資通安全管理之資訊揭露

一、資通安全管理策略與架構

本公司在2023年成立「資通安全委員會」負責執行資通作業安全管理規劃，建立適當管理架構、審核資通安全政策及四階文件、分配安全責任，並協調本公司各項資通安全措施之實施，以利資訊安全管理制度能持續穩健運作。

「資通安全管理委員會」

「召集人」:由董事長及總裁擔任，負責本公司資通安全重要事項之議決、資源調度等。

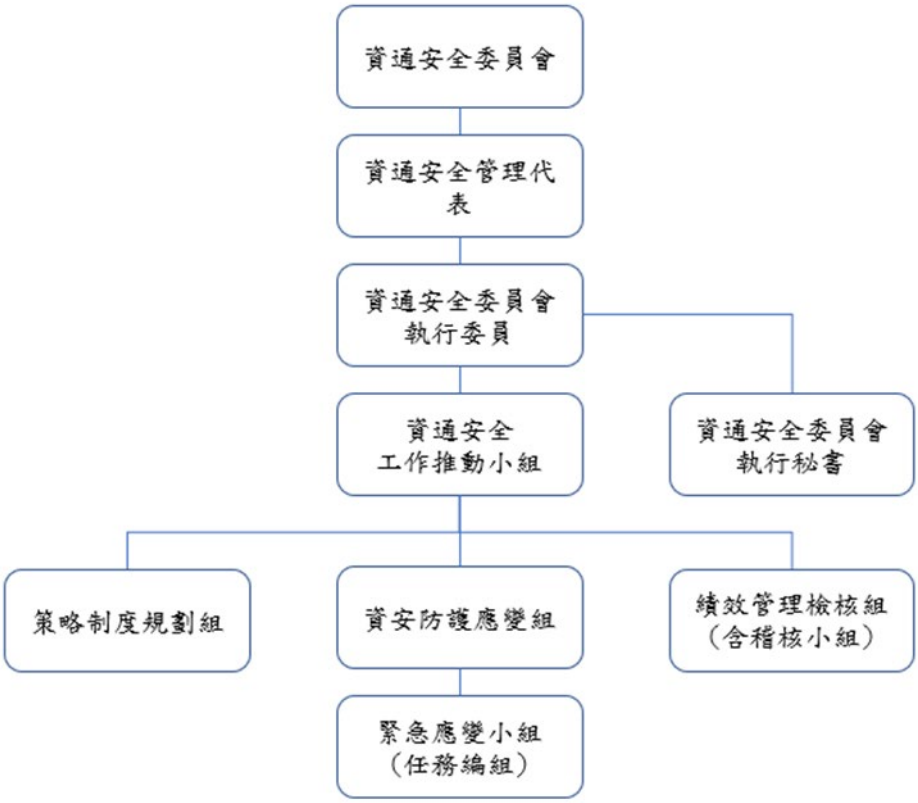
「資通安全管理代表」：由資訊安全長擔任，負責每年定期或視需要召開會議，審查資通安全管理相關事宜、視需要召開跨部門之資源協調會議及負責協調資通安全管理制度執行所需之相關資源分配。

「資通安全工作推動小組」：由資通安全委員會執行委員負責規劃及推動執行各項資訊安全作業。分依工作職掌分為「策略制度規劃組」、「資安防護應變組」及「績效管理檢核組」各司其職。

「緊急應變小組」：負責處理重大資安事件發生時之召集、聯絡、協調及督導各關鍵業務流程負責人執行應變作業，並調派各項使用資源及外部溝通。

本公司「資通安全委員會」每年至少召開一次資通安全管理審查會議，審查資通安全管理目標執行狀況及有效性評量結果，提出資通安全政策及目標執行之各項改進措施，必要時得召開臨時會議。

本公司「資通安全委員會」組織架構：



二、資通安全政策

本公司為強化資通安全管理，確保本公司資訊資產之機密性、完整性、可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，因此依據國際標準「ISO/IEC 27001:2022」、「公開發行公司建立內部控制制度處理準則」及相關法令與規定，並衡酌本公司之業務需求，訂定資通安全政策。其範圍適用於本公司全體同仁(係指員工、約聘僱人員、工讀生)、委外人員(單位)，以及所有相關資訊資產之安全管理。

資通安全政策目標在於：

- 確保公司重要業務運作之持續性。
- 確保公司面臨之資通安全風險已確實辨識、評估、處理。
- 確保同仁對資通安全之認知、有能力安全執行日常業務。
- 確保資通安全事件發生時能迅速妥善處理，保障公司、股東及利害關係人之權益。
- 確保資通安全管理措施符合政策及法令要求。

本公司依據PDCA(Plan規畫→Do執行→Check查核→Act行動)管理循環機制，檢視資安政策適用性、保護措施及執行成效，並適時導入合適之資安技術及設備，以期反映相關法令規定及資安防護需求。

「計劃階段」以資安風險防護為前提，規畫符合公司業務發展需求之資安管理系統，以降低公司資安威脅，永續經營。

「執行階段」建構多層資安防護，持續強化整合資安防禦技術及控管機制，確保營業、生產、採購、財務、股務、人資及文件檔案等重要作業流程能正常運作，以維護公司重要資產的機密性、完整性及可用性。

