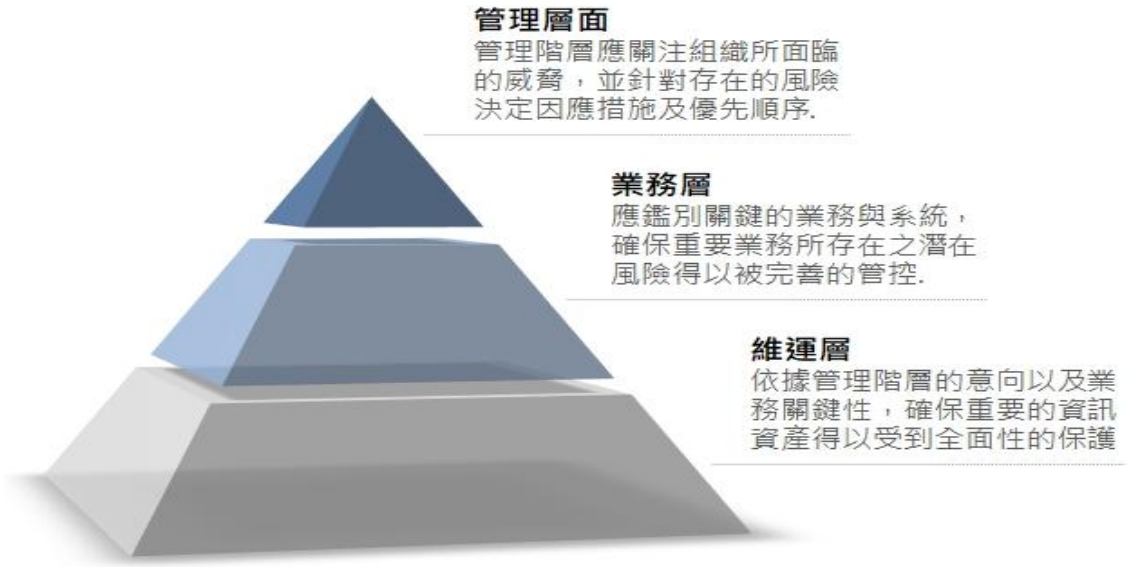
瑞軒科技-公司治理-資訊安全政策

●資訊安全治理責任

為落實經營者的責任，促進經營績效、保障投資者權益及符合相關法令要求建立資訊安全管理系統政策，以確保資訊之機密性、完整性及可用性。適用範圍設定為本公司機房、Cloud 服務維運作業系統及相關部門與維運管理人員，以充份掌握資訊運作及管理過程並滿足各項安全要求與期盼，瑞軒科技善盡資訊安全治理之責任，掌控資訊安全與企業風險管理，保護公司之研發成果資料、策略、合約文件、智慧財產、資訊系統等企業重要資產，落實資訊安全策略與內部控制，持續對資訊安全精進治理與強化防護能力，以確保公司永續營運之基礎。

●資訊安全治理架構

瑞軒科技以資訊安全治理架構作為指導及控制組織資訊安全活動之系統，目標在於確保資訊安全目標及策略承接組織營運的目標及策略，使資訊安全策略與業務目標一致，由上而下的持續回饋資訊安全治理架構，以降低資安風險。



●資訊安全治理組織

瑞軒科技為提供員工穩定持續工作環境，於 112 年度新增資通安全推動組織，成立資訊安全部門，並配置資訊安全專責主管及資訊安全人員，進行訂定資訊安全作業程序，並不定期進行資訊安全宣導，保護機敏資料。組織透過規劃、建立、執行與監督(PDCA)機制，保護資訊資產的機密性(Confidentiality)、完整性(Integrity)以及可用性(Availability)，並透過日常維運執行與監督的過程確保其持續改善，並提供組織得以再次評估回饋，落實資訊安全管理執行機制，透過治理架構向上溝通，回應組織策略之要求。

