

2.4 資訊安全與隱私權管理

為保護智慧財產權、資訊資產、用戶個資及線上營運安全，本公司依據行政院國家資通安全會報技術服務中心所發佈之「政府資安規範整體發展藍圖」規範指引，制定資訊安全管理制度及資安政策，並建立各項資安管理規範，以及滿足公司需求的資訊安全系統和必要防護機制，以降低遭受內、外部蓄意或意外災害威脅，進而造成公司損失，因此 2023 年度公司無重大資安事件與損失。

2.4.1 資通安全風險管理架構

本公司資訊安全之權責單位為資訊技術處，配置專責人員擔任資安主管及資安人員，負責推動、協調、監督及審查資通安全管理事項，並執行資訊安全政策，宣導資訊安全訊息，提升員工資安意識，蒐集及改進組織資訊安全管理系統及有效性之技術、產品或程序等。由稽核單位每年就內部控制制度 - 資通安全管控指引，進行資訊安全查核，評估公司資訊作業內部控制之有效性。

2.4.2 資訊安全政策

為強化及落實資訊安全管理，本公司訂有內部控制制度 - 資通安全管控指引，期望達成以下目標：

- 確保資訊的可用性、完整性以及機密性
- 保護客戶資料與本公司資訊資產免於遭受內、外部的蓄意或意外災害的威脅
- 確保資訊系統持續運作
- 落實稽核作業，確保資安規範持續有效

2.4.3 具體管理方案

本公司資訊安全管理運作模式採 PDCA (Plan-Do-Check-Action) 循環式管理，確保目標之達成且持續改善，具體目標與措施說明如下：



1. 電腦設備安全管理

01

本公司應用伺服器與骨幹網路設備等均置於專用機房，機房門禁採用感應刷卡進出，並保留進出記錄及 24 小時錄影存查。

02

機房內部備有獨立空調與自動偵測防煙及溫度告警設備、機房專用之噴氣式滅火設備；並配置不斷電系統與穩壓設備，防止意外斷電造成之系統毀損。以保障公司資訊系統軟硬體資產之實體安全。

03

伺服器與終端電腦設備安裝有統一管理之防毒軟體，病毒碼自動更新機制，確保所有資訊電腦設備具備相同防毒等級。

04

伺服器與終端電腦設備安裝有統一管理之智能端點防護軟體，可偵測、防止具有潛在威脅性的系統執行檔與惡意軟體運行之行為。

05

日誌管理與監控，統一收集與管理重要伺服器日誌。並針對重要系統事件撰寫告警規則，以加強早期察覺可疑之行為。

2. 網路安全管理

01

依不同組織單位實體切割為不同網路區段，防止單一單位遭惡意軟體、病毒入侵之後迅速擴散，將可能危害之風險控制於單一網路區段。

02

於網際網路連線的閘道口，配置企業級防火牆，阻擋外部攻擊與連線管制、過濾惡意網站、釣魚網站等之非法連線，強化網路安全控管與防護。

03

不同地點之辦公室間網路連線皆使用通訊加密的 VPN 連線架構進行作業，避免資料傳輸過程遭受非法擷取。

04

若同仁需要遠端登入公司內部系統存取資料，必須先申請 SSLVPN 帳號，並透過 SSLVPN 提供的安全方式進行登入。這種方式不僅保障了登入過程中的資訊安全，也能夠留下相應的使用紀錄，方便未來的稽核或調查。

05

配置有郵件防毒與垃圾郵件過濾機制，防堵病毒與垃圾郵件進入使用者終端電腦設備。

3. 存取控制

01

當同仁到職時，人力資源部會代為申請公司通用系統帳號。當同仁離職（或退休）時，則需要親自前往資訊技術處進行各系統帳號的刪除程序，並進行簽名確認。透過這樣的作業流程，可以有效地控制帳號的使用權限，防止未經授權的人員存取系統，從而提高整體資訊安全性。

