資訊安全風險管理架構及資通安全管理

1.安全風險管理架構

由財務暨行政處主管擔任管理代表，由資訊部主管執行資訊安全相關業務，執行已制定發行資訊安全管理目標及政策。定期由稽核處長檢討資訊安全管理制度及個人資料管理制度執行情形。**資訊安全風險管理架構請參閱第4頁。**

2.資通安全政策

2.1 為確保本公司資訊資料、系統、設備及網路通訊之安全，有效降低因人為疏失、蓄意或天然災害等致資訊資產遭不當使用、洩漏、竄改或破壞等之風險，應制定資訊安全政策，以建立資訊安全管理之方向。

2.2 資訊安全定義

資訊安全為一系列有計畫、持續性之控制措施，使資訊資產(含軟硬體設備)的使用得以妥善保護。

2.3 資訊安全目標

確保本公司業務資訊之機密性、完整性與可用性。

A.機密性：確保被授權之人員才可使用工作相關所需之資訊資產。

B.完整性：確保使用之資訊正確無誤、未遭竄改。

C.可用性：確保被授權之人員於工作需要時能即時取得所需資訊資產。

2.4 資訊安全範圍

資訊安全範圍涵蓋人員管理及資訊技術面等領域。

2.5 資訊安全政策內容

A.資訊安全規定必須遵守政府相關法規(如：刑法、國家機密保護法、專利法、商標法、著作權法、電腦處理個人資料保護法等)之規定。

B.成立資訊小組負責資訊安全制度之建立及推動事宜。

C.定期實施資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

D.建立資訊硬體設施及軟體之管理機制，以統籌分配、運用資源。

E.新資訊系統應於建置前將資訊安全因素納入，防範危害系統安全之情況發生。

F.建立電腦機房實體及環境安全防護措施，並定期施以相關保養。

G.明確規範資訊系統及網路服務之使用權限，防止未經授權之存取動作。

H.訂定資訊安全內部稽核計畫，定期檢視個人電腦使用情形。

I.訂定資訊安全災變回復計畫並實際演練，確保本公司業務持續運作。

3.具體管理方案

3.1 多層資安防護

A.網路安全：強化網路防火牆與網路控管，防止來自網際網路的惡意攻擊與入侵。

B.裝置安全：依電腦類型布建端點防護軟體，與防火牆區域聯防，加上雲端人工智慧與機器學習，預測惡意程式入侵行為，阻隔勒索軟體的入侵風險。另外加強重要核心個人電腦的備份。

C.伺服器安全：升級作業系統，完成伺服器虛擬化，並完成異地備份原則。

定期進行災難還原演練，以確保資料完整性與可用性。

D.異地工作資訊安全：如有分流上班之需求，員工使用公發筆電在家上班，緊急安裝端點防護軟體及防毒軟體，在家上班仍能受到防火牆及雲端軟體保護，持續維護資通安全的政策。

3.2 教育訓練與宣導：加強員工社交工程攻擊的警覺性，執行釣魚郵件防禦偵測。

4.投入資通安全管理之資源

4.1 設置人員總數2名，包含資安主管1名及資安人員1名。

4.1 針對新進員工皆完成資訊安全與保護教育訓練課程。2023年度教育訓練參與人數共計60人。

4.2 布建全公司端點防護軟體與防毒軟體。

5.運作情形：

本公司於2023年12月13日董事會報告本公司資訊安全管理小組運作情形。

資訊安全風險管理架構

1.**【資訊安全目的與範圍】**：

目的：本公司為強化資訊安全管理、確保業務永續運作特訂定本規範。

範圍：為確保本公司資訊安全，保障資訊安全維護。

2.**【資訊安全風險架構】**：

- 由財務行政處副總經理擔任資訊安全主管，資訊部主管擔任資訊安全專責人員，召集成立跨部門資訊安全管理小組，以確認本公司各單位皆落實資訊安全管理辦法，及資訊安全管理運作之有效性。
- 本小組負責制定資訊安全管理政策，定期檢討修正。
- 每年定期向董事會報告執行情形。

3.**【資訊安全政策目標】**：

- 確保本公司營運業務持續運作，且本公司提供的資訊服務可穩定使用。
- 確保本公司所保管的資訊資產之機密性、完整性與可用性，並保障人員資料之隱私。
- 建立資訊業務永續運作計畫，執行符合相關法令或法規要求之資訊業務活動運作。
- 所有使用資訊系統之人員，每年接受資訊安全宣導課程，另負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。

- 資訊部門主管取得資通安全專業證照清單中的 Certified Ethical Hacker (CEH)與EC-Council Certified Incident Handler (ECIH)並維持有效性。

4.**【資訊安全控制措施】**：

本公司實施之資訊安全管理措施，包含如下：

類型	說明	相關作業
人員管理與教育	使用者管理	人員帳號權限管理與審核
	教育訓練	新人報到時進行新人訓
實體與環境安全	電腦機房管理	設定允入清單及進出紀錄
	辦公區域管理	依照行政區與實驗區動線
	辦公桌面管理	依照行政區與實驗區需求
網路安全管理	防火牆管理	密碼長度與密碼生命週期
	伺服器管理	定時連線檢測與更新
	個人電腦管理	每年檢查軟體安裝與抽樣
	軟體下載管理	依照防火牆設定
	電子郵件管理	安裝伺服器更新程式
系統存取控制	資訊系統存取控制	帳號權限申請單
	使用人員存取管理	帳號權限申請單
業務永續運作	業務永續運作規劃	資訊安全管理辦法