針對網路防護系統安全，本公司導入雲端沙箱等級之防火牆，並留存相關連線紀錄；資訊單位即時主動偵測病毒，並使用偵測病毒軟體來偵測外來行動儲存裝置；不定期針對網路及系統伺服器做弱點掃描，加以改善；各系統主機、重要軟硬體設備皆有專人負責。公司重要系統，均有進行系統及資料備份，當發生系統異常或資料毀損時，可迅速回復正常作業；主要系統目前已導入最新超融合架構，對於資料處理的即時性有很大的提升，且在系統備援部分可做到秒級備份，整體防護更加完善；另有備份磁帶於異地存放，多重保障資料安全；另外，對於總公司與子公司間的資料傳遞安全，全面導入 MPLS 多重通訊協定標籤交換，除可保障線路穩定性，加速網路連線，更可防護網路安全；112 年度導入了全球第一品牌 CrowdStrike EDR 端點防護，加強本公司三地伺服器群資安防駭能力，更精準且快速地阻斷隱匿於內部之惡意程式及駭客攻擊行為；113 年度已導入全員無密碼登入，增加員工帳密安全及便利體驗、7*24 MDR 服務，資安監控不漏失，114 年度導入堡壘機，集中管理遠端存取與特權帳號，確保資安政策一致性；並完成全體同仁年度資訊安全教育訓

練。預計 115 年度導入 ISO27001，116 年第一季取得國際認證證書，落實執行文件內容，達到說、寫、作一致，以上規劃可降低風險及確保營運不中斷。

本公司應於相關部門及層級建立資訊安全目標方案，並可與資訊安全政策對應或連結，且必須(1)可以量測 (2)成效量測方式 (3)需訂定完成日期 (4)需有負責人員(負責單位)。

資訊安全具體管理依據 ISO 27001：2022 新版標準，涵蓋 24 項管理事項，協助組織建立起資訊安全管理系統的機密性、完整性及可用性，並全面進行風險評估、找出潛在問題，再針對已知風險做出預防措施，透過風險處理，降低未來實際發生資料外洩的損失。

管理方案事項如下：

1、資訊安全政策
2、資訊安全組織
3、人力資源安全
4、資產管理
5、存取控制
6、加密管理
7、實體與環境安全
8、營運安全
9、通訊安全
10、威脅情資管理
11、營運持續之 ICT(Information and Communication Technology)備妥性
12、實體安全監視
13、組態管理
14、資訊刪除
15、資料遮蔽
16、資料洩漏預防
17、監視與紀錄活動
18、網頁內容過濾
19、安全程式設計
20、資訊系統之取得、開發與維護
21、供應商關係與第三方管理
22、資訊安全事件管理
23、資訊安全相關之營運持續管理
24、法規遵循與適法性管理

上述管理面向係依 ISO/IEC 27001:2022 Annex A 控制措施精神進行規劃與實施，作為本公司資訊安全管理與風險控制之主要依據。

●資訊安全治理目標

項目	114 年實績	115 年計畫
設定短中長期的資安目標與工作項目	●定期全集團發布資安宣導信件 ，每月達 4 封。 ●重要伺服器端點安全防護(EDR)佈署涵蓋率達 90%以上。 ●重要伺服器上重大弱點修補率 85%以上 (以 CVSS 九分以上為標準) 。 ●關鍵應用系統可用性達 99%以上。 ●導入 7*24 MDR 服務，達到預防、預警、即時處理資安事件之目的。 ●自建內外部威脅情資蒐集系統(CVE) ，比對現有設備或系統之弱點提出警示，讓資訊同仁可即時修補系統漏洞。 ●新 BPM 主機外部服務安全測試與修補。 ●SharePoint 零時差重大漏洞說明與處理。 ●修補 ERP 系統重大漏洞。 ●某系統暗網帳密外洩事件即時應變處置。	●定期全集團發布資安宣導信件 ，每月達 4 封。 ●重要伺服器端點安全防護(EDR)佈署涵蓋率達 90%以上。 ●重要伺服器上重大弱點修補率 90%以上 (以 CVSS 九分以上為標準) 。 ●關鍵應用系統可用性達 99%以上。 ●通過 ISO 27001 認證取得證書，落實資安治理目標，大幅提升公司資訊資產安全、降低未來資料外洩的損失。
集團資安控管流程 (AmTRAN/Raken/AVTC)	●訂定、修正及實施資訊內控文件 ●落實資訊內控文件表單填寫。 ●持續落實資安政策與作為。 ●落實 PDCA 資通安全管理循環機制。 ●導入堡壘機，提供集中式的管理，界面可以方便地管理所有的遠端訪問權限，包含特權帳號，以確保安全政策的一致性。	●訂定、修正及實施資訊內控文件 ●落實資訊內控文件表單填寫。 ●持續落實資安政策與作為。 ●落實 PDCA 資通安全管理循環機制。
評估擴大 ISO27001 認證範圍 (HQ/RK)	● HQ 已完成 ISO 27001 輔導顧問及第三方驗證單位之遴選評估作業確保導入品質、合規性與　專案風險可控。	● HQ 規劃於 2026 年第二季啟動 ISO 27001 顧問輔導作業。 ● HQ 以 2027 年第一季完成驗證並取得 ISO27001 國際認證為目標。
增加員工的資安教育訓練	●定期全集團發布資安宣導信件，每月達 4 封。 ●新進同仁資安宣導與個資保護宣導改版。 ●分享時事案例，強化同仁資安應對能力及警覺性。 ●一年一次全體同仁資安教育訓練，(已於 8 月執行，時數：2 小時)。	●定期全集團發布資安宣導信件，每月達 4 封。 ●新進同仁資安宣導與個資保護宣導。 ●分享時事案例，強化同仁資安應對能力及警覺性。 ●一年一次全體同仁資安教育訓練。
內部與外部資安稽核機制	●外部資安稽核由公信力的獨立認證機構每年兩次進行之。	●外部資安稽核由公信力的獨立認證機構每年兩次進行之。 ●待導入 ISO 27001 後，將由資訊安全小組稽核組成員，進行內部稽核，半年一次。

