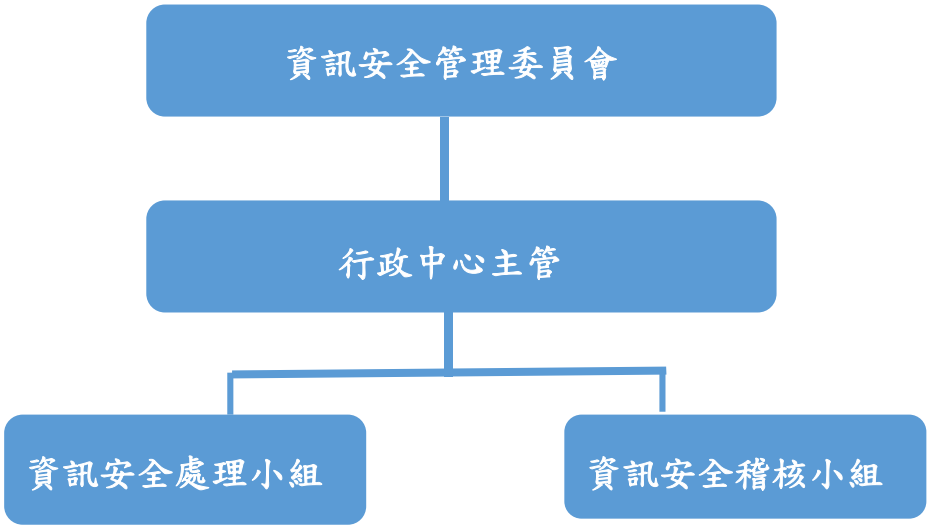
資訊安全風險管理架構

一、 組織:

為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立資訊安全管理委員會。 委員會由總經理為召集人，行政資訊中心主管負責執行並每年一次向董事會報告。組織團隊包含資訊安全處理小組與資安稽核小組；資訊安全處理小組執行資訊安全系統建置，包含網路管理與系統管理；資訊安全稽核小組配合公司稽核單位進行資訊安全稽核工作，包含內部稽核與外部稽核。



二、 資訊安全風險管理架構:

1. 本公司資通安全風險管理權責單位為資訊部門。
2. 資訊部門目前本集團拆分為四個子部門，分別為 MIS、ERP & Programming、Cyber Security、以及 Automation Technology。其中專職負責集團資安相關事務之單位為 Cyber Security，並且在重大事項上直接回報總經理以及董事會。
3. Cyber Security單位負責項目包含母公司及子公司之內部網通以及外部網路資訊環境安全配屬、對日常生產營運之資通安全工作進行定期風險評估以及模擬、規劃公司層級機房資安環境硬體以及軟體之年度計畫及預算編制、內部員工之電腦使用規範以及軟硬體設定、以及月度跟季度執行資訊安全系統管理及內部訓練宣導等相關工作程序。稽核單位依稽核計畫進行督導建議，定期編製稽核報告向董事會報告。每年資訊環境亦經會計師進行資訊作業查核。

三、 資訊安全政策:

資訊部門先針對可能發生之危害像是釣魚信件、勒索軟體、內部蓄意破壞、以及外部惡意侵入進行風險評估，之後再依各類別可能造成之傷害做風險訂定相關策略。政策制度規範主要可區分為：日常員工電腦使用規範、資訊部門基層人員之資安環境管理辦法、以及管理階層之資安戰略佈局包含檔案備份及救援管理、內外網路串聯斷點方式辦法等。

四、 資訊安全具體管理方案:

1. 建立適當防火牆:定期對於網路之進出流量、閘道傳輸速度跟頻率、以及軟體等動作進行紀錄及觀察管制。
2. Email 主機管理: 採用域名金鑰辨識系統 (DKIM) 以及認證可協助管理 (DMARC) 作為主要的防堵勒索以及病毒郵件之方式。另外密碼也採取每三個月定期更換之規定，並且在系統上可隨時監測異常流量或是 IP 來源之郵件。
3. ERP 系統權限設定: ERP 內之程式明確限定可使用之人員及單位，並且數據部分採取使用者不可逆模式 (也就是修改需要得到更高層級許可)。ERP 主機系統採取每日備份，並且主機設立在門禁管控地帶，確保外部人員無法透過網路或是實際現場輕易修改或是破壞。
4. 雲端資料庫備份以及資料取得權限: 除了各部門明確分開讀取權限 (部門平行跨越限制) 之外，單一部門內不同職級之資料取用權限也明確界定 (部門垂直跨越限制)。資料庫之主機也透過防火牆做讀取管理，確保資料庫不能任意受到外部網路讀取跟侵略。另外，資料庫也會定期在不同主機做多重備份來確保生產數據以及營運不中斷。
5. 防毒軟體: 目前公司除了做上述管制外，個別電腦以及中控主機也安裝了相對應的防毒軟體作為防範，而防毒軟體之選用主要為參考年度各大防毒軟體之病毒防堵實際數據來做為評比要素。
6. 第三方資安管理顧問:目前集團除了本身資訊團隊外，亦有簽約第三方團體針對公司整體資安環境做定期諮詢跟評估。

五、 投入資通安全管理之資源

對於現存之廠區以及工作區域，集團採取定期檢視流量及檢核點需求，每年不斷檢閱現有之設備規格並且確保符合集團程度需求之資訊安全層級，以滿足營運和業務上不斷成長及進化之需求。另外集團亦不定期委外提供諮詢建議，並升級相關軟體提升安全層級。對員工教育訓練投注人力及教育設備資源。