目錄
關於本報告書
2025 六暉永續績效

01 永續策略與實踐
02 關於六暉
03 產品責任與服務
04 永續環境
05 友善職場
06 社會共融
附錄

2.6 資訊安全與客戶隱私保護

在數位化營運與跨國協作日益密切的今天，資訊安全不只是技術管理，更是企業對客戶、合作夥伴及所有利害關係人的信任承諾。六暉將資訊安全與客戶隱私保護視為穩健經營的重要基礎，並納入營運風險管理，透過制度規範、權限控管、系統防護、資料備份、教育訓練及事件應變機制，降低資訊系統中斷、資料外洩及未經授權存取等風險，守護商業機密與客戶資料安全，持續提升資訊安全管理效能與營運韌性。

重大主題管理／資訊安全與客戶隱私保護	
重大主題意義	資訊安全管理攸關本集團營運穩定、商業機密及客戶資料安全。透過完善的資訊安全防護、資料管理及事件應變機制，可降低網路攻擊、資料外洩及系統中斷等風險，維護營運持續性，並建立客戶及合作夥伴的信任。
政策／承諾	本集團秉持「落實資通安全、強化服務品質」、「加強資安訓練、確保持續營運」及「做好緊急應變、迅速災害復原」之管理方針，持續完善資訊安全治理及風險管理機制，透過資訊安全管理制度、風險管理、教育訓練、事件應變及個人資料保護等管理措施，守護資訊資產、客戶資料及商業機密安全，建構安全、可信賴且具營運韌性之資訊環境。
正負面衝擊	**正面：** ▶ 建立完善的資訊安全防護機制，保護車廠客製化產品圖面、商業機密、資訊資產及員工個人資料安全，透過資料存取控管、資訊安全防護及風險管理機制，有效降低資訊安全事件及營運中斷風險，提升資訊系統穩定性與營運韌性，並持續強化客戶、員工、供應商及其他利害關係人對六暉集團之信任，鞏固長期穩定的合作關係。

目錄
關於本報告書
2025 六暉永續績效
01 永續策略與實踐
02 關於六暉
03 產品責任與服務
04 永續環境
05 友善職場
06 社會共融
附錄

重大主題管理／資訊安全與客戶隱私保護

正負面衝擊	**負面：** ▶ 若未落實資訊安全管理，可能因惡意程式、釣魚郵件、駭客攻擊、未經授權存取或重大災害等因素，導致系統中斷、資料外洩、商業機密流失、客戶隱私受損、法規遵循風險及商譽受損等負面影響，嚴重時更可能造成生產系統中斷、營運停擺及重大違約賠償責任，進而影響企業營運韌性及客戶信任。	
目標	**短期：** ▶ 維持全年無重大資訊安全事件及無個人資料外洩事件 ▶ 完成資訊資產盤點及風險評估 ▶ 建立資訊安全績效追蹤機制 ▶ 辦理資訊系統維護、弱點修補、備份及災害復原演練 ▶ 強化帳號權限管理、資訊設備管理及資安監控 ▶ 建立委外廠商及供應鏈資訊安全風險管理機制 ▶ 落實客戶個人資料及機密資訊保護措施 ▶ 辦理資訊安全、個人資料保護宣導或教育訓練	**中期：** ▶ 提升資安風險辨識、弱點管理及異常事件監控能力 ▶ 精進資訊安全管理制度及績效管理 ▶ 評估導入 ISO 27001 資訊安全管理系統之可行性 ▶ 強化資訊系統應變流程、災害復原及營運持續管理能力 ▶ 強化委外廠商及供應鏈資訊安全風險管理 ▶ 強化客戶個人資料及機密資訊保護管理
	長期： ▶ 精進資訊安全風險評估、個人資料保護及資訊資產管理機制 ▶ 提升資訊系統韌性、資安事件應變及營運持續管理能力 ▶ 提升委外廠商及供應鏈資訊安全管理成效 ▶ 提升客戶個人資料及機密資訊保護管理成效	