●資訊安全管理機制

資訊安全管理機制，包含以下四個面向：

（一）內控制度規範：

本公司內部訂定多項資安規範與制度，以規範本公司人員資訊安全行為，每年定期檢視相關制度是否符合營運環境變遷，並依需求適時調整。

（二）資安推展執行：

落實執行公司訂定 ISO 程序及各資安規範制度，管理與監控所有營運系統及網路服務安全事件和狀態，評估及導入資訊技術、資安設備運用。

（三）弱點風險評估：

定期審視內部資訊安全，根據資產價值、弱點、威脅與影響性，分析內部風險水平，並以此風險評估結果制定安全措施強化項目，精進且提升整體資訊安全環境。

（四）資安應用改善

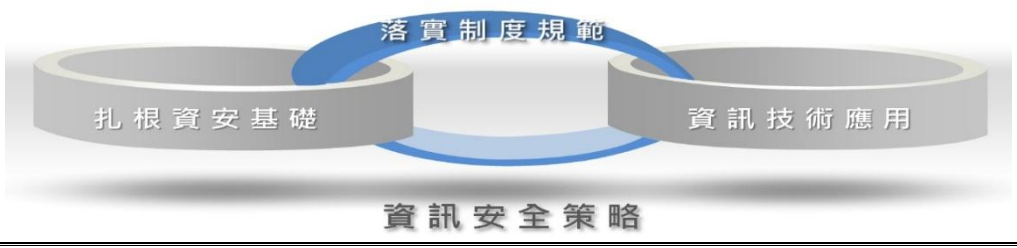
本公司為防範各種外部資安威脅，採多層式網路架構設計，更建置各式資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部人員之作業行為符合公司制度規範，亦設計作業程序和導入資安系統工具，落實人員資訊安全管理措施。

