

數位防線:企業資訊安全政策與實踐

強化本公司的資訊安全管理,建立「數位防線:企業資訊安全政策與實踐」之觀念,確保客戶及同仁資料處理之機密性、完整性及可用性,務使本公司資料之處理全程均獲安全保障,提供安全穩定及高效率之資訊服務。

5. 主題特定政策

5.1. 存取控制:

5.1.1.限制對資訊及資訊處理設施之存取。

5.1.2.確保授權使用者得以存取,並避免系統及服務的未授權存取。

5.1.3.令使用者對保全其鑑別資訊負責。

5.1.4.防止系統及應用遭未經授權存取。

5.2. 實體及環境安全:

5.2.1.防止組織資訊及資訊處理設施遭未經授權之實體存取、損害及干擾。

5.2.2.防止資產之遺失、損害、遭竊或破解,並防止組織運作中斷。

5.3. 資產管理:

5.3.1.識別組織之資產並定義適切之保護責任。

5.3.2.確保所有資產依其對組織之重要性,受到適切等級的保護。

5.3.3.防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。

5.4. 資料傳送:

5.4.1.確保資料傳送可追溯性及不可否認性。

5.4.2.維持傳送作業之可靠性及可用性。

5.4.3.實體傳送使用破壞存跡或抗破壞之控制措施。

5.4.4.使用規定之電子傳輸媒體傳遞資料,不可因貪圖方便而任意使用非法與不當之傳輸媒體。

5.4.5.不得利用任何傳輸媒介透過資料傳遞、訊息傳送、發言或視訊等方式透露機密或敏感性資訊給其他組織或人員。

5.4.6.內部資訊網站須依權責及工作需求核發適當權限,以管制相關文件之存取。

5.5. 端點裝置之安全組態及處置:

5.5.1.對使用者端點裝置分發及回收。

5.5.2.對使用者端點裝置軟體安裝進行控制。

5.5.3.對使用者端點裝置進行安全性更新。

5.5.4.使用者端點裝置經登入程序使用。

5.5.5.防範惡意軟體對使用者端點裝置危害。

5.5.6.管制私人裝置使用。

5.6. 網路安全:

5.6.1.網路使用者經授權後,只能在授權範圍內存取網路資源。

5.6.2.對使用網路系統的電腦連接線路,應適當加以控制,以減少未經授權之系統存取或電腦設施的風

險。

5.6.3.設定網路區隔之規劃,應遵循內外網路實體區隔規定,並應禁止個人無線網路裝置破壞內外網路實體區隔之安全機制。

5.6.4.非經授權嚴禁使用無線網路及私有有線設備與網路介接。

5.7. 資訊安全事故管理:

5.7.1.確保對資訊安全事故之管理的一致及有效作法,包括對安全事件及弱點之傳達。

5.7.2.建全資訊安全事故通報體系。

5.8. 資訊備份:

5.8.1.依照資訊之可用性及完整性需求,制定個資訊備份週期、方式及保存期限,並測試其有效性。

5.8.2.依照備份資料之機密性需求加以防護,避免衍生之其他資安事件。

5.9. 密碼學:

5.9.1.依照法規、客戶要求及資訊資產風險設置加密機制。

5.9.2.管制金鑰產生、分派啟用、儲存、更新、廢止到封存和銷毀等作業。

5.10. 資訊分類分級及處理:

5.10.1. 資訊標示涵蓋所有格式的資訊及其他相關聯資產。

5.10.2. 使人員及其他關注方認知標示要求。

5.10.3. 提供所有人員必要之認知方法,以確保正確標示資訊並進行相對應的處理。

5.11. 技術脆弱性管理:

5.11.1. 定義並建立與技術脆弱性管理相關聯之角色及責任。

5.11.2. 偵測其資訊資產是否存在脆弱性。

5.11.3. 軟體更新管理過程,以確保對所有獲授權軟體,安裝最新經核可之修補程式及應用程式之更新套件。

5.11.4. 使用適合所使用技術之弱點掃描工具,以識別脆弱性並查證脆弱性修補是否成功。

6. 適用性聲明書

依據「ISO 27001 資訊安全管理系統-要求」要求產出「適用性聲明書」,以書面方式列舉資訊資產是否適用其標準所列之控制措施,及其不適用之原因。當組織架構、人員、設備、實體環境等變動時,資訊安全管理委員應重新定義控制措施之適用性。

7. 實施

本政策經主任委員核定後實施,修訂時亦同。