目錄
關於本報告書
2025 六暉永續績效
01 永續策略與實踐
02 關於六暉
03 產品責任與服務
04 永續環境
05 友善職場
06 社會共融
附錄

重大主題管理／資訊安全與客戶隱私保護

行動辦法

預防管理

- 由資訊部門統籌資訊安全管理與日常維運，持續強化端點防護、網路安全、郵件安全、防火牆管理、權限控管及資料備份等管理措施。
- 建立資訊系統、資料保存、帳號權限、外部連線及資訊設備使用管理規範，降低資訊安全風險並強化資訊資產保護。
- 透過資訊安全教育訓練、社交工程演練及宣導活動，提升員工資訊安全意識及風險辨識能力。

風險因應

- 建立資訊安全事件通報及緊急應變機制，發生異常事件時即時通報、處理及追蹤改善。
- 定期執行系統弱點檢視、安全更新及修補作業，降低潛在資安風險。
- 持續辦理資料備份驗證及災害復原演練，提升資訊系統復原能力及營運韌性。

2025 年實際績效

項目	2025 成果
資安教育訓練	187 人次
訓練時數	88.9 小時
重大資安事件	0 件
個資外洩事件	0 件
資安相關裁罰	0 件
資訊投入金額	NT$5,140.11 仟元

目錄
關於本報告書
2025 六暉永續績效
01 永續策略與實踐
02 關於六暉
03 產品責任與服務
04 永續環境
05 友善職場
06 社會共融
附錄

2.6.1 資訊安全治理與管理方針

在數位化經營及全球供應鏈協作日益深化的環境下，資訊系統已成為支撐企業營運、客戶服務、生產管理及決策分析的重要基礎。六暉集團深知資訊安全不僅關係企業營運穩定，更攸關客戶信任、商業機密保護及企業永續發展，因此將資訊安全納入企業風險管理體系，持續強化資訊安全治理機制與防護能力。

為確保資訊資產之機密性 (Confidentiality)、完整性 (Integrity) 及可用性 (Availability)，集團訂有《資通安全管理辦法》及《資訊系統重大災害緊急應變管理辦法》，作為資訊安全管理、系統維護、權限控管、資料備份、異常事件通報及災害復原之執行依據。

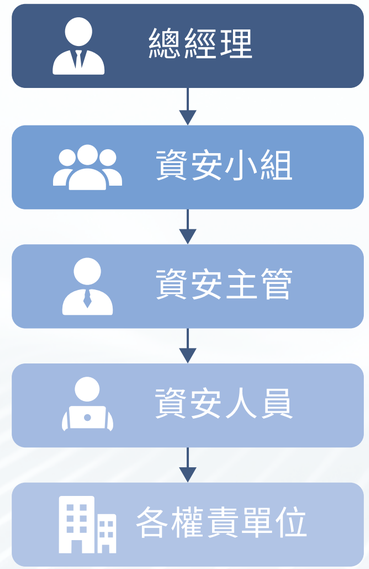
資訊安全管理涵蓋台灣、中國 (廈門、昆山) 及印尼等主要營運據點，由總經理督導資訊安全管理事項，透過資安小組統籌資安政策、管理措施及相關機制之推動，並由資安主管及資安人員負責資訊安全管理工作，各權責單位則依職責落實資料及報表資訊之使用管理與機密維護，共同維護資訊資產安全。

集團並透過內部控制制度、內部稽核及管理審查機制，持續檢視資安風險與改善措施之有效性，提升資訊安全管理效能及營運韌性。

2025 年，集團持續優化資訊安全管理制度與災害應變機制，並強化系統架構與資訊基礎建設管理，以因應日益增加之網路安全風險與數位營運需求。

資訊安全管理組織圖





總經理	督導資訊安全政策、目標及重大資安事項
資安小組	統籌資安政策、措施及管理機制推動
資安主管	負責推動、協調監督及審查資通安全管理
資安人員	執行資訊安全管理、系統維護及異常事件處理
各權責單位	落實所屬資料及報表資訊之使用管理與機密維護
稽核單位	執行資安查核及改善追蹤