●資訊安全策略

資安策略主軸聚焦於扎根資安基礎、落實制度規範及資訊技術應用三個面來進行，從內部資通安全管理辦法、並透過資訊科技主動通報資安風險事件，人員到組織全面提升資安意識。

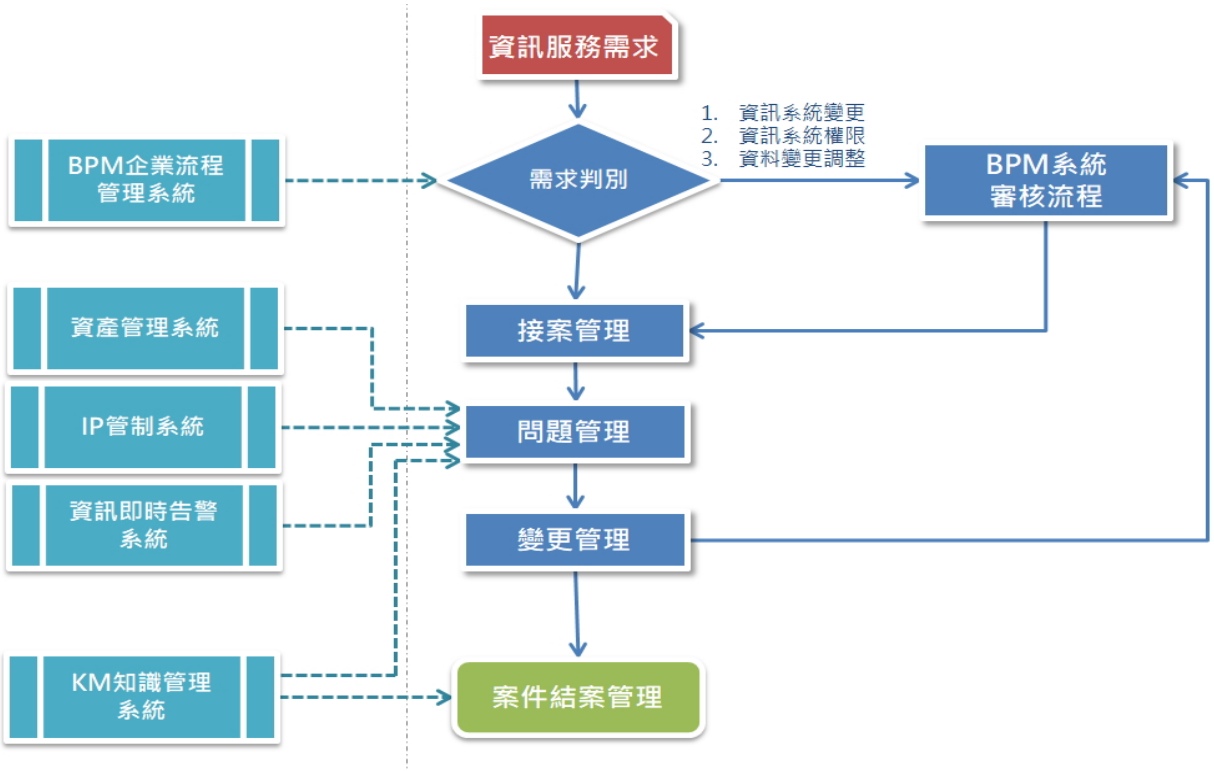
資訊安全策略

扎根資安基礎	定期檢視及升級網路基礎架構環境、持續修補內部系統潛在弱點、定期演練災難還原機制，實施人員資訊安全教育訓練實務課程，全面性的深化資安基礎防禦力。
落實制度規範	訂定公司資訊安全管理制度，定期審視及檢核資安內控執行成效，並貼合國際資訊安全規範，落實資訊安全控管機制之運行。
資訊技術應用	持續導入資訊安全設備及資安技術應用，透過如即時告警系統、端點防護系統、弱點掃瞄、入侵偵測聯防等技術應用，預先掌握資訊風險狀態，提升資安防禦力及應變能力。

