資訊安全風險管理與運作情形

資通安全風險架構

新至陞為強化資訊安全管理、確保資料、系統及網路安全，於 2023 年設置資通安全專責單位，負責管理新至陞整體營運管理單位、管理制度及核心系統，從公司資訊安全架構、內部管理流程、稽核與控制、機密資料管理等層面，全面推動資訊安全政策。確保公司能預先掌握資安風險，落實資安維運，建立快速應變團隊，並持續建置與推動資訊安全管理系統的建立、執行與改善。

基於資訊安全的重要性，資通安全專責單位每年定期(一年至少一次)向董事會報告公司資訊安全治理與執行狀況。

最近一期提報董事會日期：114 年 12 月 19 日。

資通安全專責單位

考量公司規模及營運狀況，目前編制為資訊安全專責主管 1 人，資訊安全專責人員 1 人，資訊安全專責人員已取得經濟部資訊安全工程師-初、中級能力鑑定，2025 年取得 Fortinet Certified Fundamentals in Cybersecurity 證照。

此外，稽核室稽核人員(取得 ISO27001 資安稽核員認證)亦定期稽核資通安全檢查之控制作業，考量強化 DDOS 防護服務，本公司並於 2024 年完成加入 TWCERT 資安聯盟會員。

一、 資訊安全政策目標：

1.維持各資訊系統持續運作。
2.防止駭客及各種病毒入侵及破壞。
3.防止人為意圖不當及不法使用。
4.防止機敏資料外洩。
5.避免人為疏失意外。
6.維護實體環境安全。

二、 資訊安全控制措施

1.電腦設備安全管理

(1)本公司電腦主機及各應用伺服器等設備均設置於專用機房，機房門禁採用感應刷卡進出，且保留進出紀錄存查。

(2)機房內部空調具有備援機制，可維持電腦設備於適當的溫、濕度環境下運轉；並放置 HFC-23 環保氣體自動滅火系統，可適用於一般或電器所引起的火災。

(3)機房主機配置不斷電設備，並連結公司大樓自備的發電機供電系統，避免台電意外瞬間斷電造成系統當機，或確保臨時停電時不會中斷電腦應用系統的運作。

2.網路安全管理

(1)與外界網路連線的入口，配置企業級防火牆，阻擋駭客非法入侵。

(2)台北集團總部與海外廠:昆山廠及越南廠的連線作業，使用企業虛擬網路(MPLS)方式，避免資料傳輸過程遭受非法擷取。

(3)同仁由遠端登入公司內網存取應用系統，必須申請 SSL VPN 帳號，透過 SSL VPN 的安全方式始能登入使用，且均留有使用紀錄可稽查。

(4)配置上網行為管理與過濾設備，控管網際網路的存取，可屏蔽訪問有害或政策不允許的網路位址與內容，強化網路安全並防止頻寬資源被不當占用。

(5) 本公司企業網站採委外代管，雲端伺服器 365 天全面資安防護機制。

除 IDS 及 IPS 外，為防禦 DDoS 攻擊，採 Cloud WAF 網路應用程式防火牆，基於雲安全大數據能力的實現，透過防禦 SQL 注入、XSS 跨站腳本、常見 Web 伺服器插件漏洞、木馬上傳、非授權核心資源訪問等 OWASP 攻擊，藉由過濾海量惡意 CC 攻擊，避免惡意流量入侵網站，面對 DDOS 攻擊威脅，已備妥流量監控、靜態網頁切換、流量清洗等防禦機制，可確保網站的正常營運。

● 採用框架資料庫存取安全性保護，強化 SQL Injection、XSS 防護。 ● 網站入侵檢測與防護，PHP 網站的主動防禦機制。 ● 帶有清除刪除功能的自動惡意軟件掃描程序。 ● 網站弱點自動檢查建議、虛擬補丁。 ● 具備進階防火牆、WAF、IDS/IPS、自動掃描惡意軟體及病毒等功能，並且能阻擋 DoS 攻擊、0-day 漏洞等常見攻擊手法。		
WAF 防護的主要功能：	IDS （Intrusion Detection System，入侵檢測系統）	IPS （Intrusion Prevention System，入侵防禦系統）

1. ： WAF 專注於應用層的安全防護，可以攔截如 SQL 注入、XSS、跨站請求偽造（CSRF）等攻擊。 2. 實時監控與報告： WAF 可以實時監控網站的流量，識別異常行為並生成詳細的安全報告。 3. 阻擋惡意請求： 根據自定義規則或基於已知攻擊模式來攔截可疑請求，從而保護網站免於被入侵。 4. DDOS 防護： 雖然 WAF 主要是針對應用層攻擊，但部分 WAF 也具備一定的 DDOS 防護功能，可以限制惡意流量。 5. 虛擬修補： 在未能立即修補漏洞的情況下，WAF 可以充當臨時解決方案，通過阻擋特定漏洞的利用來防止攻擊。	主要用於監控和檢測網絡或系統中的異常活動和安全威脅，通過分析流量和事件日誌來識別潛在攻擊，並發出警告。 1. 被動監控： IDS 只是檢測攻擊或異常行為，不會主動干預或阻擋攻擊。 2. 生成警報： 當系統檢測到可疑活動時，IDS 會發送警報給系統管理員，通知他們進行進一步調查。 3. 分析網絡流量： IDS 會對網絡流量進行深度檢查，尋找已知攻擊模式或異常行為。 4. 基於簽名與異常行為： IDS 可以使用已知的攻擊簽名來匹配威脅，或者基於異常行為檢測未知攻擊。	1. 主動防護： IPS 會在檢測到威脅時，直接阻止攻擊並丟棄惡意流量。 2. 即時響應： 與 IDS 相比，IPS 可以即時對攻擊做出反應，避免防止應用層攻擊攻擊進一步擴散。 3. 網絡流量控制： IPS 通常被配置在網絡流量的路徑上，所有流量在進入網絡之前會先通過 IPS 的分析與過濾。 4. 自動修復： IPS 不僅能夠阻止攻擊，還可以根據需要自動進行某些修復措施，如封鎖 IP 地址或重新配置防火牆規則。