02

若同仁需要存取與業務相關的後台管理系統，則需先提出申請，並經主管同意後，由資訊部門的同仁進行系統設置。透過這樣的申請程序，能夠確保系統的存取權限得到嚴格控管，同時也能夠有效地防範潛在的安全風險。

03

根據政府組態基準原則，設定作業系統密碼複雜度與長度要求限制、螢幕保護鎖定、登入錯誤鎖定等原則。

04

檔案伺服器根據各單位的需求，為不同的人員和群組設置不同的檔案資料夾權限，以保障資訊的安全性。同時，使用群組原則管理工具，能夠集中管理檔案伺服器的各項稽核設定，進一步提高系統的可靠性和管理效率。

4. 雲端安全

01

使用雲端 IAM 服務進行身份與存取管理，啟用帳號雙重驗證系統以提高安全性。

02

雲端服務預設啟用加密機制，並使用雲端加密金鑰代管服務以確保資料安全性。

03

雲端系統稽核日誌代管服務可蒐集雲端系統操作歷程，保留供日後查詢與分析。

04

使用雲端防火牆阻擋外部攻擊與連線管制，並整合國際流量清洗服務與網路應用層防護系統，避免遭受 DDoS 攻擊或其他網站應用層攻擊而導致營運中斷。

5. 營運持續

01

系統與資料備份採取日備份機制，備份資料儲存於本地網路硬碟並採取異地備份策略，以確保備份資料的安全。台北辦公室與台中辦公室的備份資料彼此備份，以達到最佳的備份效果。

02

每年實施一次抽測災害復原演練，選定還原日期基準點後，由備份媒體回存於系統主機，確認回復資料的可用性與完整性。



6. 用戶個資

01

為保障用戶個資，本公司遵照中華民國個人資料保護法（個資法）之規定，各產品均有隱私權條款與個人資料使用同意書，詳細告知用戶並取得用戶同意個人資料之蒐集、處理、利用。用戶並得向本公司請求停止蒐集、處理、利用及請求刪除。

02

個人資料於資料庫預設加密儲存，並使用資料遮罩與隱碼方式進行存取保護。

03

個人資料之存取與傳遞均使用 SSL 安全加密管道進行存取，防止網路傳遞時被竊取。資料存取日誌留存備查。

04

加強同仁個人資料處理法相關之教育訓練。



7. 智慧財產

01

本公司之智慧財產（如原始程式碼、圖片、影像、音效等）均存放於機房中版本控制系統進行版本控制，保留歷程版本。

02

依照營運持續之措施，版本控制系統定期完整備份，並異地備份於台北與台中辦公室。

03

使用雲端 DevOps 軟體開發流程與版本控制服務，並採用雲端服務業者提供備份資源與機制。

04

新進同仁到職，必須簽訂保密協議，同仁任職期間負有保護公司智慧財產之責任。

2.4.4 投入資通安全管理之資源情形



資安意識與教育訓練

- (1) 資訊安全之主管及人員須定期接受資訊安全專業課程訓練。
- (2) 每年不定期對內部同仁實施資訊安全相關的教育訓練課程。新進同仁到職必須接受新人資訊安全講習課程。
- (3) 每月定期製作資訊安全電子報，宣導各類資訊安全相關報導與時事，提醒同仁對可疑之人事物應加強注意與提高警覺。
- (4) 不定期實施社交工程演練，針對資訊安全意識不足之同仁加強資訊安全課程與訓練。
- (5) 訂閱「台灣電腦網路危機處理暨協調中心 TWCERT/CC」，取得資安事件來源管道，以及收集資安情資，提供內部宣導。



專業技術資源

本公司有專業資安團隊，定期執行各項資安檢測，並導入防護機制及監控全域異常設備。



編列適當資安預算

除現有資安相關維修運行費用外，各資訊作業開發及營運系統建置均需編列必要防護、監控、檢測等資安費用。