目錄
關於本報告書
2025 六暉永續績效
01 永續策略與實踐
02 關於六暉
03 產品責任與服務
04 永續環境
05 友善職場
06 社會共融
附錄

2.6.2 資訊安全風險管理

六暉集團依據資訊資產重要性及風險程度，持續推動資訊安全風險管理機制，透過風險辨識、評估、監控及應變管理等作業，降低資訊系統中斷、資料外洩、未經授權存取及網路攻擊等風險對營運之影響。

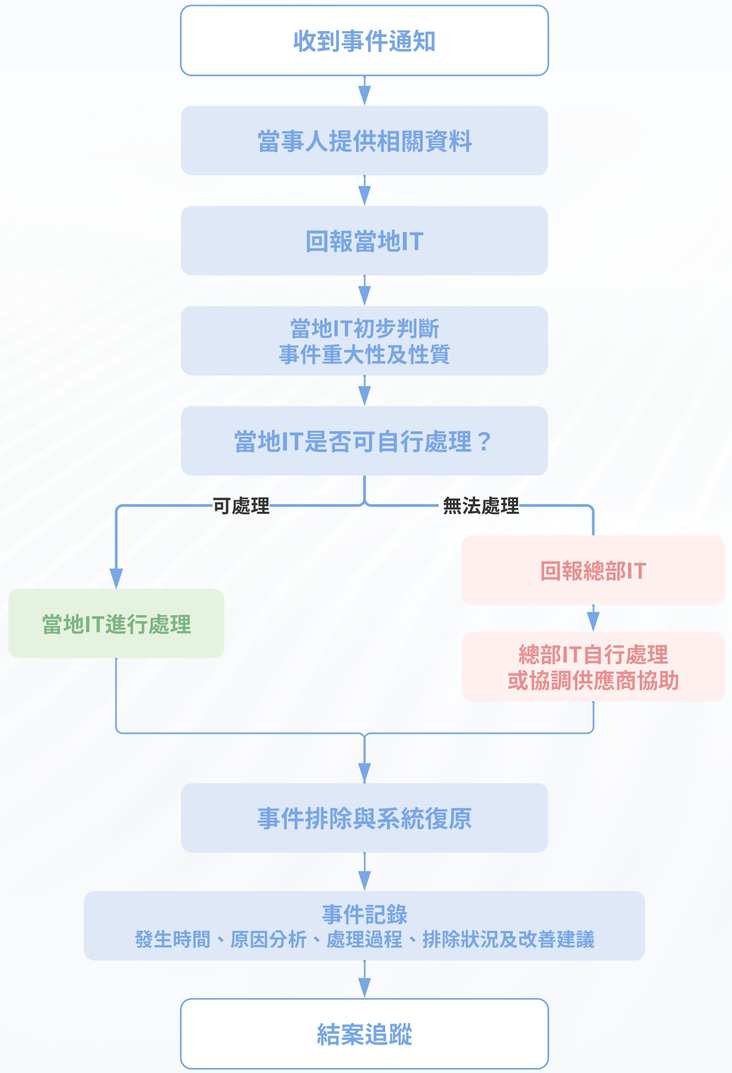
在風險管理實務上，集團定期檢視資訊系統運作狀況、網路環境及資訊設備安全性，並針對帳號權限管理、惡意程式防護、郵件安全、資料備份及災害復原等面向進行風險評估與管理，以提升資訊資產保護能力及營運韌性。

如發生資訊安全事件，相關單位將依事件通報及應變程序進行處理，並依事件影響程度執行調查、改善及追蹤，以降低事件對營運之衝擊。

風險類型	風險說明	潛在影響
惡意程式與勒索軟體攻擊	▶ 系統遭病毒、木馬程式或勒索軟體入侵	▶ 系統中斷、資料毀損或遺失
網路釣魚與社交工程攻擊	▶ 員工誤信不明郵件、連結或詐騙訊息	▶ 帳號遭盜用、機敏資訊外洩
未經授權存取與權限濫用	▶ 權限設定不當或帳號遭冒用	▶ 商業機密外洩、資料遭竄改
資料外洩與個資保護風險	▶ 客戶資料、商業機密或個人資料外洩	▶ 法規遵循風險、商譽受損及客戶信任下降
系統異常與營運中斷風險	▶ 系統故障、設備異常或重大災害造成服務中斷	▶ 影響生產、營運及客戶服務
委外及供應鏈訊安全風險	▶ 外部服務商、維護廠商或委外單位造成資安風險	▶ 第三方風險擴散及資訊安全事件

