一、資通安全風險管理架構

大園汽電資通安全之權責單位為管理部資安組,設有資安專責主管及資安專責人員各一位,負責明訂公司資訊安全政策。大園汽電稽核人員每年定期就內部控制制度及資訊作業循環進行稽核;截至 113 年 11 月,公司無發生任何重大資訊安全事件,以及因事件所遭受之損失,於 113 年 12 月 17 日向董事會報告。

二、資通安全政策

當公司營運數位化的程度越深,資訊安全問題的重要性就日益增加,為避免公司因資安疏失問題而遭受任何損失,特訂定資訊安全作業規範,建立「資訊安全,人人有責」觀念,並全方位做好資訊安全措施。

資訊安全政策如下:

1.機密性:確保各項業務相關資料之機密安全,並予以適當的規範及保護。

2.完整性:確保各項資訊資產的完整,以期正確運用該項資產。

3.可用性:確保各項資訊資產能提供即時且正確的服務,以滿足使用者之需求。

本年度資通安全政策檢討會議已於 11 月 27 日召開。

三、具體管理方案

本公司具體管理方案如下:

| | |
|---|---|
| 系統存取控制 | 公司的資訊系統皆依單位、職位各別授權存取權限予使用者,當員工轉換單位或工作進行調整時,根據工作需求調整資訊存取權限。 |
| 電腦系統管理 | 公司資訊系統伺服器設置於專用機房,內部設有獨立空調及不斷電系統,確保伺服器穩定運作;重要資料使用本地及異地儲存設備備份主機資料。 |
| 網路安全管理 | 公司設置新型防火牆設備,並購買整合式威脅管理授權,包含韌體及一般更新、入侵防禦、病毒偵測 |

| | |
|---|---|
| | 與攔截、網頁過濾等，持續更新、有效偵測阻擋入侵事件；公司電腦系統安裝防毒軟體並持續更新版本與病毒碼。 |
| 郵件安全管理 | 開啟電子郵件驗證機制及對應的防護措施。 |

四、本年度新增資通安全執行成果

1. 113 年 4 月加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)，接收最新資安預警情資、資安威脅與弱點資訊。
2. 113 年 7 月執行社交工程演練，透過寄送釣魚測試郵件，統計員工的開信率、附檔開啟率、郵件連結點擊率等資訊，統計點選各類誘騙信件的比率，瞭解員工的資安意識程度，並於 9 月進行教育訓練課程，增強員工資安意識。
3. 113 年 7 月執行主機弱點掃描，針對公司重要主機如 ERP、KM、大同遙測以掃描工具進行安全弱點掃描，評估主機是否存在已知的安全弱點，依結果報告作為弱點修補參考。
4. 113 年 10 月執行資安健診，項目涵蓋網路架構檢視、有線網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、防火牆連線設定檢視等檢測服務，依據檢測結果及改善建議逐步修正。