資通安全管理

1.敘明資通安全風險管理架構、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：

(1)資通安全風險管理架構

本公司已於 112 年 11 月 9 日董事會決議通過設置綜理資訊安全政策推動及資源調度事務之資訊安全長，並暫由資訊部門原有人力兼任資安專責單位，負責資通安全風險管理作業。

(2)資通安全政策

為落實資安管理，公司訂有內稽內控制度—電腦化資訊系統處理循環及資通安全管控指引，藉由資訊部門執行推動，全體同仁共同努力遵守達成下列政策：①電腦系統管理政策②網路安全管理政策③系統存取控制管理政策④系統發展及維護安全管理政策⑤業務永續運作之規劃。

(3)具體管理方案

①電腦系統管理政策：

a.將資安要求納入資通系統開發及維護需求規格，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等。

b.定期執行資通系統安全性要求測試，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾測試等。

c.妥善儲存及管理資通系統開發及維護相關文件。

d.對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。

②網路安全管理政策：

a.依網路服務需要區隔獨立的邏輯網域(如：DMZ、內部或外部網路等)，並將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施。

b.針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。

③系統存取控制管理政策：

a.訂定到職、在職及離職管理程序，並簽署保密協議明確告知保密事項。

b.建立使用者通行碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制，並評估於核心資通系統採取多重認證技術。

c.定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。

d.建立資通系統及相關設備適當之監控措施，如：身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。

e.針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。

f.留意安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。

g.訂定資通設備回收再使用及汰除之安全控制作業程序，以確保機敏性資料確實刪除。

h.訂定人員裝置使用管理規範，如：軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等管控使用規則。

④系統發展及維護安全管理政策：

a.訂定資訊作業委外安全管理程序，包含委外選商、監督管理及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施。

b.訂定委外廠商之資通安全責任及保密規定，於採購文件中載明服務水準協議(SLA)、資安要求及對委外廠商資安稽核權。

c.公司於委外關係終止或解除時，確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。

(4)投入資通安全管理之資源

本公司已規畫建立基礎防護架構之經費，確保企業營運皆在安全範圍。

2.列明最近二年度及截至公開說明書刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：本公司最近二年度及截至公開說明書刊印日止無重大資安事件導致營業損害之情事。