裕民航運

公司資訊安全風險管理

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，強化本公司資訊安全管理。
2. 依據公務機關及一般上市公司實際資安管理做法，並參照過去工作經驗，經與各部門協調討論後，訂定本公司「**資安管理組織架構**」如附(連結)，由本公司徐執行副總國安擔任本公司資訊安全長(Chief Security Officer, CSO)，對內統合相關資源，納編台北、新加坡、廈門有關主管、承辦資訊業務相關同仁，相關職掌(含船岸端)初步完成律訂，並奉准施行。
3. 本公司資訊安全長主要職責為，帶領其轄下的資安管理小組，共同規劃、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。
4. 另由本公司「電腦室」主責一般例行或常態資訊/資安事務，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。
5. 目前單位內已規劃並培訓指定人員擔任「資安官」，該員已完成資訊安全管理系統稽核員/主導稽核員訓練(ISMS, ISO/IEC 27001:2013 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，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。

具體措施

1. 針對本公司內部資訊服務系統程式主體、個人電腦等，針對弱點掃描、電腦惡意程式檢測等工作事項，於 2019 年已完成資安健檢作業，高風險部分於當年度限期完成改正，其餘風險部分則依照等級優序及工作任務，陸續於 2020 年進行修補。
2. 鑒於 2020 年第 1 季 COVID-19 疫情期間異地辦公等資訊連網需求，也完成 VPN 及 Go-Global (iPad 用)之連網系統建置作業，目前可滿足同仁安全連網需求，運作狀況良好。
3. 數位憑證部分於 2020 年完成更新，確保使用者連網認證，其作用如同網路環境中使用的護照，利用公開金鑰密碼技術來提供身份識別的能力，以保護

網路上資料的正確性、保密性等。

4. 已於 2021 年 1 月 7 日完成『裕民航運資訊安全政策』之修訂，相關實施細則依循 ISO-27001 架構編修資訊安全政策細則，於 2021Q1 進行委員會討論修訂與發佈，目前計畫每年至少召(委員)會提報資安業務推動近況乙次並持續依照實況或資安威脅(風險)修訂本公司作法。
5. 已完成 2020 年度資安宣導教育訓練(二梯次)：
   - 2020/11/19 - Cybersecurity awareness training 1st round
   - 2020/12/9 - Cybersecurity awareness training 2nd round

   ※利用搭配線上即時直播及回播課程影片，本公司暨新加玻、廈門子公司全體同仁皆於 2020 年底前完成受訓。
6. 其他：持續進行年度資安教育訓練、資訊資產盤點、源碼檢測、弱點掃描及社交工程等資安業務執行，同時，也將支援船務部針對船端資安業務需求，適時給予協助，以逐步強化本公司整體資安防護能力。已執行
7. 2020 年度「資通安全檢查之控制作業」:

日期: 2020 年 1 月 1 日至 2020 年 12 月 31 日

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。	1.36	4.55
	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。	1.36	4.45
	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	1.27	4.64

目標	風險	控制點	風險等級	自評分數
		使用，否則無法登錄。		
		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。	1.27	4.55