2025 年資訊安全管理執行情形

資安策略與治理

飛宏不斷精進資訊安全管理制度並強化防護能力，透過資訊安全管理委員會統籌推動並落實各項資訊安全管理措施，以保護公司智慧財產與客戶資料，同時提升員工資訊安全意識，並持續完備風險管控機制，以強化公司的資訊安全。

為落實資訊安全管理機制，確保資訊資產之機密性、完整性與可用性，飛宏於2024年取得 ISO/IEC 27001:2022 資訊安全管理系統（Information Security Management System, ISMS）國際標準認證，並依據 P-D-C-A（Plan-Do-Check-Act）循環管理模式，建立持續改善之資訊安全管理架構。2025年，本公司通過外部第三方稽核機構（SGS）之年度審核，驗證資訊安全管理制度的落實，並維持證書之有效性，證書效期至2027年9月10日。

未來，飛宏將持續強化各項安全措施，落實資訊安全政策、提升員工資安意識，並導入專業資安技術，藉此降低資安威脅所帶來之營運與財務風險，提升公司整體資通訊防護強度，進而取得客戶與利害關係人之信任。


Certificate TW24/00000802

The management system of

PHIHONG TECHNOLOGY CO., LTD.

SGS

No. 568, Fuxing 3rd Rd., Guishan Dist., Taoyuan City 333, Taiwan (R.O.C.)

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2022

For the following activities

Information security management activities provided in accordance with the Statement of Applicability Version A2. The activities include,

1. Development and maintenance of the Business Process Management system (BPM), and management and operation of directory service management system, email service management system, network and computer room provided by the Information Technology Department of Phihong.
2. Maintenance of network and backup computer room provided by the Information Management Department of Zerova.

This certificate is valid from 16 October 2024 until 10 September 2027 and remains valid subject to satisfactory surveillance audits.

Issue 2. Certified since 10 September 2024

Multiple certificates have been issued for this scope, the main certificate is numbered TW24/00000802

Certified activities performed by additional sites are listed on subsequent pages.

