

銘旺實業股份有限公司

資通安全管理

依據資通安全管理法第 3 條定義，資通安全係指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

為了提升資通安全，針對風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等項目，進行政策宣導及管理。

一、資安風險管理架構

本公司為確保資訊環境之安全，資訊部門負責資訊安全事項的協調與推動，本公司至少設置一名資安主管及一名資安人員，其工作範圍及架構主要如下：

- (1) 風險評估和識別：定期進行資通安全風險評估，識別可能的威脅和弱點。
- (2) 風險處理和控制：制訂完善的控制程序，包含數據加密、身分驗證、授權機制以及發生資通安全威脅時之緊急應變計畫。
- (3) 教育培訓：負責教育訓練公司員工資通安全之知識，並確保員工了解資通安全的重要性並保持一定之警覺。

二、資通安全政策

- (1) 加強公司全體同仁資訊安全之認知。
- (2) 訂立資訊保密相關規範。

- (3) 設置緊急聯繫通道，一但有資訊安全之疑慮，應立即通報相關單位。
- (4) 確保依據部門職能規範資料存取，防止未經授權修改或使用。
- (5) 確保資訊系統之持續運作。
- (6) 定期執行資安稽核作業，以確保資訊安全各政策之落實。

三、具體管理方案及投入資通安全管理之資源

- (1) 定期及不定期的人員資訊安全訓練及宣導，提防釣魚郵件、勒索軟體、網站惡意連結。
- (2) 人員依部門職能規範各資訊存取權限定期稽核並及時調整。
- (3) 定期變更各系統密碼，強化密碼強度。
- (4) 完善防火牆與網路控管、防毒軟體等資訊安全設備，定期更新軟體，強化病毒攔截、網頁過濾、惡意軟體，防止災害擴散。
- (5) 設置備份系統及第三地備存。
- (6) 各子公司與母公司建置VPN，資料傳輸更安全。
- (7) 設備報廢前需將機密性、敏感性資料銷毀，版權移除。
- (8) 遠端登入需經核准授權。

四、投入資通安全管理之資源量化數據

- (1) 資安團隊人數：2 人，葉宥澤、蔡柏青。
- (2) 資安主管人數：1 人，葉宥澤。
- (3) 114 年度資安宣導次數：13 次。