資通安全風險揭露

(一)資通安全風險管理架構

1、企業資訊管理架構

本公司成立「資安小組」內設置資安主管與資安專員，負責資訊安全相關維運及保護政策的規範、執行暨風險管理，遵循內部稽核與會計師年度查核，並定期評估資訊安全政策及作業適當性與有效性，擬定專案計畫持續強化保護措施讓資訊安全風險降低。同時參考資訊安全管理系統（Information Security Management System / 簡稱：ISMS）標準相關規範建置標準之資訊安全管理基準，以 PDCA 精神，持續執行資訊基礎建設、資訊安全措施，確保公司重要資訊的機密性(Security)、完整性(Integrity)及可用性(Availability)。

每年落實資訊安全宣導並定期維護及更新系統相關設備，培養員工使用合法軟體的正確觀念；資安小組也定期執行資訊安全檢查，檢查確認結果呈送權責主管覆核，並依檢查結果列舉清單，予以瞭解進而提出改善，並追蹤確認後續改善之情形，確保內外部相關人員與單位皆遵循公司資訊安全政策。

每年依稽核計畫檢視公司的資通安全，並進行相關項目的查核，稽核結果定期向董事會進行報告，視情節影響層面也向董事長報告；資安專員也每日持續監察內部控制功能運作現況，防止其發生異常變化時，能在最短時間發現並及時處置。

2、資訊安全組織架構

資安小組統籌並執行公司資訊安全政策，不定時宣導資訊安全訊息，培養員工資安意識。並不定期逐一確認內部稽核提出安全問卷報告，不定時評估公司內部資訊作業控制有效性，以求保障資訊的機密性、完整性與可用性。

(二)資通安全政策

企業資訊安全管理策略及具體管理方案:

本公司依下列管理方案促使公司降低面臨的資安風險。透過規範努力提升資訊科技與安全，提升員工工作效率，保障所有投資人的相關權益。

A.尊重智慧財產權

公司網路資源及資訊資產使用要求員工應尊重智慧財產權，力求避免可能涉及侵害智慧財產權的行為：要求員工不使用非法之電腦軟體，並定期執行內部清查是否有不適當的軟體或設備安裝。

B.資訊系統權限管控

資料修改申請:申請人一律須填寫申請單並經主管核可進行申請，系統修改須經

權責主管及資訊部主管核准後方可執行，以降低資料未經授權而遭修改之風險。

權限使用申請：使用者依權限開放相關功能，非相關使用者，無權使用跟業務無關之系統。

C.帳號密碼之安全控制

帳號：每位員工各自的使用帳號及密碼，離職或調職，則帳號立即停用或更新，並移除相關所屬群組。

密碼：要求員工使用有嚴格複雜度的密碼且定期更新，以降低風險。

D.外部威脅管控

定期更新軟硬體系統，阻斷防堵安全性漏洞；定時防毒軟體更新及掃描，防垃圾郵件加強防郵件病毒入侵。定期審視對外開放連線適當性與必要性，關閉不必要的對外連線。

E.個資保護

組織公司跨部門個資緊急聯絡小組，定期盤點公司內部個資資料；並加強在系統上個資的存取權限控管與隱藏非必要顯示之欄位。

F.資通安全稽核

每年定期數次內部資訊稽核與一次的外部資訊稽核，並依結果加以檢討改進。

G.具體資安措施

防毒軟體、防火牆防護、內外網管制、儲存媒體控管、郵件安全保護、網站保

護機制、資料備份落實、資通安全宣導、軟硬體定期更新、定期設備檢查紀錄、使用嚴格密碼原則。

H.機房及重要區域之安全控管、人員進出管控、環境維護

(如溫度、溼度控制通知) 、消防自動啟動設置等項目建置並設定適當之管理措施。

I.定期瀏覽資安情資分享情報並加入會員

取得資安預警情報、資安威脅與弱點公告，例如：臺灣電腦網路危機處理暨協調中心 TWCERT/CC 等等。

目前本公司已加入：TWCERT/CC 成為會員之一。

J.資通設備回收再使用與汰除訂定安全控制作業程序

以確保機敏性資料刪除且無法回復。公司內部公佈文件加印浮水印；定期請廠商拍照出具證明公司內部文件紙類銷毀與破壞報廢儲存媒體至不可回復狀態。

K.設定異地備份並確實執行實施

每日觀察是否有異常備份狀況；並使用防勒索備份軟體備份。

L.到職、在職與離職訂定管理程序，且簽署保密協議，明確規範保密事項。

(三)企業資訊安全風險管理與持續改善架構

資訊安全目標：「資訊安全、人人有責」。企業資訊安全不定時發佈資安訊息，讓組織內各職掌皆有資安意識，有效落實資安防護，才能建立安全的資訊使用環境；透過稽

核落實軟體授權使用，避免使用者安裝到有植入危害程式的非法軟體，並定時要求集團相關公司回報目前授權使用狀況，也不定時要求各相關集團公司，回報目前資安狀況。依據規畫、執行、查核與行動（Plan-DoCheck-Act, PDCA）的管理循環機制，檢視資訊安全政策適用性與保護措施。也每年規畫實施不定期執行緊急應變演練，培養員工相對映的緊急應變處置，實機、實物操作演練，針對缺失檢討改進，增進人員應變力。

(四)投入資通安全管理之資源

本公司資通安全政策為「維護公司資通之機密性、完整性、可用性與適法性，避免發生人為疏失、蓄意破壞與自然災害時，遭致資通與資產遭致不當使用、洩漏、竄改、毀損、消失等，影響本公司作業，並導致公司權益損害」。本公司重要之資通系統已遷移至取得第三方驗證雲端平台，並持續維持其驗證有效性，平台亦通過美國註冊會計師協會(AICPA)發展之 SOC 2 服務組織之 Type 2 合規標準認證，以維持公司穩健之資訊安全，強化資通安全事件之應變處理能力，保護公司與客戶之資產安全。

目前已取得 SOC 2 Type 2 簽署函蓋從 2024 年 8 月 1 日至 2025 年 7 月 31 日，及過渡聲明書從 2025 年 8 月 1 日至 2025 年 11 月 30 日。

本公司內部訂定發佈多項資安規範及制度，以規範公司內部人員資訊使用安全行為，並不定時檢視相關制度是否符合現況與環境變遷，適時調整。針對資訊安全每年定期執行內部稽核，與每年執行外部稽核。並依稽核結果改善相關資訊安全規劃。

今年度投入資安相關量化數據：

114年資通安全管理之資源量化數據		
項目	單位	數據
重要設備已移至美國註冊會計師協會(AICPA)發展之SOC 2服務組織之Type 2合規標準認證平台	-	已取得SOC 2 Type 2簽署函蓋從2024年8月1日至2025年7月31日，及過渡聲明書從2025年8月1日至2025年11月30日
資安人員	人	1
重要系統弱掃	次	2
重要系統滲透測試	次	1
機房消防設備投保	NTD	12,600
機房重要資通設備年度維護合約	NTD	650,000
重要系統廠商系統維護合約	NTD	529,127

(五)資通安全管理未來目標

預計 115 年執行全公司增加社交工程演練外，並加強升級相關資安設備防護。並不定期派送資訊安全相關公告以資安意識宣導，藉此提升並鞏固企業員工資安意識警覺性、培養良好資訊安全使用的習慣。

(六) 重大資安事故

截至 2025 年底止，無重大資安事故。