L. Moran

Authorised by

Liz Moran

Business Manager

SGS United Kingdom Ltd

Rosemore Business Park, Ellesmere Port, Cheshire, CH65 3EN, UK

t +44 (0)151 350-6666 - www.sgs.com

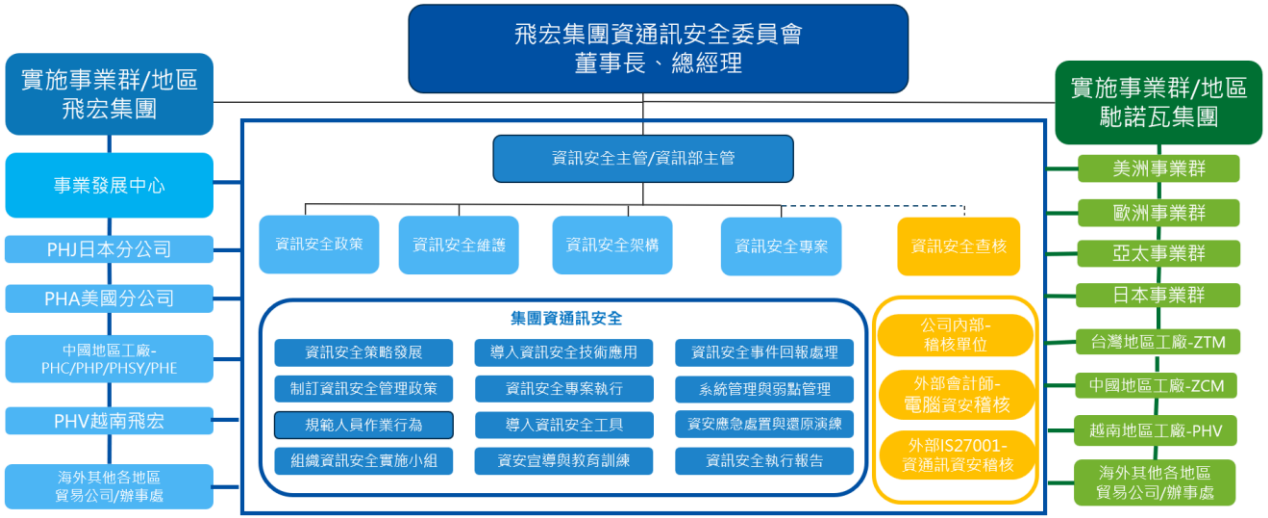
UKAS

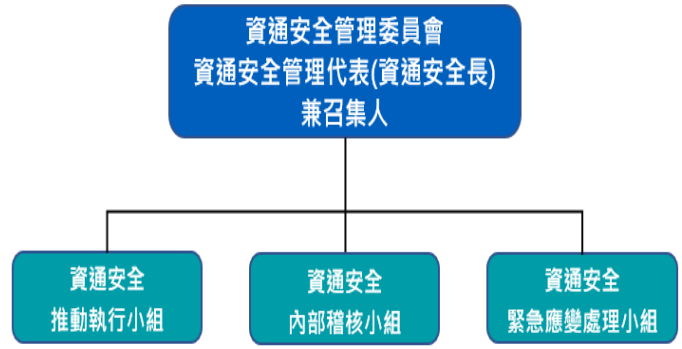
IAF

Page 1 / 3

資通安全政策與組織 (GRI 418-1)

為確保資訊及相關資產的機密性、完整性、可用性，並符合法規要求，飛宏導入資訊安全管理機制，防止資通系統遭未授權存取、使用、洩漏或破壞，以維護業務服務安全，保障產品、客戶及個人資料隱私，確保業務持續運作。飛宏於 2021 年成立資通安全委員會，由總經理擔任資安長。2023 年設立資訊安全部，專責制定與監督資通安全政策，推動相關專案。資通安全委員會透過管理審查會議評估風險並採取防護措施，每年向董事會報告治理成果。委員會下設置「資通安全管理代表」(資安長)、「資通安全推動執行小組」、「資通安全內部稽核小組」及「資通安全緊急應變處理小組」，共同維護公司資訊安全。





資通安全管理措施

管理構面			管理措施
治理	Governance	(GV)	監控與評估資安策略與實踐，確保合規，持續改進資安管理，保障組織的資安目標。
識別	Identify	(ID)	識別資安風險、資源與需求，進行風險評估，制定策略與政策，確保資安治理基礎。
保護	Protect	(PR)	實施安全控制措施，保護資源免受未授權存取，進行加密與配置管理，防止資安事件。
偵測	Detect	(DE)	監控系統異常，部署偵測工具，收集日誌與監控數據，快速發現潛在的資安威脅。
回應	Respond	(RS)	迅速應對資安事件，建立事故響應計劃，減少損失並有效管理資安事故。
復原	Recover	(RC)	恢復業務運作與數據，實施災難復原計劃，確保在事件後快速重建並維持業務連續性。

