資通安全政策

本公司於 2023 年 11 月 8 日董事會決議通過設置資訊安全主管，並委任 Dewar Michael Patrick 先生擔任，負責公司資通安全事務。

資通安全政策

為確保資訊的可用性、完整性以及機密性，並免於遭受內、外部的蓄意或意外的威脅，本公司在資訊安全管理政策說明如下：

- 資訊設備

  本公司各應用伺服器等設備均設置於專用機房，機房設置門禁管理。

  機房內部備有獨立空調，維持適當溫度及濕度。設置二氧化碳滅火器，可適用於一般或電器所引起的火災。

  機房主機配置 UPS 不斷電與穩壓設備，連結公司自備發電機供電系統，避免意外瞬間斷電，造成系統毀損。確保停電時，不會中斷電腦應用系統的運作或損傷。

- 網路安全管理

  強化網路監控，建置防火牆及擬定策略，規範內外流量，阻擋駭客非法入侵。

  同仁由遠端登入公司內網存取資訊，須事先進行申請，使用安全的方式登入使用，且均留有使用紀錄可稽查。

- 病毒防護與管理

  伺服器與用戶終端電腦設備內均安裝有防護軟體，定期更新病毒碼，同時可偵測、防止具有潛在威脅性的系統執行檔之異常行為。

  電子郵件伺服器搭配防毒、垃圾過濾機制，防堵病毒或垃圾郵件進入用戶端電腦。

  防病毒系統偵測攔截到病毒，立即予以隔離或刪除，並主動發出風險報告，以利管理人員採取相關措施。

- 資訊存取控制

  同仁對各應用系統使用，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，依所申請的功能權限做授權方得存取。

  帳號密碼設置，規定適當強度、字數，且必須文數字、特殊符號混雜，才能通過。

  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。

  與本公司業務往來之廠商、訪客等，有存取本公司資訊資產需求時，應進行必要審核。且該等人員負有保護本公司資訊資產責任。

- 確保系統的永續運作

  備份：定期進行資料備份，確保資料被破壞後，可立即還原。
  災害復原演練：每年定期實施演練，確保備份媒體的正確性與有效性。

- 資安宣導與教育訓練

  向同仁宣導資安重要性，勿進行違反資訊安全政策之行為。
  不定期對內部同仁實施資訊安全相關的教育訓練課程。

投入資訊

- 投入資源：

  2023 年投入經費約新台幣 235 萬；實施網路安全提升專案。

- 具體成果：

1. 建立各項資安管制措施，諸如：機房維護、作業電腦維護、機房門禁管制、網路管制、人員存取權限控管、資料異地備份、即時更新防毒軟體版本、定期弱掃... 等。
2. 不定期進行資安宣導。
3. 每年舉辦1 場資安教育訓練/ 宣導，參與人數約100 人。
4. 每年進行資通安全內外部稽核。
5. 雲伺服器請安全廠商做了一次流量檢測。根據流量監測報告分析，針對發現的問題進行完善。
6. 增加上網行為管理：實施了全面的上網行為管理方案，加強了對員工上網行為的監控和管理，提高了網路安全和員工生產效率。

7. 增加獨立Web 防火牆：部署了Web 應用防火牆(WAF)，增強對Web 應用的安全防護，有效地防止了SQL 注入、跨站腳本等常見的網路攻擊。
8. 增加終端安全EDR：通過引入終端安全EDR 技術，加強對終端設備的安全防護，提高了企業整體的安全防護能力。