V5 TECHNOLOGIES CO., LTD. | 企業永續與治理揭露

倍利科技資訊安全治理與實踐報告

Information Security Governance & Practice Report (2025–2026)

ISO/IEC 27001:2022	嚴重 / 高風險弱點	XDR 與資安訓練	重大資安與外洩事件
連續兩年通過 SGS 驗證	分別大幅下降 91% / 89%	涵蓋率與完訓率皆達 100%	2026 年度維持 0 事故

一、資訊安全管理政策與國際驗證

為保障客戶資料安全、維護營運持續性並強化企業信譽，倍利科技股份有限公司（V5 TECHNOLOGIES CO., LTD.）積極推動系統化資訊安全管理制度（ISMS），以「機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）」為三大核心原則，持續深化內部資訊防護機制。

本公司於 2024 年正式成立【資訊管理委員會】與【資訊安全小組】，制定《倍利科技資訊安全政策》，全面導入符合國際標準之資訊安全管理架構。透過制度化管理流程、定期風險評估與持續性演練，具體落實企業對資訊安全治理之承諾。

國際標準驗證里程碑：ISO/IEC 27001:2022 驗證通過

- 驗證歷程：2025 年 6 月 28 日首次取得 ISO/IEC 27001:2022 合格證書；2026 年 5 月順利通過 SGS 年度有效性實地審查，第二年證書持續有效（證書編號：TW25/00000581，效期至 2028 年 6 月 28 日）。
- 驗證範圍（適用性聲明書 V02）：(1) 研發部門之 Macro Inspection、Micro Inspection 及 Micro Measure 演算法開發與單元測試；(2) 資訊部門之支援系統、資料中心及網路環境維運管理。

二、資訊安全組織架構與權責分工

為確保資訊安全政策有效推行並具備跨部門協調能力，本公司建立由高階主管領軍之資安治理組織，明確劃分決策、執行、應變與獨立稽核職責。2026 年度委員會完成成員優化調整（共 8 名委員），核心運作團隊無縫接軌，持續穩健推動各項資安作業：

組織單位	召集人／核心成員	主要職責與運作機制
資訊管理委員會（最高決策機構）	主任委員：總經理 執行秘書：協理 委員：各營運部門高階主管（共 8 人）	審核資訊安全政策與管理指標、督導 ISMS 運作有效性、每年定期召開管理審查會議並核定重大資安資源配置。
資訊安全小組（專責推動單位）	組長：協理 擔任 核心成員：資訊經理及副理級主管	負責 ISMS 日常維運、威脅情資分析、弱點掃描修補、存取權限審查、教育訓練及社交工程演練執行，並每月召開資安月會。

緊急處理小組（事件應變團隊）	核心成員：資訊安全小組技術骨幹	建立資訊安全事件通報與緊急應變標準作業程序（SOP），負責資安異常偵測、損害控制、系統復原及年度營運持續演練。
獨立稽核小組（內部監督機制）	稽核人員、協同各營運部門受稽窗口	獨立執行年度 ISO 27001 內部稽核作業，客觀檢視各部門法規與制度遵循度，並追蹤矯正預防措施至 100% 完成改善。

三、資通安全治理演進（2025 至 2026 年度比較）

2026 年倍利科技資安治理正式由「制度建立期」邁入「持續維運與深化期」。透過量化指標追蹤與技術防護升級，各項資安風險顯著收斂：

治理構面	2025 年度實績	2026 年度進展	年度差異與治理意義
管理制度與國際驗證	2025/06/28 首次取得 ISO/IEC 27001:2022 合格證書；3 月正式啟用 ISMS。	2026/05 通過 SGS 年度有效性實地審查，第二年證書持續有效。	制度由「建立」穩健邁入「維運」，持續落實風險評估、內部稽核與改善追蹤。
治理組織與權責分工	委員會 9 人；	委員會調整為 8 人（	資安小組組長及技術骨幹維持不變，組織交接順暢完成，日常維運與應變零中斷。
防護技術與量化成效	首次弱掃嚴重 22 項、高風險 90 項全數修補；完成 XDR 部署；資安訓練完訓率 100%；社交工程點擊率 2.8%。	弱掃嚴重風險降至 2 項（-91%）、高風險降至 10 項（-89%）；完成 14 項風險改善；社交工程點擊率降至 2.17%；XDR 涵蓋率 100%；納入 ERM R01 企業風險管理。	縱深防禦與員工資安意識同步提升，威脅暴露面大幅縮減，並與企業全面風險管理接軌。

四、六大資訊安全執行重點、指標與達成成效

本公司針對組織治理、存取控制、實體與網路防護、風險應變、人員意識及供應鏈管理六大構面，訂定明確量化指標並定期追蹤執行進度：

策略構面	管理指標要求	核心執行重點	2026 年度達成成效
1. 組織架構與治理機制	• 管審會 ≧1 次/年 • 資安月會 ≧1 次/月 • 內稽 ≧1 次/年 • 資產盤點 ≧1 次/年 • ISMS 有效性量測不符 ≦2 次/年	定期召開資訊安全月會與管理審查會議；執行年度內部稽核、資訊資產盤點與 ISMS 有效性量測。	• 4 月完成年度管審會及 ISMS 有效性量測審查。 • 已召開 9 次資安月會（5、6 月合併執行）。 • 3 月完成年度內部稽核，缺失改善率達 100%。

