裕民航運

公司資通安全風險管理

管理架構

1. 依據台灣證券交易所 108 年 1 月 25 日台證上一字第 1081800376 號函暨公司治理評鑑指標及辦理並因應 2021 年起國際海事組織(IMO)對於資通安全之作業要求，強化本公司資通安全管理。

2. 並依據 110 年 12 月 28 日金融監督管理委員會金管證審字第 1100365654 號令增訂「公開發行公司建立內部控制制度處理準則」第九條之一，本公司屬於第二級上市公司：

   - 第一級上市公司(資本額 100 億元以上、臺灣 50 指數成分股、主要從事電子銷售平台及人力銀行等電子媒介商品所有權移轉或提供服務者)：111 年底前須設置資安長、資安主管及至少 2 名資安人員。
   - 第二級上市公司(第一級以外之上市公司，最近三年度之稅前純益未有連續虧損，且最近年度財務報告每股淨值未低於面額者)：112 年底前設置資安主管及至少 1 名資安人員。
   - 第三級上市公司(第一級以外上市公司，最近 3 年度稅前純益有連續虧損，或最近年度每股淨值低於面額)：鼓勵設置至少 1 名資安人員。

3. 為強化本公司資訊安全管理機制，並配合集團資通訊安全政策，已於 112 年 11 月提報本公司董事會通過並發布重大訊息申報。

   - 於總經理下成立「資訊安全管理委員會」
   - 資安人員配置：劉士綺經理 Aron Liu 任**資安主管**、陳志傑系統分析師 Ron Chen 任**資安人員**。統籌資通訊安全相關事務與資源，以配合國際與國內主管機關相關法令與法規要求。

4. 本公司訂有「資安管理組織架構」如附，除資安主管，資安人員外，並包含台北、新加坡、廈門三家公司部門主管及承辦資訊業務相關同仁。

5. 本公司資安主管主要職責為，帶領其轄下的資安人員及資安管理小組，遵循「遠東集團資通訊安全政策」，規劃、維護與處理本公司公司層級之資訊安全與風險管理事宜，訂定/檢討資安政策，並定期向董事會報告。相關工作職責說明如下：

- 推動資通安全管理政策及目標。
- 協調資通安全責任之分配。
- 綜理資通安全資源之調度。
- 監督資通安全防護措施之施行。
- 進行資通安全事件之通報、應變及檢討。
- 核定資通安全相關規章與程序及制度。
- 辦理資通安全管理年度工作計畫。
- 督導資通安全相關工作事項及績效管理 。
- 定期向董事會與經營階層報告。
- 辦理資訊安全教育訓練。
- 將資安風險納入經營決策考量，帶動重視資安的組織文化。
- 建置 ISO27001 資訊安全管理系統(Specification for Information Security Management Systems)

6. 本公司「電腦室」為主要負責/執行資通/資安事務之單位，依照資安事件等級及屬性，視況納入資安管理委員會運作或報告。

7. 本公司資安主管劉士綺經理已具備資訊安全管理系統主導稽核員認證(ISMS, ISO/IEC 27001:2022 Auditor/Lead Auditor Training Course);資安人員陳志傑系統分析師 Ron Chen，已被指定擔任「資安官」，該員也已完成資訊安全管理系統稽核員/主導稽核員訓練(ISMS, ISO/IEC 27001:2022 Auditor/Lead Auditor Training Course)、網路安全封包分析(NSPA)以及 EC-Council Ethical Hacking and Countermeasures Course 等認證課程並獲證在案，上述人員均取得相關資通安全職能證照，符合任用資格，目前在資安研析等具備基礎能量，可有效支援船岸同仁一般性資安事務。

<u>具體措施</u>

1. 本公司資訊安全管理委員會年度會議已依規定完成召開，並完成組織架構及資訊安全政策之滾動修正事宜，後續亦將循序按計畫逐步推動各項資安業務。

2. 配合遠東集團管理，完成內網部分 End of Lifecycle 主機作業系統汰換，因牽涉作業系統與應用程式相依性，依使用服務與資訊安全風險等級評估，將按照服務系統等級優先順序及工作任務與系統導入之進

程，賡續於 2025 年進行替換。

3. 因 COVID-19 之後疫情時代，配合使用 VPN 及 VDI 軟體之連網系統建置與系統性(效)能優化作業，滿足同仁安全遠距上班需求，維持公共安全、資訊安全與網路安全的合作運轉。

4. 依資安規範完成 2024 年度核心系統備份演練，狀況正常。

5. 依照資安情資進行 2024 年度資安教育訓練及各項船岸資訊安全相關工作，以強化本公司整體資安防護能力。

6. 根據「上市上櫃公司資通安全管控指引」，於 2024 年度辦理「船岸惡意程式檢測服務」、「社交工程郵件檢測」、「網頁與主機弱點掃描及滲透服務」等，其中船端主機可疑程式比例約為 1.2%，社交工程演練 133 人次，主機弱點掃描後屬於中度(含)以上之風險均已於年度內修復，將逐年強化各類資安作為。

7. 2024 年 11 月完成年度資通安全檢查之控制作業查核，結果各項作業無重大異常情事。

8. 2024 年度進行船岸惡意程式檢查，偵獲少量 APT 進階惡意潛藏之程式，均已完成檢整，同時，發布相關資安注意事項，提請船隊強化資安警覺，增加防毒(駭)之防禦力。

9. 2024 年 12 月完成資訊安全宣導教育訓練二場次，主要置重點於資安相關法規、網路安全、個人隱私權與資料保護、在外差旅安全事項、AI 應用風險、釣魚郵件與詐騙注意事項與航運領域常見資安事件個案分享等，並開放完成線上補課，各級主管部分也已完成相關資安宣導事項。全員參訓率達95%。

10. 為強化內部資訊安全並滿足供應鏈資安要求，2024 年度已啟動導入 ISO 27001 資通安全體系，預計 2025 年可完成驗證。

11. 有關 2024 年度「資通安全檢查之控制作業」風險等級分析，詳請參考附表。

目標	風險	控制點	風險等級	自評分數
確保系統及資料安全，不被輕易破壞。	若無控制將造成資訊系統輕易被侵入破壞。	一、防止不明人士入侵破壞：防火牆機制的建立，並隨技術的更新，不斷提昇防止駭客及不法人士入侵的防範機制。	1.27	4.73
	系統遭病毒侵入破壞，使系統當機或毀損。	二、避免病毒傳遞入侵為害：1.防止病毒的入侵，安裝防毒軟體做第一道已知病毒防護，進入郵件伺服器的E-mail會先過濾。2.PC安裝使用者端防毒程式。3.建制對E-mail的附加檔案限制，針對特殊危險的附加檔名過濾，以因應病毒的不斷更新。	1.27	4.82
	相關系統資料被竊取外洩。	三、相關系統登錄密碼管制：依據公司資訊控制管制要點所定密碼管理規則，於伺服器建立控管機制，使用人依規定使用，否則無法登錄。	1.18	4.82
	相關系統資料被竊取外洩。	四、系統使用權限的管制：系統使用的權限，包括資料的顯示及報表的輸出，皆須依管理單位所核准的人員及其權限做嚴密的控管，以防資料的外洩。	1.18	4.73