資訊安全事件通報與處理流程

本集團建立資訊安全事件通報與處理機制，適用於系統異常、資料安全疑慮、資訊設備異常、帳號權限異常及其他資訊安全事件，透過事件通報、調查、處理、追蹤及改善流程，及時降低資訊安全風險，確保營運持續性及資訊資產安全。



目錄
關於本報告書
2025 六暉永續績效

01 永續策略與實踐
02 關於六暉
03 產品責任與服務
04 永續環境
05 友善職場
06 社會共融
附錄

2.6.3 資訊安全管理措施

面對資訊環境快速變遷與資安威脅日益嚴峻，六暉集團持續強化各項資安防護措施，從制度面、技術面、人員面及供應鏈面建構多層次防禦機制。透過系統化管理、日常維運、稽核追蹤及災害復原演練，降低營運中斷、資料外洩及未經授權存取等風險，提升資訊系統穩定性與營運韌性。

分類	管控項目	執行措施
制度面	資訊資產管理	▶ 建立設備、系統及重要資料管理機制，依資料重要性及使用需求控管存取權限。
	存取與權限管理	▶ 規範帳號建立、變更與停用流程，並依職務需求設定權限。
	合規與稽核	▶ 納入內控制度並由稽核單位定期追蹤改善。
技術面	系統與裝置管理	▶ 針對裝置管理、硬體防護、上網及行動安全規劃管控措施；維護防毒、防火牆系統並定期更新。
	郵件與防毒防護	▶ 郵件伺服器設有病毒防護與垃圾郵件過濾機制，降低病毒、惡意附件及釣魚郵件風險。
	備份與資料保存	▶ 重要資料依內部規範執行備份，並透過備份與還原機制降低資料遺失風險。
	異常事件應變	▶ 建立資訊安全事件通報與應變程序，發生異常事件時依事件影響程度進行處理、調查及追蹤改善。
	營運持續與災害復原	▶ 定期執行資料備份及災害復原演練，透過離線還原或復原測試確認營運回復能力。 ▶ 2025 年，廈門據點導入超融合系統 (Hyper-Converged Infrastructure, HCI)，整合運算、儲存及虛擬化資源管理，強化資料備份、系統容錯及災害復原能力，提升資訊系統穩定性與營運韌性。
人員面	資安意識與教育訓練	▶ 透過資安宣導、社交工程影片或資訊安全意識培訓，提升員工資訊安全意識、風險辨識能力及資安防護觀念。
	資安事件通報	▶ 建立資訊安全事件通報機制，要求員工發現異常事件、可疑郵件或潛在資安風險時即時通報，由資安人員依事件通報與應變程序進行評估、處理及追蹤，以降低資訊安全事件對營運之影響。
供應鏈面	委外與供應商管理	▶ 透過保密條款、連線授權、安全性檢查及權限管理，降低外部資安風險。

目錄
關於本報告書
2025 六暉永續績效

01 永續策略與實踐
02 關於六暉
03 產品責任與服務
04 永續環境
05 友善職場
06 社會共融
附錄

2.6.4 個資與客戶隱私保護

六暉重視個人資料保護，視其為保障員工、客戶及合作夥伴基本權益的重要責任。為確保個資於蒐集、處理與利用各階段皆符合法規要求，集團依據相關法規及內部管理規範，訂有《個人資料保護管理辦法》，並定期檢視相關作業流程及管理措施之有效性。

在客戶資訊保護方面，六暉長期遵循與客戶簽訂之保密協議（NDA）及相關合約要求，落實客戶機密資訊、技術資料、個人資料及隱私資訊之管理，維護客戶權益及商業機密安全。2025 年度未發生違反客戶保密義務、客戶資料外洩、侵犯客戶隱私或涉及顧客個人資料之事件。