資訊安全執行成果

管理類別	2025 年執行情形	管理構面
資訊安全管理系統(ISMS)及稽核機制	飛宏 2025 年完成 ISO 27001:2022 國際標準年度審查，驗證資訊安全管理系統（ISMS）之落實，以符合客戶及利害關係人要求。主要措施包括： • ISO 27001:2022 管理與實施：依據 ISMS 國際標準，透過 PDCA 循環持續改善，降低資安風險。 • 資安政策與文件管理：定期檢視與更新資安管理文件，確保制度符合實際運作需求。 • 執行與稽核：定期進行內外部稽核，確保符合資安標準並持續優化。 • 認證與維護：2024 年 10 月取得 ISO 27001:2022 認證，並於 2025 年完成外部第三方年度稽核作業，持續維持 ISMS 證書之有效性，以確保合規與客戶信任。	(GV) (ID)
帳號與認證管理加嚴	• 加強帳號與認證管理：提升密碼長度與複雜度，並設定定期更新要求，強化帳號安全性。 • AD 帳號保護平台：加強對 Active Directory (AD) 帳號、特權帳號與服務帳號的管理與監控，確保帳號的安全與保護。 • 全面導入 MFA 機制：全公司各系統全面導入多因素認證（MFA），結合生物辨識技術，擺脫弱密碼風險，提升帳號安全性、認證效率及整體資安防護強度。	(PR)
強化端點設備管理	• 資產管理工具導入：全數端點設備導入資產管理工具，強化對作業系統、軟體版本及網路使用的控制，進一步加強設備的安全性及資料保護。 • 防毒與端點偵測軟體導入：在所有端點設備中全面導入防毒軟體與端點偵測系統，防範惡意軟體、入侵行為及其他網路攻擊，提升資安防護層級。	(PR) (DE)
資安防護預警與提升同仁資安意識	• 資安情資通知：透過政府及各類情資來源，提前通知相關單位，以預防資安事件發生。 • 資安教育訓練：製作內部教材與影片，涵蓋 ISO 27001 程序要求、資安趨勢、釣魚郵件識別與防範等主題，並要求員工每年完成 2 小時培訓，以深化資安意識。 • 社交工程演練：定期模擬網路釣魚攻擊，結合時事詐騙手法提升員工對惡意郵件的警覺。2025 年共實施 12 次演練，並為誤點擊者提供補充訓練，以強化資安應對能力。 • 資安意識宣導：每日更新資安趨勢與重大事件，並舉辦資安月活動，提高員工警覺性與防範意識。	(PR)
系統弱點偵測與修補	• 內部弱點掃描與修補：每週掃描內部系統與網路環境，制定並執行修補計畫。 • 外部情報與漏洞修補：運用外部安全情報識別潛在漏洞，規劃並執行設備、系統與軟體的修補與升級，提高系統安全性。	(PR) (DE)
網路安全提升	• 強化防火牆備援機制：升級至 7×24 服務等級，提升容錯能力，降低營運中斷風險。 • 優化防火牆安全策略：定期檢視與調整防火牆服務政策，以強化網路安全防護。 • 建置 SIEM 資安管理系統：整合 EDR、NDR、防火牆日誌與威脅情資，實現自動化偵測、告警與回應機制。 • 導入 NAC 系統：即時監控網路存取並驗證連網裝置合規性，確保只有符合資安政策之設備方可接入。 • 導入 DDoS 防護機制：提升系統韌性與服務可用性，防範 DDoS 阻斷式攻擊。	(PR) (DE) (RS)
軟體開發安全	• 版本控管系統：實施 Git、SVN 等版本控管工具，確保軟體程式碼的完整性、可追溯性與安全性，降低未授權變更的風險。 • 強化程式碼安全檢測：利用源碼檢測工具，定期執行靜態應用安全測試（SAST），識別並修正潛在漏洞，防範 SQL 注入、XSS 攻擊等威脅。 • 帳號與權限管理：強化 CI/CD 流程中的存取控制與憑證管理，確保開發、測試與生產環境的安全隔離，避免未經授權的操作。	(PR)
資安通報與事件管理	• 依據資安事件管理程序，資訊安全事件發生時須立即通報並應變，以確保迅速恢復運作。飛宏導入進階持續性威脅（ATP）監控系統，結合外部資安專家支援，使維運與應變小組能快速掌握警訊並處理事件，大幅提升偵測與回應效率。 • 2025 年資安事件揭露：委外網站託管之雲端服務廠商遭受 DDoS 攻擊，間接影響官網短暫停止服務，已即時通報並啟動資通安全事件處理機制，當日恢復正常運作，未造成任何資訊外洩。	(RS)
營運持續管理與災難復原演練	• 為確保營運與關鍵業務在重大災難情境下持續運作並降低服務中斷風險，針對核心系統建置雲端異地備份及備援環境，每年定期進行還原演練，測試備份資料之可讀性、儲存媒體可用性及回存流程，以強化系統可回復性與驗證備份可靠性。藉由相關措施提升災難復原能力，確保災難發生時系統可於各廠區快速恢復運作，維持業務連續性並降低營運風險。	(RC)