資通安全管理

（一）資通安全管理策略與架構

確保公司營業機密與依循政府個人資料保護法，持續強化資訊安全防護能力，人員到組織全面提昇資安意識,以符合國、內外資訊安全法令規範。

（1）資安組織

本公司由總經理兼任資訊安全長 (轄下設置資訊安全主管 1 人、資訊安全人員 1 人，資通安全設置人員總數共3人)，其轄下掌管單位及負責職務：

1.資安稽核單位：依內控內稽要求，進行資安稽核。

2.資安管制單位：依法令規範與企業要求,進行資安軟硬體設置與設定。

3.資安管理單位：管理部門內作業，確保符合企業對於資安的要求。

資安人員：主要資安設定與管制作業之網管人員。

（2）資安防護重點

1.防災

1-1 地震：設備安裝要做必要之防傾與固定。

1-2 電力：必須提供必要的 UPS 供電,始能及時關閉設備、保護資料。

1-3 防火：提供必需的防火與滅火設備。

1-4 資料：異地備份。

2.防毒

安裝防毒軟體、定期更新版次與病毒碼。

3.防竊

必要的門禁設備與人員進出管理；資料加密與使用者管理。

4.防駭

必要的軟硬體、及時更新。

（3）資通安全政策-企業資訊安全管理策略與架構(PDCA)

1.「規畫階段」著重資安風險管理

建立資安管理系統 (Information Security Management System, ISMS)，從系統面、技術面、 程序面降低企業資安威脅，建立符合客戶需求的機密資訊保護服務。

2.「執行階段」則建構多層資安防護

持續導入將資安防禦創新技術，將資安控管機制整合內化於平日軟硬體維運作業流程，監控資訊安全，維護公司重要資產的機密性、完整性及可用性。

3.「查核階段」積極監控資安管理成效

依據查核結果進行資安指標分析與資訊安全成熟度評鑑。

4.「行動階段」則以檢討 與持續改善為本

落實監督、稽核確保資安規範持續有效；當員工違反相關規範及程序時，依據資安違規處理流程進行處置，並視違規情節進行人事處分（包括員工當年度考績或採取必要的法律行動）；此外，亦依據績效指標及成熟度評鑑結果，定期檢討及執行包含資訊安全措施、教育訓練及宣導等改善作為，確保公司重要機密資訊不外洩。

（4）具體管理方案及投入資通安全管理之資源

1.資安防護

1-1 網路安全：

防堵入侵攻擊於機房端，阻絕目前各式各樣的網路攻擊；設有垃圾郵件篩選及隔離機制，以防止收到夾帶病毒之電子郵件；強化網路防火牆與網路控管，避免病毒傳播。

1-2 裝置安全：

機台安裝時必須掃毒；依機台類型設置端點防毒措施。

1-3 應用程式安全：

應用程式開發須檢視資訊安全性，並持續強化。

1-4 資安保護技術強化：

強化資料機密分類與保護；引進新技術，優化文件檔案管理與管制。

1-5 重要資料回復：

定期演練重要備份資料回復，確保系統異常時能迅速恢復運作。

1-6 資料安全保護技術更新

導入虛擬化及光纖儲存備份架構，提升系統資料安全性。

2.檢討與改善-教育訓練與宣導

加強員工對郵件、軟體、檔案...惡意攻擊的警覺性，提升員工資安意識。

3.資安成效-盤點與稽核

定期盤點軟硬體與使用者端設備稽核；有重大異常須檢討管制程序與技術提升。

（二）資安相關會議開會次數

民國 113年共舉辦3次資通安全相關會議，包含2次資安講習會議及1次資安事件報告會議。

（三）投保資安險(含電子設備險)金額

民國 113 年資安險(含電子設備險)投保金額：新台幣 32,556,217 元。

（四）重大資通安全事件

民國 113年10月21日本公司部份資訊系統遭受駭客網路攻擊，本公司自行偵測到部份郵件系統使用者帳號遭受駭客網路攻擊，資安部門於第一時間即全面啟動相關防禦機制與修改使用者帳號密碼作業，目前對公司營運無重大影響，本公司後續仍將持續提升網路與資訊基礎架構之安全與密碼管控以確保資訊安全。