資通安全管理

（一）資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源

1.資訊安全組織架構：

本公司於民國 111 年設立『資訊安全委員會』，負責統籌資訊安全管理策略，建置並維護資訊安全管理體系（ISMS）。其職權涵蓋資安政策之制定與推動、風險管理及合規性查核。

該委員會由研發中心張執行副總經理擔任資安長（CISO），資訊技術處柯處長擔任總召集人，成員包含各事業處指派之代表。委員會每年至少召開一次會議，審議資安政策及重大議題，致力於確保資通安全管理之機密性、完整性與可用性。此外，委員會每年定期向董事會匯報執行成果；民國 114 年度之資通安全執行情形，資安長於同年 11 月 7 日向董事會完成報告。

2.資訊安全政策：

資訊安全治理與合規承諾：

建立資訊安全政策與目標，全面保障客戶隱私與機密資料，並嚴格履行合約義務，確保公司核心資產的機密性、完整性與可用性，符合國際標準及法規要求。除通過 ISO 27001:2013，並於 114 年完成 ISO27001:2022 轉版認證，持續依循資訊安全管理體系，強化資安治理，確保資訊安全管理機制的長期穩健與持續優化。

風險控製與管理：

定期召開資安委員會，監督資安策略執行，確保公司核心資產的安全性。定期執行弱點掃描、滲透測試與社交工程演練，主動找出公司系統和人員的資安弱點，強化防禦，防止駭客利用這些漏洞造成資料洩漏、服務中斷等損失，確保企業符合法規並保障營運安全。

防禦與監控：

採用先進資安技術與聯防機制，確保網路環境安全，並落實事件通報與應變流程。

3.資訊安全風險管理與防護機制：

本公司資安治理體系已取得 ISO 27001(證書效期自 2025 年 10 月 31 至 2028 年 10 月 31 日)資訊安全管理系統驗證，以此國際標準作為風險管理的核心架構與成效檢驗依據。透過標準化之 PDCA 循環，我們持續優化防護體系，強化數位信任。

3.1 規劃與策略(Plan) -國際標準接軌，建構韌性

- 風險治理體系：依據國際標準架構導入第三方風險評估系統，建立全方位監控機制，確保資安威脅可視化。
- 制度與標準化：制定標準化「資安事件通報與應變程序」，並定期檢視資安政策與目標，確保管理制度之有效性與適用性。

3.2 執行與運作(Do) -落實縱深防禦，強化防護廣度

強化資料生命週期防護：

- 加密機制：針對關鍵資料實施儲存與傳輸之高強度加密，確保資訊在靜態與動態過程中均具備嚴密防護。
- 分級治理：建立資料分類制度，依據敏感度與合規要求進行分級管理，提升資料治理效率。
- 數位信任：採用電子簽名技術驗證資料完整性與使用者身分，確保交易與文件之可信度。

多層次技術防護網：

- 部署次世代防火牆、IPS 入侵防禦系統及 WAF 軟體層防火牆，即時阻斷惡意流量。
- 實施 MFA 多因子驗證，針對特權帳號(PAM)執行分級控管，並嚴格限制 USB 存取以防資料外洩。

資安文化深植：

- 落實新進與在職人員資安意識培訓，年度完訓率達 100%，持續深化全員資安防禦觀念。

3.3. 查核與驗證(Check) -落實安全檢測與合規驗證

- 安全檢測機制：透過實施 SAST 原始碼檢測，在開發階段早期發現潛在漏洞，確保應用程式安全性。
- 稽核與演練：定期執行社交工程演練及供應商稽核，並依據 ISO 標準進行有效性驗證。

3.4. 行動與改善(Act) -持續優化精進

- 系統化修正：針對風險評估與檢測發現之弱點，立即執行修補與強化作業，消除潛在風險。
- 管理審查：每年召開管理審查會議，由高階主管檢視整體績效。
- 動態調整：依據審查結果與演練經驗，動態調整資安策略，確保持續符合 ISO 驗證標準與企業發展需求。

4.投入資通安全管理資源：

本公司視資訊安全為營運基石，致力於建構安全可信賴的資訊環境。透過組織治理、管理制度、技術防護及持續演練，確保資訊資產之機密性、完整性與可用性。具體管理方案與資源投入情形如下：

管理面向	執行重點與具體方案
1. 組織架構與專責人力	完善資安治理體系： 設有資訊安全組織，並配置資安長 (CISO)、資安主管及專責人員及技術支援小組。 統籌與職責： 該單位專職統籌全公司之資訊安全策略規劃、防護技術導入、架構建置及相關稽核事項，以維護並持續強化資安防護能力，確保管理制度之有效運作。

管理面向	執行重點與具體方案
2. 管理制度與認證稽核	接軌國際標準： 持續維持 ISO 27001 資訊安全管理系統認證有效性，並已規劃於 2025 年完成新版標準轉版作業，確保管理制度與國際最新規範同步。 內外稽核機制： 每年定期實施內部稽核與接受第三方驗證機構稽核，目前歷次稽核結果均無重大缺失，驗證本公司內控作為之有效性。
3. 教育訓練與資安意識提升	內部員工 ・新進人員：到職時即須完成資安教育訓練課程，並簽署「資通安全保密協定」，確立保密責任。 ・在職訓練：全體員工每年須完成至少一次線上資安教育訓練及考核，確保認知與時俱進。 ・社交工程演練：年度執行兩次社交工程釣魚郵件測試，提升員工對惡意郵件之警覺性與辨識能力。 ・宣導機制：不定期發布資安公告，即時傳達最新威脅資訊與重要防護規定。 供應鏈資安管理 ・承攬商管理：既有與新進承攬商需完成規定之入廠資安教育訓練外，每年亦需接受一次定期回訓。 ・保密責任：所有委外廠商均須簽訂保密協議，明確規範其保護資訊資產之責任與義務。
4. 技術防護與設備維運	終端防護： 所有個人電腦均部署企業級防毒軟體並自動更新病毒碼，嚴格禁止使用未經授權之軟體，降低端點風險。 網路邊界管控： 持續強化上網行為管控策略與邊界防禦，主動排除可疑連線與潛在入侵管道。
5. 備份、應變與營運持續(BCM)	韌性架構： 針對關鍵系統已建置異地備份、備援機制及災難復原計畫，並定期檢視其完整性。 事件應變處置： 已制定標準化之「資安事件回應及通報程序」，確保發生資安事件時能即時控制損害範圍。 持續營運演練： 配合公司營運持續管理(BCM)機制，定期執行關鍵應用系統之災難復原演練，以驗證復原目標(RTO/RPO)之達成率，維持系統適用性與韌性。
6. 執行成效與指標	零重大事故： 本年度無發生重大資訊安全事件，亦無違反客戶資料遺失或外洩之投訴案件。 合規與有效性： 透過週期性的演練、稽核與檢討，確保各項資訊安全制度與控制措施持續有效，保障公司與客戶之權益。

（二）最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：最近年度及截至年報刊印日止無重大資安事件發生。