資訊安全管理相關資訊揭露:

(一)政策適用範圍

本辦法適用於本公司各單位之全體同仁、委外廠商、第三方人員及相關資訊資產安全之管理。

(二)資訊安全管理架構

(1) 資通安全長：由資通管理處主管擔任之，負責定期召開及主持資通安全管理議，並依會議結果作出裁決交付執行。

(2) 資通安全小組：由各業務單位主管共同組成，根據資通安全管理事宜提出議案進行討論和建議，並對決議負責規劃、推動及協調。

(3) 資通安全會議由資通安全長召開及主持，核定各項資通安全事項、宣達新安全政策、檢討矯正預防措施、資通安全危機事件應變及依本辦法規範相關人員之獎懲事項。

(三)資訊安全政策

(1) 確保公司相關資訊之機密性，保障公司與個人機密資料。

(2) 確保公司業務相關資訊之完整性及可用性，提高行政效能與品質。

(3) 配合國家政策之推動，提昇資訊安全防護能力，達成業務持續運作之目標。

(四)資訊安全具體管理方案

目前公司並未購買資安險，但在人才培訓與資安上已建立聯防機制。

(1) 實體及環境安全管理

電腦設備安全及機房管制管理包含硬體環境控制、電源供應、電纜線安全、設備維護。資訊資產實體設備報廢，為避免個資外洩，由資訊單位依程序辦理。

(2) 軟體使用安全管理

本公司嚴禁使用非法軟體，公司內部使用之軟體已由廠商授權使用，未經資訊管理部門主管同意，不得任意下載軟體或擅自安裝使用，以避免侵犯智慧財產、誤觸法律或啓動惡意執行檔。

(3) 周邊安全管理

管制人員進出需設有可辨識身分之識別卡，達成安全控管的目的，資訊支援人員或維護服務人員，只有在資訊管理部門人員陪同或是被授權的情形下才能進入，並應留有進出的記錄。

(4) 網路安全與資料安全管理

1. 網路安全管理:責成專人管理網路系統，維持網路系統正常運作，設置防火牆、資訊安全防護等設備，以防止非法入侵破公司造成商業機密及個資外洩風險，且內部網路、主機系統保有所有人員登出入系統完整紀錄。
2. 資料安全管理:存取控制與資料存放安全，嚴格執行密碼管理及定期資料與軟體備份，重要資訊之儲存採取異地存放機制。
3. 本公司無法完全保證避免來自第三方癱瘓網路系統之惡意攻擊，但 107 年度及截至年報刊印日止並未發生網路惡意攻擊事件，影響公司正常營運。

本政策未盡之事宜，悉依有關法令及本公司相關規定辦理。