資訊安全管理機制

針對資通安全政策，本公司訂定「資訊安全管理機制」，從科技運用、資安治理、及法令遵循等三個面向來進行。

一、 科技運用

1. 資訊機房網路架構整體清查、建議及規劃

針對資訊安全維運與強化防衛能力，委外進行整體清查、建議及規劃，報告結論，第一階段先更新網路資安設備，以滿足資訊安全需求，第二階段，更新系統伺服器，減少實體伺服器機台，改用虛擬伺服器(Virtual Server)，也節省電力使用，並增建儲存設備與網路備援機制，提升資料安全與系統效能。

2. 社交工程郵件測試服務

本公司在加強資訊安全管理方面，除了用最嚴謹的資安要求規劃網路架構外，也定期委外進行社交工程郵件測試服務(社交工程釣魚測試)，每半年各測試一次。演練的目地，在強化同仁的認知能力。

3. 弱點掃描、防毒軟體

安裝於公司系統上的網頁，必須要進行系統測試、通過弱點掃描、系統復原等測試；伺服器及個人電腦使用中控式端點防護，軟體授權每三年一簽採購，包含防毒軟體及防火牆，管理主控台可自動派發病毒碼、軟體更新、安全策略，並設定病毒爆發防範，可預先阻擋病毒傳染。防毒軟體及社交工程攻擊演練等，強化處理人員的應變能力，以

期能在第一時間即偵測到並完成阻擋,從制度到科技,從人員到組織，全面性提升資安防護能力。

4. 網路資安設備更新

完成第一階段資訊機房網路資安設備更新案，包含：網路交換機、防火牆(含 VPN 功能、中控管理、網路防護監控)、流量控管、網路負載平衡器、SSL 解密設備、無線網路設備、不斷電系統等，另進行數個改善措施，如集團各辦公室與台汽電台北總公司資訊機房，從直接連線改經由防火牆連線；資訊管理軟體應用(如電腦資產盤點、資訊申請單)及無線網路落實實名制申請管理軟體並保留紀錄供查核等,並將持續更新與新增設備。

二、 資安治理

1. 企業網路管制及使用規則

為提高集團資通安全性，經參考資安法管制措施，研擬公司網路管制及使用規則等資安措施如下：

- 已於 2019 年公告台汽電集團台北辦公室無線網路使用規則、及集團公司網路上網管制規則。
- 台北辦公室會議室所有實體網路埠與內部網路隔離，確保資訊安全，並請同仁使用會議室如有連接內部網路需求，可申請無線網路使用。
- 集團電腦禁止所有自動執行及播放功能(外接設備及光碟機等)，

避免病毒感染。

- 私人網路設備(如電腦、手機、平板、無線 AP 等)，非經許可不可使用台汽電集團內部網路及無線網路，以免病毒感染、惡意程式入侵。

2. 資通安全檢查之控制查核

本公司內部控制制度中有關資通安全檢查，為內部控制資訊循環之重要項目，資訊循環包含資訊處理部門之功能及職責劃分、系統開發及程式修改之控制、編製系統文書之控制、程式及資料之存取控制、資料輸出入之控制、資料處理之控制、檔案及設備之安全控制、硬體及系統軟體之購置、使用及維護之控制、系統復原計畫制度及測試程序之控制、資通安全檢查之控制,每年進行資通安全檢查控制查核作業，稽核室檢查結果送交董事會查核；本公司風險評估實施方案：由企劃及轉投資管理部制/修訂公司風險管理運作機制，供各部門依循，並執行全公司風險管理狀況監測，定期提報經營階層會議檢討，其中資通安全部分由行政管理部評估提報，每年配合公司風險評估作業運作。

3. 強化教育訓練

社交工程釣魚測試，測試完成後，依據測試結果安排同仁教育訓練，集團各電廠以視訊同步進行，並提供錄影檔予無法參加人員及各工地外部據點。

4. 資訊安全基礎架構設計

集團各公司導入資訊安全防護架構(網路架構布置方案、雙防火牆、真實體隔離)，與解決方案(資產管理、異常偵測、弱點掃描)，規劃建置資安即時監控系統。

三、 法令遵循

為持續精進資訊安全管理機制，本公司規劃比照資通安全管理法中，對關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，來整合及建立本公司之「資通安全維護計畫」，包含：成立「推動小組」並指派管理代表、年度教育訓練計畫、維護計畫實施情形、稽核計畫、稽核項目、稽核結果及改善報告、與績效追蹤報告等，定期檢視及修訂循環機制與內部作業規範以符合資通安全法令。