資訊安全風險管理與運作情形

本公司於 2023 年設置資通安全專責單位，設置資訊安全專責主管及資訊安全專責人員，負責訂定公司資訊安全政策，規劃資訊安全措施，並執行相關之資訊安全作業，此外稽核室稽核人員(取得 ISO 27001 資安稽核員認證)亦定期稽核資通安全檢查之控制作業。

基於資訊安全的重要性，資通安全專責單位每年定期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：112 年 12 月 27 日。

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、深圳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 ERP 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。

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：各系統每年實施一次演練，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)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。

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

112 年企業資訊安全措施推動執行成果

- 112 年投入資通安全防範暨應變處理措施之成本約$165 萬。
- 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。
- 教育教練：
  - ✧ 資通安全專責單位之專責人員不定期參加相關教育訓練課程，持續提升專業知識並因應資訊科技之進步及時調整資通安全防範措施及硬體升級規劃，112 年參加外訓課程包括 2 場「Fortigate 基礎課程」、「中小企業接班，不可不知的數位轉型力！」等資訊安全教育訓練課程，累計訓導時數 7 小時，累計參與人數 4 人次。
  - ✧ 112 年共舉辦 6 場「居家工作之資安保密及個資保護」、「中小企業都該懂的 AI 人工智慧」、「企業資安【風險評估與管理】」、「垃圾郵件過濾軟體及電子郵件系統操作訓練」、「企業資安【軟體開發安全概念】」、「社交工程宣導教育訓練」、等資訊安全教育訓練課程，累計訓練時數 30 小時，累計參與人數 28 人次。
  - ✧ 所有新進員工皆完成資訊安全與保護教育訓練課程。
- 112 年資通安全教育按月宣導：

(累計參與人數 481 人次，累計宣導時數 962 小時)

月份	宣導主題
1 月	90%網路攻擊「得逞」！2022 年全球 1/3 企業發生超過 7 次的資安事件
2 月	ASRC 2022 年電子郵件安全趨勢回顧
3 月	假冒 HR 線上問卷,網路釣魚利用微軟 Excel 和表單（Forms）進行攻擊
4 月	勒索病毒再進化的 4 類資安風險
5 月	ASRC 2023 年第一季電子郵件安全觀察
6 月	FBI 認為比勒索病毒更嚴重的威脅:BEC 詐騙

7 月	ASRC 2023 年第二季電子郵件安全觀察
8 月	慢霧首席資訊安全官：WinRAR 存在安全漏洞，且 WinRAR 漏洞檢測工具也是惡意釣魚程序
9 月	2023 上半年三大行動裝置資安威脅以網路釣魚居冠
10 月	QR Code 釣魚攻擊來襲，企業用戶應提高警覺
11 月	ASRC 2023 年第三季電子郵件安全觀察
12 月	收到 Microsoft 帳號異常登入活動,是被駭了？還是網路釣魚？

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。2023 年度未發生重大資訊安全事件。