資料相同。 |
| | 異常事件處理及災害復原計劃 | ✓針對常見資安事件與異常情況，擬定異常事件識別與記錄、事故分裂與評估、事故通報、事故處理與矯正預防及檢討預防等流程處理。<br>✓定期評估及檢視營運衝擊分析(BIA)。<br>✓擬定、維護營運持續計畫、營運持續演練計。<br>✓定期依據營運持續演練計畫，實施營運持續演練及檢討完善營運持續演練計畫。 |
| | 資料刪除 | ✓儲存設備或媒體報廢時需實體破壞。 |
| | 系統環境安全 | ✓應設置分離之系統開發、測試和維運環境，以減少維運環境遭受非授權存取之機會。<br>✓應分群隔離網路中之資訊服務、使用者和資訊系統。<br>✓系統環境之設定和使用，應分離責任和分工衝突，以降低非授權或非故意修改或誤用資訊資產之機會。<br>✓資訊資產分級為「高」之伺服器，伺服器管理員應每月定期檢查伺服器之狀況，並記錄於「ISMS-L4-32伺服器檢核表」，以確保設備之安全性。<br>✓如果委外廠商代表本公司儲存其資訊，則應考慮將資訊刪除要求納入委外合約中，以在此類服務期間和終止時強制執行。 |
| | 資源管理 | ✓資訊室應依據目前資源使用狀況，界定目前及未來的資源需求，包括容量及效能、資源的數量、大小、規格、資源需求的時間。<br>✓資源需求可能包括執行服務所需之人力、系統及相關設備、網路、機房空間、經費等。<br>✓資訊室定期實施資源量測及監控，如發生異常時，應即時處理。<br>✓實施有關資源之管理措施，如：資源調適、資源升級。<br>✓資訊室應評估資源調適或升級對業務服務及資源之衝擊，並建立解決方案。 |
| | 稽核日誌管理 | ✓啟動稽核日誌功能時，應避免影響日作業之進行或對業務流程產生衝擊。<br>✓系統管理員應每年定期審查系統管理者和使用者活動、例外、錯誤和資訊安全事件等稽核日誌內容，並記錄於「ISMS-L4-33稽核日誌審查作業一覽表」中。<br>✓稽核日誌至少保留一年。 |
| | 鐘訊同步管理 | ✓本公司之資訊設備皆執行鐘訊同步作業，內部之資訊設備與AD服務進行自動同步，提供對外服務之設備與中原標準時間進行自動同步。<br>✓無法自動同步之資訊設備，則以人工之方式進行鐘訊同步作業，執行頻率可依據資訊設備之情況而定。 |
| | 技術漏洞管理 | ✓資訊室應指定弱點管理員負責管理技術漏洞，包括弱點監控、風險評鑑、弱點修補等。<br>✓弱點管理員於發現弱點或接獲弱點通報時，若弱點等級為為高(含)以上或經討論需要修補之弱點，則應填寫「ISMS-L4-35弱點處理通報單」，交由資訊主管決定需採取之應變措施。<br>✓弱點管理員應建立弱點修補機制，不定期獲取經驗證之弱點補強軟 |

| | | |
|---|---|---|
| | | 體，降低因系統之弱點所造成之威脅衝擊。<br>✓如有必要，弱點修補程式於安裝前，應進行測試，以避免弱點修補程式所造成之危害。 |
| | 威脅情資管理 | ✓資訊室應指派人員關注內、外部資訊安全相關議題，包括重大資通安全漏洞與事件、政府政策調整、客戶營運的變化等資訊，並有相關因應措施。 |
| 人員安全 | 人員安全管理 | ✓對公司資訊單位人員的職責進行明確定義。<br>✓新進人員報到時發給或告知「ISMS-L3-06員工資訊安全管理作業規範」相關內容以供參考，並依據相關法令簽具「ISMS-L4-21保密同意書」，俾瞭解個人應負的資訊安全責任。<br>✓人事部門應向新進人員說明，其所簽署之保密同意書，其資訊安全責任和義務，於本中心和聘僱人員終止聘僱關係後，仍然有效。<br>✓各種資訊安全工作，需建立代理人制度，以應付緊急情況的需要。 |
| | 安全認知訓練 | ✓應界定資訊安全管理要求，瞭解與評估年度之資訊安全訓練需求，特別是影響資訊安全績效之工作人員所需要的工作能力與知識。<br>✓依據已界定之訓練需求，規劃年度訓練活動，以符合本公司資訊安全管理技能及知識需求，並透過E-mail或適當發佈管道，通知受訓人員。<br>✓規劃時程，執行訓練課程。每一次訓練課程皆應進行訓練績效評估。<br>✓所有正式員工和約聘人員，每人每年應接受至少3小時與工作相關之資訊安全政策、程序或認知訓練，以維持正確資訊安全認知。<br>✓資訊安全事件納入教育訓練，提升同仁資安意識。 |
| 委外 | 資訊安全供應商管理 | ✓針對資訊系統、設備需委外時，需針對委外專案實施專案風險評估。<br>✓應於採購前，評估與管理資訊服務或系統之合格供應商。<br>✓本公司供應商合約之簽訂單位應對供應商之服務紀錄進行審核，以識別服務改善之機會。<br>✓供應商人員於提供服務前，應簽署「ISMS-L4-76委外廠商保密同意書」或依照本公司合約管理之要求簽署相關保密協議，確實遵循相關之保密要求。 |