2. 系統與存取管理	• 權限審查不符 ≦1 件/年 • 弱點與異動檢視 ≦2 件/季	落實帳號與資料夾「最小權限原則」定期審查；持續追蹤威脅情資、軟體異動與系統漏洞修補。	• 2 月完成年度全公司帳號及資料夾權限審查。 • 持續蒐集外部威脅情資，已完成 14 項資安風險改善措施。
3. 實體與網路安全	• 門禁監控審查 ≧2 次/年 • 網路與備援監控不符 ≦1 件/半年	機房與辦公區域實施門禁管制與 24 小時監控；導入自動化即時網路監控與系統備援機制。	• 4 月完成門禁權限與監控設定審查，執行率 100%。 • 透過自動化監控系統即時掌握網路與系統狀態並完整留存紀錄。
4. 風險控管與應變機制	• 風險評估與弱掃 ≧1 次/年 • 資安演練 ≧1 次/年 • 端點防護異常 ≦1 件/季	每年執行風險評估與弱點掃描；辦理緊急應變與營運持續演練；全面部署端點偵測與自動防護系統（XDR）。	• 3 月完成年度弱點掃描，嚴重風險由 22 項降至 2 項（-91%），高風險由 90 項降至 10 項（-89%）。 • 辦公區域 XDR 涵蓋率達 100%。
5. 教育訓練與文化宣導	• 員工年度資安課程 ≧1 小時/年 • 定期辦理社交工程演練	新進與在職同仁皆須完成年度資安課程；透過內部郵件、影片、螢幕保護程式及月會宣導強化防詐意識。	• 全體在職與新進同仁資安教育訓練完成率達 100%。 • 社交工程演練點擊率由 2025 年 11 月之 2.80% 下降至 2026 年 3 月之 2.17%（降幅 0.63%）。
6. 顧客與供應鏈資訊保護	• 權限與合規檢視不符 ≦1 件/季	依循《個人資料保護法》與歐盟 GDPR 精神落實最小權限控管；要求供應商簽署並遵守資訊安全保密條款（NDA）。	• 2 月完成客戶與專案相關帳號權限審查。

五、資訊安全風險管理與營運韌性強化藍圖

倍利科技將資訊安全納入企業全面風險管理（ERM R01）範疇，針對六大關鍵風險情境建立「現行控制機制」與「中長期精進藍圖」，持續強化基礎架構高可用性與營運韌性：

風險主題與情境	現行控制環境	精進改善措施／後續規劃	執行時程／狀態
IT 基礎架構與管理（系統中斷或資料損失）	資安政策與教育訓練、ISO 27001 管理審查、核心系統定期檢視、權限控管與行為監控／DLP。	持續落實 ISO 27001 管理機制與定期管理審查（Review）。	**2026 已完成（持續維持）**
機密與個人資料外洩（內部疏失或未授權存取）	資安意識宣導、網路隔離、最小權限控管、郵件垃圾信（Spam）與自動防護機制。	導入 NAC 網路存取控制裝置識別、強化無塵室（FAB）USB 管控及網路區隔。	**進行中**
網路與系統外部入侵（弱點攻擊與惡意程式）	定期弱點掃描與修補、XDR／防毒即時監控、備援備份、防火牆規則審查與外部服務控管。	維持既有縱深防禦與即時監控，定期檢視威脅情資並持續修補改善。	**持續執行（穩定維持中）**
關鍵服務中斷（伺服器或儲存設備故障）	硬體狀態即時監控、系統備援與資料備份機制、關鍵伺服器與共享儲存可用性規劃。	導入企業級共享儲存設備（Share Storage），建置高可用性架構（HA）。	**2026/06/30（已完成建置）**
地緣政治與供應鏈風險	邊界入侵防護、VPN 裝置識別控管、	完成企業級 Share Storage 高可用性	**2026/06/30**

（營運與設備供應不確定性）	網路與重要服務維運監控與備份。	架構建置；持續評估安全庫存與替代設備標準化。	**（已完成核心建置）**
天然災害衝擊（停電、地震與營運持續）	機房不斷電系統（UPS）與環境告警、機櫃固定防震、營運持續計畫（BCP）、業務衝擊分析（BIA）及本地／核心異地備份。	持續辦理年度營運持續演練；規劃進一步擴大異地備份涵蓋範圍，強化災難復原能力。	**核心異地備份已完成；擴大範圍規劃中（2027）**

六、年度治理總結與持續承諾

- **持續落實資訊安全治理制度：**嚴格依循 ISO/IEC 27001:2022 資訊安全管理制度，透過管理審查、內部稽核、風險評估及定期檢討機制，持續強化資訊安全治理效能。2026 年度本公司未發生任何重大資訊安全事件或客戶資料外洩事故。
- **深化技術防護與風險控管能力：**全面落實最小存取權限管理、網路與端點安全監控（XDR 100% 涵蓋）、系統弱點快速修補及全員資安教育訓練，顯著降低關鍵資訊資產暴露風險並提升組織整體防護力。
- **精進高可用性架構與營運韌性：**透過企業級高可用性（HA）儲存架構建置、NAC 網路存取控管導入及異地備份機制擴大，持續強化業務持續運作與災難復原能力，以穩健回應不斷演變的資安威脅與全球客戶之高度信賴。