個資保護原則

合法蒐集與清楚告知：

- 依相關法規規定辦理個人資料蒐集、處理及管理作業，並清楚告知蒐集目的、使用範圍及保存期間等資訊。

安全處理與風險控管：

- 採取適當之管理及資訊安全措施，降低個人資料遺失、竄改、洩漏或遭未經授權存取之風險。

責任分工與制度推動：

- 由權責單位負責個人資料保護制度之推動、執行及管理，透過教育宣導，持續落實個資保護要求與法規遵循。

客戶隱私保護績效

指標項目	2025 年績效
經證實侵犯客戶隱私之投訴	0 件
涉及顧客個人資料之資安違反事件	0 件
經證實遺失客戶資料事件	0 件
因客戶資料洩漏而受影響之顧客與員工人數	0 人

2.6.5 資訊安全教育訓練與演練

六暉集團重視資訊安全文化之建立，深知資訊安全防護不僅仰賴技術設備與管理制度，更有賴全體員工共同參與及落實。因此，集團持續推動資訊安全教育訓練與宣導活動，透過教育訓練、影片宣導及案例分享等方式，提升員工資訊安全意識、風險辨識能力及異常事件通報觀念，降低因人員疏忽或不當操作所造成之資訊安全風險。

訓練內容涵蓋帳號密碼管理、資料保密、可疑郵件辨識、設備使用管理及異常事件通報等主題。2025 年度集團共辦理資訊安全相關教育訓練及宣導活動，累計受訓 187 人次、總受訓時數 88.9 小時。

未來將持續推動社交工程演練及風險情境教育訓練，強化員工辨識資安威脅與異常事件通報能力，建立全員參與之資訊安全文化。

各營運據點資訊安全教育訓練及宣導情形如下：

營運據點	訓練或宣導主題	對象／受訓人數	總受訓時數
台灣	社交工程演練影片宣導	46	6.9 小時
廈門	資訊安全意識培訓	20	20 小時
昆山	資訊安全、ERP 系統及資訊管理相關訓練	120	60 小時
印尼	互聯網使用對資訊科技基礎設施的安全性和效率	1	2 小時



2.6.6 資訊安全管理成果

為持續提升資訊系統穩定性及資安防護能力，六暉集團透過制度建立、風險管理、教育訓練及資訊資源投入等多項措施，持續強化整體資訊安全管理效能。2025 年度集團資訊相關投入總計新台幣 5,140.11 仟元，主要用於雲端服務、營運系統維護、資安防護及資訊基礎架構升級等項目，以提升資訊系統穩定性、資料保護能力及營運韌性。

資訊安全管理成果

項目	2025 年成果
資安教育訓練人次	187 人次
訓練時數	88.9 小時
資安治理會議	20 次
重大資安事件	0 件
個資外洩事件	0 件
資安相關裁罰	0 件
資訊投入金額	NT$5,140.11 仟元

各營運據點資訊資源投入情形：

單位：新台幣

項目	項目說明	營運據點	2025 年資訊支出
雲端服務	支援電子郵件、帳號及雲端郵件服務使用	台灣	121.58
		廈門	191.65
		昆山	109.10
		印尼	300.95
資安防護	強化端點設備及網路邊界防護能力	台灣	284.00
		廈門	399.32
		昆山	67.03
		印尼	120.21
營運系統維護	維持核心營運系統及相關設備穩定運作	台灣	441.11
		廈門	1,173.91
資安基礎架構升級	提升系統資源管理、風險隔離及事件應變能力	廈門	1,931.25

2.6.7 未來精進方向

- 持續投入資訊安全管理資源，強化網路安全防護、系統監控及資料備份機制，提升整體資安防護能力。
- 定期辦理資訊安全教育訓練及宣導活動，提升員工資安意識與個人資料保護觀念。
- 持續檢視資訊安全管理制度及應變流程，強化資安事件通報、應變及復原能力，降低營運中斷風險。