二 投入資通安全管理之資源及運作情形：

本公司新購入電腦安裝即時防毒軟體，並啟動自動與定期更新病毒碼功能，設置對外網路防火牆及電子郵件過濾機制。每年進行ERP權限稽核防止不當存取。公司內部定期由資訊室發布資訊安全意識文章，每年實施資訊安全教育訓練、及社交工程演練，加強員工資訊安全知識，期能持續健全保持資訊安全。

為持續保持本公司無資訊安全事故導致系統資料遺失發生情形，針對機房溫濕度進行監控並設置消防設備，機房採門禁管制，限制特定人員進入，重要資料庫每日進行備份，並建置備援機制。

本公司一向重視集團資訊安全相關作業，以維護公司資訊之機密性、完整性、可用性與適法性為目標，並致力於避免發生人為疏失、蓄意破壞與自然災害時，遭致資訊與資產遭致不當使用、洩漏、竄改、毀損、消失等情形；本公司資訊系統硬體基礎設施及各項防護設施由集團資訊室統一管理，並於 112年開始啟動導入 ISO 27001 資訊管理系統，預計113年申請外部稽核 ISO 27001 認證。透過 ISO 27001 資訊安全管理系統之導入， 強化資訊安全事件之應變處理能力，保護公司與客戶之資產安全。

資訊室每年均定期執行各項資訊安全相關之檢測及評估作業，112 年度各項資安檢測評估作業頻率及執行結果如下：

| 項　　目 | 作業頻率 | 112年度作業期間 | 結果 |
|---|---|---|---|
| ERP 系統災難復原測試 | 每年一次 | 112/6 | 無應列重大風險情形 |
| 電腦合法性軟體檢查 | 每年一次 | 112/12 | 無應列重大風險情形 |
| ERP 系統權限設定檢查 | 每年一次 | 112/8 | 無應列重大風險情形 |
| ERP 系統個人密碼定期變更 | 每季一次（ERP設定） | ERP設定開啟，自動化管理 | 無應列重大風險情形 |
| 資訊安全宣導 | 不定期，每年至少一次 | 112/12/14 | 無應列重大風險情形 |
| 機房巡檢 | 每日 | 週末及國定假日除外 | 無應列重大風險情形 |
| 資料庫備份作業 | 每日(採系統自動異地備份) | 週末及星期日除外 | 無應列重大風險情形 |

| 112年度目標規劃 | 控管方法及執行情形 |
| --- | --- |
| 持續發布資訊安全意識文章 | •Q4資安宣導&資安知識問卷作答 |
| 人員進修 | •資安專責人員取得資訊安全管理系統ISO27001證照。 |
| 持續保持無資訊安全事故發生( 資訊安全) | •定期執行弱點掃描作業。<br>•定期更新防火牆及垃圾信系統的韌體及特徵碼。<br>•評估進階版本的防毒軟體，發現惡意程式自動通知資訊人員&中央控管。 |
| 台灣電腦網路危機處理暨協調中心 | •已申請通過加入TWCERT/CC聯防。 |
| 持續保持無資訊安全事故導致系統資料遺失發生 | •機房設置溫度監控設備及消防設備。<br>•機房採門禁管制，限制特定人員進入。<br>•確實系統資料庫每日備份，建置備援機制及異地備份機制。<br>•執行UPS檢修及電池更換。 |

112 年度本公司無因重大資通安全事件遭受損失或嚴重影響營運運作的情形。