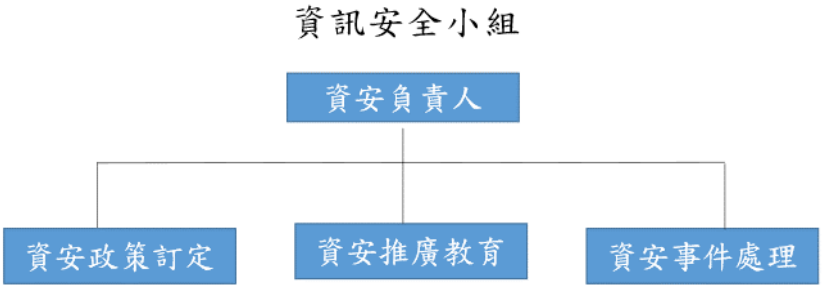
資安防護建置規範及實際執行與因應措施:

●資訊安全風險管理小組

本集團透過建立資通安全管理體制建置專責之資安單位(資訊部)，適用範圍涵蓋本公司、子公司、客戶及供應商，針對營運過程中所涉及之個資隱私之蒐集、處理、利用及保護，遵循政府相關法令，依循公司政策落實執行，致力維護資料安全及隱私權利，強化執行資安防護、資安檢測、宣導及資通安全教育，透過每月內部經營會議及每季定期向董事會彙報資安治理概況，由專人專職規劃設計與管理，並確保資訊系統之正常運作、降低資安事件及資料保全，亦適時更新、提升軟硬體設備資源，以確保本集團資料的機密性、完整性、可用性及個人資料的保護。

●本集團為落實個人資料之保護與管理，於 2024 年 8 月 12 日訂立「個人資料保護法」(簡稱個資法)。

本小組主要權責如下：



資安政策訂定組:負責各項資安政策的訂定，並持續依法令規定及資訊技術調整相關政策。

資安推廣教育組:負責公司資安政策教育訓練及公司員工是否有相關資安概念測試。

資安事件處理組:負責公司資安事件的處理及零時差攻擊時的緊急修補。

●資訊安全政策

(1)網路連線政策辦法:

公司對外連線、對外開放主機、無線網路服務、VPN 連線政策、弱點偵測。

(2)資料備份政策辦法:

備份模式採用本地備份、異地備份及離線備份三種模式。

(3)備份資料驗證辦法:

本地備份、同廠異地備份、遠距異地備份、離線備份。

(4)E-Mail 資安政策辦法:

訂定相關電子郵件處理政策、公司過濾郵件政策、資安宣導、E-Mail 資訊安全使用守則。

(5)機密性裝置棄置辦法:

本公司儲存重要資料之裝置因故障或汰舊換新時，為確保資料不外洩，特訂定此辦法以備在出售各類資訊產品時，有所處理依據。

●資訊安全具體管理方案

(1)Palo Alto 網路防火牆

防堵各類不正常的網路使用，確保企業對外網路的安全與順暢及企業員工上網的合理性管理，提升人員及網路資源的使用效率，符合資通安全檢查之控制。

(2)中華電信 hinet 企業資安服務

導入中華電信網路資安服務，阻絕 99%以上的網路攻擊於境外，確保公司資訊環境安全無虞，符合資通安全檢查之控制。

(3)達新 ERP 備援系統

建立本集團管理資訊系統備援制度，確保企業營運的系統安全及永續發展，每年定期排練復原程序，確保人員技術落實及經驗傳承，符合系統復原計劃及測試程式之控制。

(4)鎧睿郵件防禦系統

垃圾郵件管理機制，阻絕垃圾郵件於境外及惡意電子郵

件之防禦，防堵並降低各類資安事件，符合資通安全檢查之控制。

(5)本集團郵件備援系統

建立本集團網路郵件安全檢測系統線上備援制度，確保企業的郵件系統安全及時及永續配合電子郵件法規，備分歷史郵件存放十年期資料，以確保各項交易資訊的查詢應用，符合系統復原計劃及測試程式之控制。

(6)防毒系統

建立企業內部的電腦病毒防禦處理機制及入侵偵測控制，以防駭客攻擊，確保電腦資源有效運用，符合資通安全檢查之控制。

(7)本集團文件檔案備份機制

建立文件檔案本地備份、同廠異地備份、遠距異地備份、離線備份等機制，採用網路硬碟、外接式硬碟二種媒體，每日定時執行備份資料驗證，確保檔案之存取控制、帳密管理之安全性。

●投入資通安全管理之資源、執行情形及目標

(1)專責人力

設有專責之資安單位(資訊部) ，資安小組設置 4 位，負責公司資訊安全規劃、技術導入及資通安全內控制度等稽核事項，以維護及持續強化資訊安全。

(2)資安會議

每星期定期內部資安檢討及每月經營會議中回報執行成效，每季定期向董事會彙報資安治理概況。

(3)客戶滿意

無重大資安事件，無違反客戶資料遺失之投訴案件。

(4)資安公告

不定期透過公司內部郵件平台及達新入口網站傳達資安防護重要規定與注意事項。

(5)資訊安全教育、宣導、演練測試執行情形：

2024 年度

教育宣導 (視訊會議)	時 數	人 數
社交工程及網路攝影機資安	1.5H	167
社交工程及生成式 AI	1.0H	75

2025 年度截至 3 月底

教育宣導 (視訊會議)	時 數	人 數
社交工程及個人資安	1.0H	176

社交工程演練測試結果		測 試 員 工		
執行日期	內　　容	總數量	數量	佔比
2024/03/18	點擊連結	248	24	9.6%
	輸入資料		9	3.6%
2024/10/16	點擊連結	221	7	3.1%
	輸入資料		4	1.8%
2025/03/10	點擊連結	221	12	5.4%
	輸入資料		2	0.9%
2025/03/17	點擊連結	221	4	1.8%
	輸入資料		2	0.9%

●114 年度資訊安全執行目標：

1.持續控管資安現況及落實追蹤資安個案處理。

2.定期評估資安系統、調整資安策略，以確保有效性及資安維護。

3.加強員工資安意識，年度安排 2 次資安教育課程，於日常營運、執行業務時應遵循之相關規範，以保系統的穩定性與安全性。

4.強化本集團營運潛在風險之維護，制定存取控制、加密保護，防護資訊系統及相關資產，防止本集團機敏資料之外洩。