鈺齊國際股份有限公司

資通安全風險管理政策

本公司設置資訊部門負責公司資訊發展策略、資訊安全政策以及資訊系統之管理與改善，並持續關注資訊環境變化趨勢。本公司定期執行安全性檢測、資通安全問券健診、社交安全及資安事件演練，強化公司同仁資安危機意識及資安處理人員應變能力，以期能事先防範及第一時間有效偵測並阻絕擴散。本公司風險管理工作小組於 2024 年 12 月 26 日向董事會報告 2024 年未發生影響公司營運之重大資安風險情事。

在資訊安全風險控管上，本公司訂定資安政策如下：

(一)資通安全檢查之控制

防範企業資訊系統不受外來資訊病毒或駭客入侵，影響企業正常運作或損及公司權益。

(二)系統復原計劃及測試程式之控制

確保企業資訊系統遭受不可抗力之災害或其他人員破壞時，能在最短時間內復原至正常企業營運。

(三)檔案及設備之安全控制

防範檔案資料遭電腦病毒侵入，維護資料檔案及各項電腦設備之安全。

(四)程式及資料存取控制

建立本公司使用者對系統程式及資料存取之權限及範圍，防止系統公用程式、工具及指令被不當存取。

其具體管理方案分述如下：

(一)資通安全檢查之控制

A. 公司郵件伺服器裝設防火牆及防毒軟體以隔絕外來侵害。
B. 外包商定期檢視伺服器上郵件收發情形，異常狀況呈報權責主管處理。
C. 資訊部門利用設備管控上網行為及查看網路狀態，防止未經授權之存取。
D. 定期檢視及評估網際網路可能之安全性弱點，以採取防護措施。

(二)系統復原計劃及測試程式之控制

A. 制定系統復原辦法並定期修訂。
B. 系統定期做備份，並指定專人保管。
C. 電腦系統及其設計，加入適當之預防措施，減低不當破壞之機率。

(三)檔案及設備之安全控制

A. 於日常作業依檔案及設備之安全控制之規定進行檔案備份。
B. 各項電腦設備及周邊設備、消防設備、支援設備定期檢查、維修及保養。
C. 系統發生異常狀況時，應加以瞭解原因、改進及記錄。
D. 機房人員進出確實管制。
E. 定期更新偵測病毒軟體之版本，並定期掃描電腦硬碟。

(四)程式及資料存取控制

A. 程式檔案的存取使用應依帳號權限加以管制。
B. 重要之系統公用程式、工具及指令應依其使用者權限限制存取查詢。
C. 一般應用系統之使用者除執行應用系統外，無存取系統公用程式、工具及指令之權限。
D. 程式檔案的存取使用均留下可追蹤的記錄。
E. 權責主管定期覆核相關記錄。
F. 密碼不可顯示於電腦螢幕上，亦不可未經亂碼化即列印於任何報表。

此外，新進員工需先進行電子郵件及資訊系統相關基本培訓後始核發帳號，以確保資訊安全觀念融入日常作業中。

2024 年度執行情形如下：

(1) 2024 年共進行 2 次內部培訓分享以及為其他部門進行資安教育，培訓內容包含系統總體安全、資安、視訊軟體操作、郵件及網站防釣魚安全培訓，共計 175 小時，250 人次，2024 年全集團未發生危害集團的資安事件。
(2) 每天進行異地備份資料，每半年進行災難還原演練，確保異地備份資料能正常還原。
(3) 持續投入建設雲桌面：雲桌面使用者資料存放在伺服器上，並對雲桌面進行備份，配合 AD 域更精密的管控 USB 等設備輸入和輸出，減少中病毒機率，提升整體安全性。
(4) 每年的 2 月份全集團定期投保【ESET 防病毒系統】。