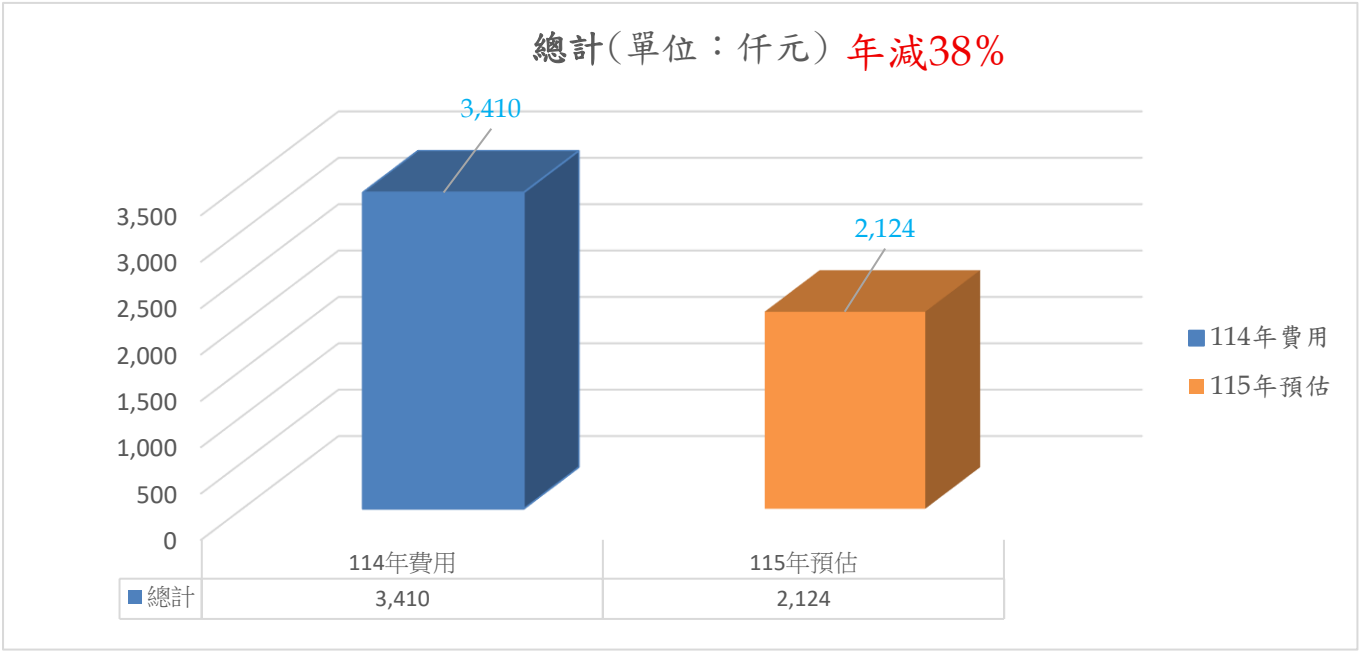


●資安服務處理流程

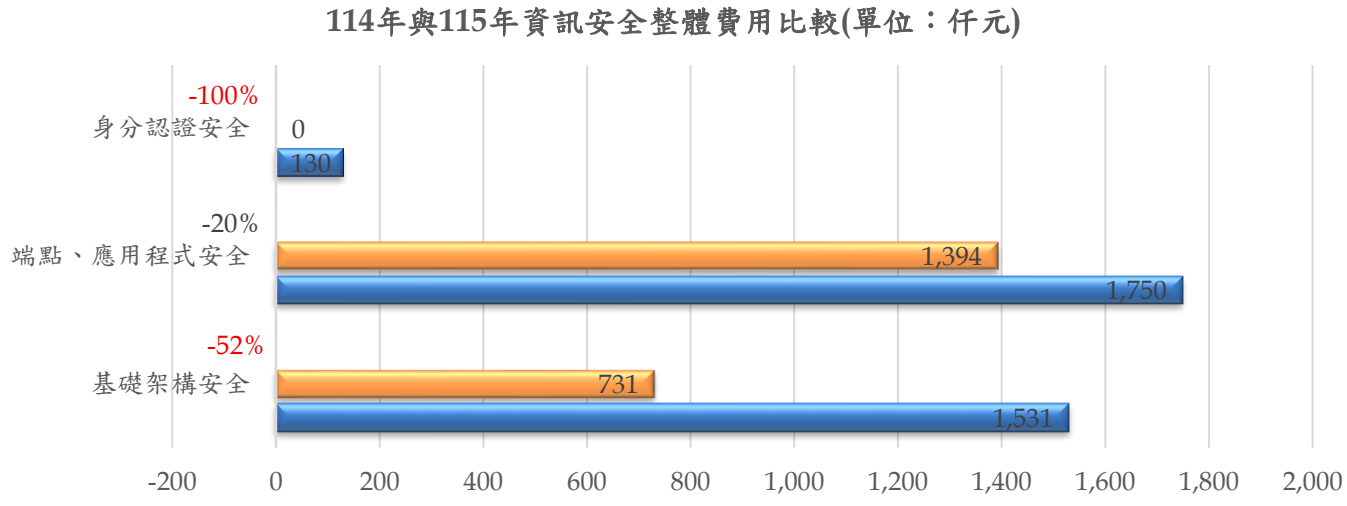
依據公司訂定之資訊管理辦法及案件管理流程，由資訊服務需求開始至案件結案，針對整體流程中各逐一環節，進行審核、分析、管理、記錄，並應用資訊系統之輔助，以有效控制資訊案件之管理、預先掌控及降低資訊風險發生。