「查核階段」落實評量及內外部稽核監督，並依查核結果，檢討改善資安缺失及強化資安防護。

「行動階段」積極監控資安管理成效，以確保資安規範持續有效；並透過定期教育訓練及社交工程演練，提高員工資安防護警覺意識。

三、具體管理方案

為達資安政策與目標，建立全面性的資安防護，推行的管理事項及具體管理方案如下：

導入ISO27001資訊安全管理系統：

本公司已依ISO 27001標準，建立ISMS管理框架，以提升客戶和利益相關者對資安的信任度、加強資安風險管理、符合法規要求及優化資安業務流程，以控制並降低資訊安全事件所帶來的威脅和衝擊。並規劃在2025年取得ISO27001認證，獲得公正第三方對本公司資安系統之肯定。

資通環境設備安全管理：

1. 選擇安全適當地點設立機房，安置保護重要資通設備，減少環境(火災、水災、地震等)引發的危險，並管制記錄進入機房人員。
2. 電力供應設置符合設備規格需求及穩定電源之要件，並定期進行檢測；重要資通設備安置預備電源或使用不斷電系統。

核心系統安全管理：

1. 每年進行弱點掃描，強化漏洞修補作業。
2. 安裝MDR主動收集端點系統活動資訊，比對MITRE ATT&CK®的攻擊方式，能及時辨識威脅，有效防禦未知攻擊。
3. 透過掃毒軟體檢測、深度學習，防止惡意軟體攻擊，提供全面的安全保護。

網路通訊安全管理：

1. 授權專責人員管理網路設備，隨時監測網路狀況。
2. 導入SecuTex Network Protection 先進資安威脅防禦系統紀錄全部網路流量，增加網路可視性，透過SOC資安監控服務即時提供網路流量分析與可疑活動告警，在入侵情事發生時即時通報。並可於事後當作事件調查工具，協助事件調查時使用。
3. 連外網路建置NGFW防火牆及掃毒防護機制，提升對應用層級的威脅，防範網路通訊可能漏洞及強化偵測惡意軟體行為。
4. 網路主機關閉非必要服務程式，並即時更新程式版本。

資通系統開發安全管理：

1. 強化自行開發資訊系統或現有系統之安全需求，購入使用正版軟體。
2. 設定應用系統使用者通行密碼及限制使用權限。
3. 事前審慎評估委外資訊業務之可能潛在安全風險，與廠商簽訂資訊安全協定，並將相關的安全管理責任納入契約條款。

資通系統營運持續管理

1. 識別並評估所有資通系統/服務之復原時間目標(Recovery Time Objective, RTO)、復原點目標(Recovery Point Objective, RPO)、最大可容忍中斷時間(Maximum Tolerable Period of Disruption, MTPD)。以此規劃資通系統/服務之災難復原策略。
2. 制定資通系統、網路通訊、機房維運之營運持續計畫。
3. 定期針對關鍵資通系統/服務執行營運持續演練，以強化企業韌性。

資料安全管理：

1. 落實定期備份作業及強化備援回復機制，發生災害時，迅速回復正常作業。
2. 依報廢程序處理設備報廢，報廢儲存媒體設備前詳加檢查，以確保機密敏感性資料及有版權的軟體已被移除。
3. 防範網路使用者以任何儀器設備或軟體工具竊取網路通訊資料。

資安教育訓練與宣導

1.定期對員工辦理資安相關教育訓練課程。
2.因應資安風險狀況及事件，公告宣導資安相關信息及因應措施。
3.不定期進行社交工程釣魚郵件測試，以提升資安意識。

四、資通安全風險與因應措施

本公司已建立網路與電腦相關資安防護措施，且已加入「台灣電腦網路危機處理暨協調中心(TWCERT/CC)」會員，即時接收及傳遞「資安資訊分享與分析中心(TW-ISAC)」資安情資，亦加入「CISO台灣資安主管聯盟」、「CISA中華軟協資安長聯誼會」等資安組織，以達到縱向與橫向資安聯防，提升整體資安防護能量，但為確保能阻絕來自任何外部第三方惡意駭客以非法方式入侵公司內部網路系統，進行破壞公司營運成果、財務狀況、窺探竊取機密資訊與個人資料、植入惡意軟體敲詐勒索及其它損及公司商譽及權益等活動，本公司仍將持續檢視和評估資安規章及程序,確保其適當性和有效性,並持續進行下列資通安全相關防護措施，儘可能降低各項可能發生之資安風險所造成之損害，以維持公司正常運作，保障客戶、股東、供應商及員工等重要關係人之權益。

1.強化網路防火牆與網路控管機制。
2.強化端點偵測、防護及掃毒機制。
3.強化資安教育訓練及社交工程演練，強化員工資安意識。
4.導入自動化防禦系統強化資安維運平台。
5.委外第三方資安顧問輔導強化資安管理體系。

五、投入資通安全管理之資源

本公司2024年遵循「上市上櫃公司資通安全管控指引」「資通安全管理法及施行細則」等法令規範要求，計投入8,592,657元，購置或更新「伺服器主機及作業系統、端點防護、弱點掃描、網路及防火牆監控、雙因子身分驗證及社交工程(釣魚郵件滲透測試)、實體環境CCTV」等資安防護工具軟體、設備及專案輔導，以強化公司資安防護能力；並針對公司各部門338名種子員工進行資安教育訓練及宣導。

六、本公司2024年及2025年截至年報刊印日止，未因發生重大資安事件遭受損失。