3.病毒防護與管理

(1)伺服器與同仁終端電腦設備內均安裝有端點防護軟體，病毒碼採自動更新方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。

(2)電子郵件伺服器配置有郵件防毒、與垃圾郵件過濾機制，防堵病毒或垃圾郵件進入使用者端的 PC。

4.系統存取控制

(1)同仁對各應用系統的使用，透過公司內部規定的系統權限申請程序，經權責主管核准後，由資訊部建立系統帳號，並經各系統管理員依所申請的功能權限做授權方得存取。

(2)帳號的密碼設置，規定適當的強度、字數，並且必須英文、數字、特殊符號混雜，才能通過。

(3)同仁辦理離(休)職手續時，必須會辦資訊部，進行各系統帳號的刪除作業。

5.確保系統的永續運作

(1)系統備份：建置雲端備份系統，採取日備份機制，除了上傳一份於 Microsoft OneDrive 雲端儲存服務外，電腦機房存一份複本，以確保系統與資料的安全。

(2)災害復原演練：每年實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機，再由使用單位書面確認回復資料的正確性，確保備份媒體的正確性與有效性。

(3) 每年對核心系統執行弱點掃描或者滲透測試。

(4)租用電信公司兩條數據線路，透過頻寬管理設備，兩線路並聯互為備援使用，確保網路通訊不中斷。

(5) 配合證交所發布「上市上櫃公司資通安全管控 指引」，加入台灣電腦網路危機處理暨協中心 (TWCERT) ，不定期接收威脅情資，及時修補具威脅之弱點。

6.資安宣導與教育訓練

(1)提醒宣導：要求同仁定期更換系統密碼，以維帳號安全。

(2)講座宣導：每年對內部同仁實施資訊安全相關的教育訓練課程。

三、 投入資通安全管理之資源

114 年企業資訊安全措施推動執行成果

- 每天執行異地備份。
- 本年度執行 1 次電子郵件社交工程演練。
- 本年度辦理 1 次災害還原演練。

- 本年度辦理 1 次核心系統執行弱點掃描或者滲透測試。

- 教育教練：
  - ✧ 資通安全單位同仁持續進修相關教育訓練課程，持續提升專業知識，114 年參加外訓課程共 5 堂，進修總時數 18 小時。

課程	人數	每堂授課時數
上市上櫃公司資通安全管控指引說明 E-Course	2	1.5
資訊安全意識、必備知識與責任 E-Course	2	2
資安事件說明及預防措施 E-Course	2	2.5
ISO 27001 控制措施與資通系統防護基驗證實務	1	3
資通安全弱點通報機制（VANS）	1	3

  - ✧ 114 年共舉辦 6 場「垃圾郵件過濾軟體及電子郵件系統操作訓練」、「防毒伺服器中心管理」、「ISO 27001 如何強化企業防禦體系」、「VMware 基礎觀念」、「企業網路基礎概念與實務」、「社交工程暨資安教育訓練」、等資訊安全教育訓練課程，總人次 47 人，累計訓練時數 128.5 小時。
  - ✧ 所有新進員工皆完成資訊安全與保護教育訓練課程。

- 114 年資通安全教育按月宣導主題

月份	**宣導主題**
1 月	HTML Phishing 正流行，將連結隱藏件 html，搭配混淆手段躲避資安偵測
2 月	假市調公司搜集聲紋？！網路釣魚 AI 助攻，從釣魚信、簡訊進化到分聲/分身詐騙
3 月	解析三種 AI「走鐘」情況與應對之道/紙本郵寄附假名片，投資詐騙新招
4 月	駭客偽冒財政部發動社交工程郵件攻擊
5 月	ASRC 2025 年第一季電子郵件安全觀察
6 月	AI 與協作軟體成駭客攻擊幫兇 中小企業資安事件 4 個月激增 8500 筆
7 月	KnowBe4 發布 2025 年第一季釣魚報告：內部通訊成為最具欺騙性釣魚郵件類型

月份	宣導主題
8 月	AI 瀏覽器可被誘騙，引導至冒牌電商網站自動下單
9 月	AI 推波，社交工程攻擊持續升溫
10 月	國家資通安全研究院提醒勿用有規則性弱密碼溫
11 月	ASRC 2025 年第三季電子郵件安全觀察
12 月	防範 QR Code 詐騙陷阱

四、 重大資訊安全事件對公司影響及因應措施

本公司為上市公司，依證交所「對有價證券上市公司重大訊息之查證暨公開處理程序」第 4 條第 26 款發生重大資訊安全事件時，除依公司資訊安全緊急通報暨應變作業辦理外，應發佈重大訊息；如符合第 11 條扣除其依保險契約設算獲賠金額後之預估損失超過公司股本百分之二十或新台幣三億元以上者，由資通安全專責單位陳報董事會召集人暨本公司發言系統核定後召開重大訊息說明記者會。

本公司資訊安全專責單位除了提供例行每月資訊安全宣導，並針對出現大量將釣魚連結隱藏在 QR Code 的郵件，或將釣魚用的 QR Code 內嵌於加密過的 Word 附件中，讓釣魚連結無法直觀的被安全設備偵測或人員辨識手法，加強對員工資訊安全宣導與教育訓練，以有效避免員工落入社交工程的圈套而點擊釣魚郵件的風險，故本公司 2025 年並未發生重大資訊安全事件。