●資訊安全年度所投入資源說明



●114 年與 115 年資訊安全整體費用



	基礎架構安全	端點、應用程式安全	身分認證安全
年度增減%	-52%	-20%	-100%
115年預估	731	1,394	0
114年費用	1,531	1,750	130

主要聚焦於營運核心重要系統之安全防護強化，透過整體性資安架構優化，提升組織資安成熟度，同時有效降低後續年度可能衍生之高額維運成本。

其中：

在身分認證安全方面，因 114 年採堡壘機一次性買斷之建置方式，以避免後續年度因長期訂閱所帶來之持續性費用負擔；在端點應用程式防護層面，除持續維持既有之 MDR 與 EDR 防護機制外，並配合 114 年度新購防火牆所整合之端點防毒功能，逐步汰換原有獨立防毒解決方案，藉此達成資安防護之整合化，並同步降低 115 年度整體採購與維運成本。

在基礎架構安全層面，因 114 年度已完成新防火牆之建置與汰換，115 年度無需再新增相關採購項目，爰整體資安預算相較前一年度有所下降。

此亦顯示在既有資安投資基礎上，透過既有設備延續使用與架構整合，即可持續維持必要之防護水準。

115 年度擬新增：

1. 導入 ISO/IEC 27001 資訊安全管理系統認證，取得認證證書。
2. 加強軟、硬體安全漏洞情蒐，快速擬出因應措施，修補風險。
3.加強瑞軒同仁資訊安全宣導。

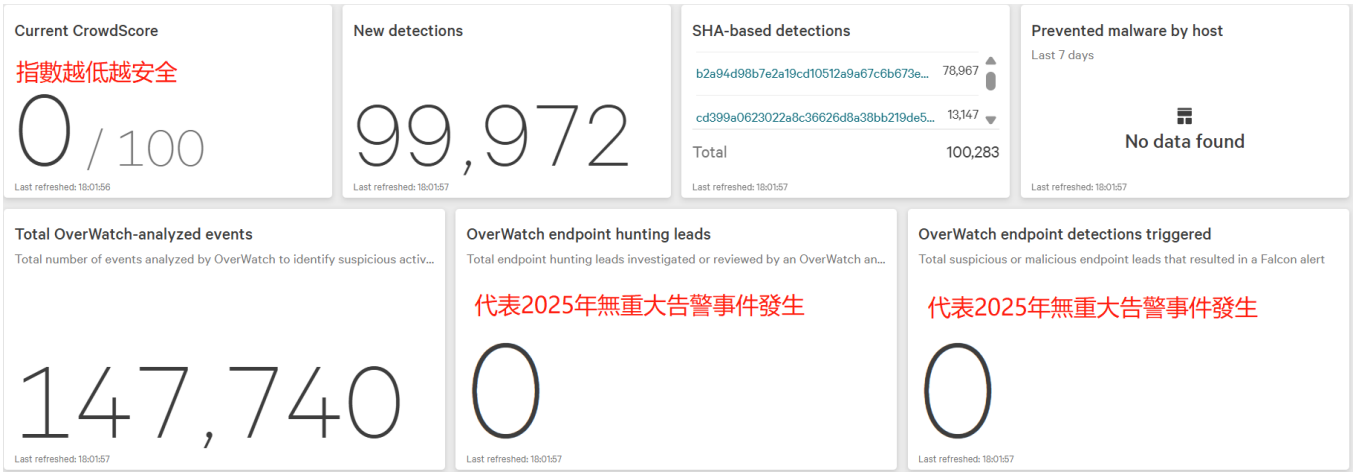
● 資訊安全事件(114/1/1~114/12/31)

本公司 114 年度無重大資訊安全事件，在各資安技術防護層面有效防止各式內、外部攻擊並記錄如下:

114 年度防火牆攻擊防護成效紀錄(114/01/01~114/12/31) 資料來源：防火牆

114 年度事件均被監控與阻隔，期間無重大資安事件產生。

主機端點防護安全指數(114/1/1~114/12/31) 資料來源：端點防護



主機端點防護軟體，佈建於公司三地核心主機，分析事件總數為 147,740 次，所有事件均被阻斷隔離，目前威脅指數為 0，期間無重大資安事件發生。