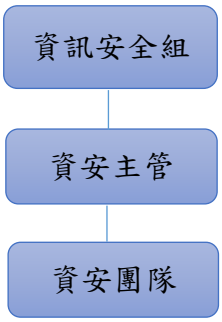
資通安全管理

資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源

(一)資通安全風險管理架構

本公司於管理處下設資訊安全組，設立一名資安主管及相關資安人員，統籌集團的資安運作，包含資安政策、人員配置、軟硬體規劃及經費配置等。並對子公司的資安運作進行監督、複查，確保資安政策被執行及符合要求。



(二)資通安全政策：

1. 資安治理：控制風險加強防範，強化資訊安全架構

   制定完整管理制度，強化教育訓練、資訊安全基礎架構設計及保護技術。確保資訊之系統可用性、限制權限及存取管理、抵抗外部威脅。

2. 法令遵循：建置合規機制，定期檢視/修訂

   建立符合規範機制，定期檢視及修訂相關作業規範以符合資安標準。

   資安政策亦隨時審視、評估，因應資安法規及現況定時更新及發布。由資訊安全組確保各子公司之作業符合新規定。

(三)具體管理方案

1. 制定資訊安全管控文件，包含組織權責、檔案及資料管理、機房安全管理、網路及資料存取控制、系統開發管理等控制文件。
2. 隨時注意或參與資安資訊分享平台（ISAC）、資安通報（CERT）之新聞或通報，做適當處置。
3. 提供最新資安訊息，加強員工網路安全意識與訓練，對未知的資訊內容保持警戒。
4. 外部防護包含檢視威脅，網路、防火牆、主機、重要檔案及紀錄檔(Log)是否異常，並進行相關防禦措施。
5. 網路/應用程式/檔案等存取權限經風險評估，並經相關主管核可，避免不當或不法存取。
6. 程式開發依循程序書，須有完整權限控管，完成後須經完整測試，確保資料完整性。

7. 資訊資產保全(如機房安全管制，消防措施)，報廢時確保資料無法回復。
8. 充分備份、異地備援、災害復原演練。
9. 系統或開發委外需界定雙方有關人員權責、使用安全控管措施及作業程序、賦與廠商相關的安全管理責任。

(四)投入資通安全管理之資源及執行情形：

1. 根據稽核計畫，定時進行內、外部稽核作業，定期追踪改善進度與成效。
2. 檢查各電腦或主機之軟體是否合法，符合公務使用，定時更新系統或防毒軟體。
3. 定期抽查人員異動其作業之權限是否確實更新或取消。
4. 每年度至少召開一次資訊安全管理會議，檢討各單位資安政策之執行情形。

   本年度無發生危害資訊安全之事件。
5. 不定期向公司內部員工發電郵宣導「定期資料備份」或「異地備份」，請大家平時養成做好備份資料的習慣。
6. 製作超過 10 份的資安公告，傳達資安防護重要規定與注意事項。
7. 為提升同仁的資安防範意識，所有新進員工到職前皆完成資訊安全教育訓練課程。本年度已進行了員工的資安教育內訓宣導，共計 798 人次，每人次受訓約一小時。
8. 逐步推動資訊安全認證：

   透過資訊安全認證的程序，完善公司資訊安全程序書及作業，汰換老舊的資訊設備以加強資安防護。

   TISAX 認證：

   本公司重要子公司浙江智泓科技有限公司已於2024年7 月13日通過第三方TUV公司認證，取得 ENX ASSOCIATION 出具的 TISAX 認證證書，有效期限至 2026 年 11 月 13 日。Trusted Information Security Assessment Exchange（可信任資訊安全評鑑交換），是德國汽車工業聯合會(VDA)依據 ISO 27001 的標準規範，所制定在汽車製造商、服務提供商和供應商之間的資訊安全統一標準，確保車輛能夠在製造到運作的完整性及可用性中得到保障，提供汽車產業的資訊安全評估與審核。
9. 以上，於 114 年 11 月 10 日向董事會報告，報告各項資訊安全的政策、投入各項資安的資源及執行情形。