資通安全管理

一、資通安全風險管理架構

1-1. 人力之配置

1-1-1. 雙資安長

本公司由營業管理處副總經理以及製造管理處副總經理擔任共同資安長，負責督導資通安全相關事項，其任務包括：

資通安全管理政策及目標之核定及督導。

資通安全相關規章與程序、制度文件核定。

資通安全相關防護措施之責任、資源分配及協調。

資通安全事件之檢討及監督。

其他資通安全事項之核定。

1-1-2. 資安專職主管

資安專職主管1人，其工作如下：

負責推動資通系統防護需求分級、資通安全管理系統導入、內部資通安全稽核、教育訓練。

資通系統分級及防護基準、安全性檢測、業務持續運作演練、資通安全監控管理機制、資通安全防護設施建置、資通安全事件通報及應變及法遵義務執行事宜。

1-2. 資通安全推動小組

1-2-1. 組成

由資安長召集各部級主管或指派適當人員代表成立資通安全推動小組，小組人員名單及職掌應填寫於「資通安全推動小組成員及分工表」，並適時更新之。

1-2-2. 任務

跨部門資通安全事項權責分工之協調。

應採用之資通安全技術、方法及程序之協調研議。

整體資通安全措施之協調研議。

資通安全計畫之協調研議。

資通安全政策及目標之研議。

訂定公司資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。

依據資通安全目標擬定年度工作計畫。

傳達資通安全政策與目標。

資通安全技術之研究、建置及評估相關事項。

資通安全相關規章與程序、制度之執行。

資訊及資通系統之盤點及風險評估。

資料及資通系統之安全防護事項之執行。

資通安全事件之通報及應變機制之執行。

辦理資通安全內部稽核。

每年提報資通安全維護計畫之實施情形。

二、資通安全政策

為防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

應因應資通安全威脅情勢變化，本公司同仁應參與資通安全教育訓練，以提高資通安全意識。

應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

定期進行內部稽核，確保相關作業皆能確實落實。

三、具體管理方案

本公司強化資訊安全管理，確保資訊資產之機密性、完整性及可用性，以提供本公司之業務持續運作之資訊環境。

3-1. 全面檢討網路及系統安全性，針對漏洞追蹤改善

訂定定期盤點資訊資產及資料清冊依資訊安全風險評估，進行風險管理，落實各項管控措施。

資訊系統建置情形指派專責管理人員，依安全等級定期記錄檢查。

外包專業電腦資訊廠商之維護服務。

3-2. 訂定主機安全等級，加強資訊安全稽核

將資訊安全及個資保護檢查控制作業，列為年度稽核項目。

年度內部控制制度自行檢查作業，將實施成效提報董事會，並出具內部控制制度聲明書。

3-3. 資訊單位定期進行弱點掃瞄及社交工程郵件演練及滲透測試

至少每半年做一次通盤性弱點掃瞄及社交工程郵件演練及滲透測試。

對較嚴重的特定弱點或病毒，則不定期依需要掃瞄。

3-4. 加強宣導一般人員對資訊安全的認知

不定期辦理資訊安全及個人資料保護教育訓練及宣導作業。

新進人員須簽署資通安全保密協定，遵守公司資訊或保密安全規範。

要求個人電腦均安裝防毒軟體並定期更新，並禁止使用未經授權的軟體。

3-5. 提升系統管理人員資訊安全管理能力

主機建立系統稽核檔，避免被植入後門或木馬程式。

即時更新作業系統及應用程式之修補程式。

注意網路上相關安全議題，及早防範。

按時分析系統紀錄檔。

加強系統管理者對主機系統紀錄(LOG)之解讀能力。

3-6. 加強網路安全管理

採用防火牆保護，隔離外部及內部網路，避免攻擊者以間接方式入侵內部網路。

將重要的資訊系統或資料從網際網路隔離出來。開放外界連線使用之資訊系統，可能以代理伺服器(ProxyServer)提供存取。

3-7. 落實系統取存控制

系統存取權限應嚴格控管。

使用者帳號密碼應定期更新，且不得使用不安全密碼。

需以遠端登入方式維護之主機，需限制存取清單，並加強控管。

本公司供應商及委外廠商應遵守本公司資訊安全規範約定。

3-8. 重要資訊系統或設備已建置適當備份及備援

四、投入資通安全管理之資源

對應資安管理事項及投入之資源方案概述如下：

4-1. 專責組織

專責資訊安全組織-「資通安全推動小組」，設立雙資訊安全長(CISO)、一名資安主管與二名專責資安人員，負責製修資安政策，規劃、協調與執行資訊安全防護措施。

4-2. 管理審查

「資通安全推動小組」每年定期向管理階層報告資通安全執行情形，審核資訊安全政策及其執行與落實情形，以確保資訊安全政策之有效性和適宜性，以符合相關法令及主管機關的要求。

4-3. 關係人議題

2024 年未發生重大資通安全事件與機密資料外洩情事，也未造成公司及客戶的損失。

4-4. 宣議與訓練

企業內部每年持續進行資訊安全宣議與訓練，針對所有使用資訊系統人員，透過教育訓練、內部會議及張貼公告等方式實施資訊安全宣導課程；負責資訊安全的主管及人員接受專業課程訓練；同時向服務供應商及連線作業相關單位宣導資安政策與目標，並檢視執行成效。

4-5. 資安規範

2024年已修訂資訊安全政策暨施行細則，以符合國內外法規要求及因應外在環境的變遷。

4-6. 資安檢測

2024年已進行第三方資訊安全風險檢測作業。