資安重要議題

資安重要議題	
政策及承諾	● 資通安全是企業營運與風險管理的一環，資通安全的落實需要全體同仁認知及充分支持。 ● 有效的資安政策，可達保護資訊資產，包括人員、設備、系統、資訊、資料及網路等安全，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險。
管理目標	● 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。 ● 讓資訊資產的風險降至可接受程度。 ● 提升人員資安防護意識、有效偵測與預防外部攻擊。
行動計劃	資安行動計劃
有效性評估	有效性評估
資安風險事件	資安風險事件

資安行動計劃

行動計劃	要點
提升人員資安意識：	● 「資通安全政策及目標」置於企業入口網站，提供員工遵循 ● 持續辦理「資安教育訓練」（同仁每年每人3小時/專業人員12小時） ● 每年進行「電子郵件社交工程演練」
全面評估資安風險：	● 定期辦理系統弱點掃描、網站安全檢測、滲透測試、防火牆規則檢視等作業 ● 持續評估內外部威脅可能造成之資訊風險
法遵資安認證導入：	● 檢視內部作業辦法，確保符合「上市上櫃公司資通安全管控指引」及相關法令 ● 2023擬導入「ISO 27001認證」，以確保整體資訊安全
業務運作資料保全：	● 強化資料備份 ● 每年進行「核心業務持續運作演練」：BPM、PLM、ERP、MES 核心業務
提升資安管理量能：	● 配置資安專責單位及人員 ● 建立資通安全事件通報窗口

有效性評估

資安違反狀況	2020	2021	2022
重大資訊安全事件數	0	0	0
涉及客戶隱私之違規事件數	0	0	0
因資訊洩露致受影響的客戶數量	0	0	0
因資訊安全事件而支付的罰款/罰金/賠償總額	0	0	0

資安風險事件

<table>
<tr><th>資安風險事件</th><th>發生時間及經過</th><th>處置方式/改善計劃</th></tr>
<tr><td>管道間漏水</td><td>2022年6月初，ISP數據機因管道漏水，造成設備損毀。</td><td>報修廠商至現場更換機器、測試後，恢復正常。此外，遷移中華電信數據機至機房，與另一線路各居一處，互為備援。</td></tr>
<tr><td>網路安全及病毒攻擊</td><td>2022年偵測一般性網路異常及病毒/惡意程式。
<table>
<tr><td>2022年</td><td>Web Security</td><td>Virus</td></tr>
<tr><td>偵測/阻擋次數</td><td>1206</td><td>88</td></tr>
</table></td><td>成功阻擋病毒、惡意程式.....</td></tr>
</table>

電子郵件社交工程演練

- 2022年6月21日進行第1次釣魚信測試，主旨為「郵件信箱超過上限」：
  點擊連結比率：Ubiqconn：42.17%、Ruggon：31.25%
  輸入個資比率：Ubiqconn：19.13%、Ruggon：12.5%
- 2022年7月6日進行第2次釣魚信測試，主旨為「保護您的電子郵件！」：
  點擊連結比率：Ubiqconn：8.68%、Ruggon：4.76%
  輸入個資比率：Ubiqconn：1.83%、Ruggon：0%
- 兩次測試間有進行1.5小時的資安意識訓練課程，未事先告知使用者將有第二次測試的情況下，數據顯示，該課程已幫助使用者提高警覺，儘量避免開啟可疑郵件內的連結或輸入個資，甚至多數同仁未開啟可疑郵件，成效甚好。
- 多數公司平均結果為78%開啟郵件、39%輸入個資。
  (source: https://blog.usecure.io/holiday-phishing-simulation)

核心業務持續運作演練

- 演練之場地擇於中和廠（異地），演練之核心業務應用程式包含ERP, BPM, PLM，計有5台VM參與，一台筆記型電腦做為License server，所有且包含參與的VM皆於夜間完成覆寫至中和廠。VM開機後逐一驗證，皆可順利執行核心業務應用程式，核心業務得於異地持續運作，且符合資安核心三要素：
  - 於異地存放虛擬機器複本，以驗證可用性。
  - 傳輸通道經由site-to-site VPN加密，以驗證機密性。
  - 還原虛擬機器、開機測試，以驗證完整性。


Your Unmet Needs,Our Expertise