資訊安全與隱私保護

為強化資訊安全管理，確保資訊的可用性、完整性以及機密性，以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，並以持續經營不中斷的目標。隆中參考行政院國家資通安全會報技術服務中心所發佈「政府資安規範整體發展藍圖」之共通規範指引，足見公司對於資安與隱私保護的重視，也因此 2021 年公司無重大資安事件與損失。

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 AI 人工智慧端點行為監控軟體，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。

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

各據點間建立 VPN 連線作業，使用通訊加密的方式，避免資料傳輸過程遭受非法擷取。

04

員工由遠端登入公司內網存取系統，必須申請 SSLVPN 帳號，透過 SSLVPN 的安全方式始能登入使用，且均留有使用紀錄可稽查。

05

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

存取控制

01

員工辦理到職時由人力資源部代為申請公司通用系統帳號。離(休)職手續時，必須親至資訊技術處，進行各系統帳號的刪除作業並簽名確認。

02

員工需要存取使用業務相關之後台管理系統，需提出申請並經主管同意後，由資訊單位同仁進行設置。

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

檔案伺服器依照各單位設置人員與群組之檔案資料夾的權限配置。群組原則管理工具，來集中管理檔案伺服器的各項稽核設定。

雲端安全

01

採用雲端IAM(Identity and Access Management)服務進行身分與存取管理，並強制啟用帳號雙因素驗證系統。

02

雲端服務預設所有系統與資料啟用加密機制，並採用雲端加密金鑰代管服務。

03

雲端系統稽核日誌代管服務，收集雲端系統操作歷程，保留備查。

04

雲端防火牆阻擋外部攻擊與連線管制，並啟用網路應用層防護系統，整合使用國際流量清洗服務，防止分散式阻斷式服務攻擊(Distributed Denial-of-Service Attack，簡稱DDoS攻擊)與網站應用層之攻擊而造成營運中斷。

營運持續

01

系統與資料備份採取日備份機制，系統與檔案資料備份儲存於本地網路硬碟。再經由各據點定期相互傳遞異地備份，以確保備份資料的安全。

02

災害復原演練，每年實施一次抽測演練，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。

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。

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，並異地備份於各據點。

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

新進員工到職，必須簽訂保密協議，員工任職期間負有保護公司智慧財產之責任。

資安意識與教育訓練

01

資安宣導，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。

02

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。

03

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。

04

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。