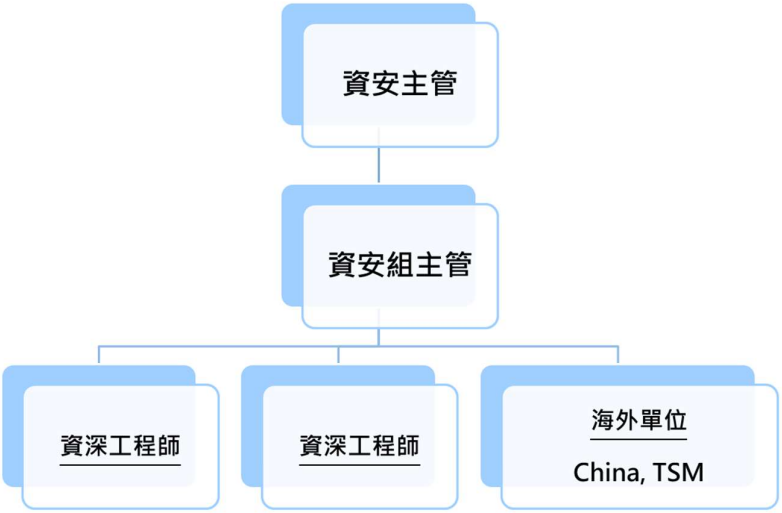
台橡股份有限公司
TSRC CORPORATION

資訊安全政策與管理

1 資訊安全組織架構

本公司資訊安全之權責單位為資訊安全組並隸屬於資訊部，組織設置資安主管乙名，資安組主管乙名與專業資訊人員數名，負責規劃內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實，並每年定期向董事會報告公司資安治理概況。



2 資訊安全政策

組織依 ISO 27001:2022 標準建立並維護資訊安全管理體系，確保資訊與資產獲得適當保護。

透過制度規範，維護資訊資產的 機密性、完整性與可用性，並展現公司對資訊安全的支持，降低資安事故衝擊，持續改善，保障公司、客戶與利害關係人之權益。

2.1 目的

資訊安全政策制定的目的為防禦一切有計畫的、意外的、來自內部的或外部的威脅，以保護公司重要資訊資產之安全。並為宣達公司對資

訊安全推動的支持與決心。

2.2 範圍

資訊服務的所有用戶都有義務保護公司的技術和信息資產，以防止未經授權的訪問、盜竊和破壞。公司的技術和信息資產包含以下：

2.2.1 個人電腦之軟硬體及應用

2.2.2 通信網路硬體和軟體

2.2.3 系統軟體

2.2.4 應用軟體

2.2.5 資料：由公司內部各部門使用，包括員工資料、供應商資料、客戶資料、物料主檔資料、庫存資料、銷售資料、財務資料、製造資料及各應用程式計算後產生的資料

2.3 使用者的責任

規範公司所屬的個人電腦系統，網路和資訊系統等資源的使用政策。

2.3.1 合適的使用權

(1) 公司資訊系統上的用戶帳號僅用於公司業務，不得用於個人活動

(2) 使用者有責任保護其帳號所使用和存儲的所有機密信息

(3) 使用者不得故意從事以下活動：騷擾其他使用者、降低系統的性能、訪問他們沒有授權的公司資訊系統

(4) 使用者不得在其個人電腦上附加或使用未經授權的軟硬體，除非提出申請且獲得主管同意，始得授權使用

(5) 使用者必須向公司直接主管報告其個人電腦中可疑的資安狀況

2.3.2 網路使用規範

(1) 公司的電腦及網路設備，是公司提供員工執行公司業務之工具，公司因促進資源合理使用、保護公司營業秘密、維護公司權益等目的，得對於員工的電腦及網路設備，進行必要的監督或管理

(2) 員工應於合理的限度內，合法使用電腦及網路設備，不得用以處理個人事務、妨害工作效率、干擾網路流通、佔用過多網路頻寬或瀏覽內容不當的網站，亦不得下載、上傳、發送或重製有害、非法或任何足以損害公司信譽、權

益或致公司應對第三人負法律責任之任何軟體、資料或檔案

(3) 不得流通含有猥褻、誹謗、電腦病毒、歧視、騷擾等性質之不當或有害資訊

(4) 員工之間，非經他人明示同意，不得窺伺、讀取或篡改他人電腦內部資料

(5) 研發相關部門的員工，和承包商/外部廠商/顧問必須獲得其主管的許可，並向資訊單位資訊安全管理員提出請求網際網路使用權

2.3.3 授權的登入控制

公司資訊安全政策的控制，主要須防止未經授權的披露或修改關鍵資訊系統的登入控制，登入控制的基本含義是將權限分配給有權訪問特定資源的個人或系統。登入控制主要由登入的帳號和密碼實現。在重要的資訊系統，可以實現進一步的登入限制(例如：雙重認證)。

2.3.4 公司網路遠端登入

遠程連接到內部網絡的唯一可接受的方法是使用 VPN 連線。登入 VPN 必須使用帳號、密碼並搭配多因子認證。

2.4 資安威脅預防措施

2.4.1 員工

員工須對資訊安全威脅進行下列必要措施以降低威脅機率：

(1) 若於非企業網路，必需透過 VPN 連入公司網路

(2) 不要使用共用帳戶。切勿與同事分享登錄信息員工應保護個人電腦資產的安全，離開座位時，將電腦系統鎖上或關機

2.4.2 資訊部

資訊部須對資訊安全威脅進行下列必要措施以降低威脅機率並緩解資安危害的程度

(1) 終端使用者安全管理措施

(2) 當員工離職或受到紀律處分時，應於規定時間內刪除或限制對系統的登入及使用

(3) 定期針對重要系統執行弱點掃瞄

(4) 監控資訊系統的日誌並針對可疑事件進行判斷及處理

(5) 定期評估最新資安解決方案，以提昇公司資安防護能力

2.5 外部廠商資訊安全管理規範

規範委託第三方處理或協助處理資訊作業應注意的安全事項

2.5.1 管理權責

(1) 外部單位: 遵守並簽訂資訊安全作業規範與保密合約，溝通存取方式，提供驗收文件

(2) 資訊協調人員: 告知外部單位相關安全規範、協助簽訂資訊安全作業規範與保密合約、協助權限申請、監督合約遵循、風險評估與報告審核、需求結束後移除權限

2.5.2 資訊提供與存取管理

(1) 提供外部單位機密之資訊時，須簽訂「保密合約」

(2) 存取權限須經核准並說明「委外廠商資訊安全作業規範」及填寫「第三方委外風險評估表」

2.5.3 外部單位責任

(1) 存取控制依保密合約辦理，資訊僅限原申請範圍

(2) 遵循公司合約範本，並經法務審理

2.5.4 資訊需求安全管理

(1) 進行中: 檢視外部單位服務與設備連線

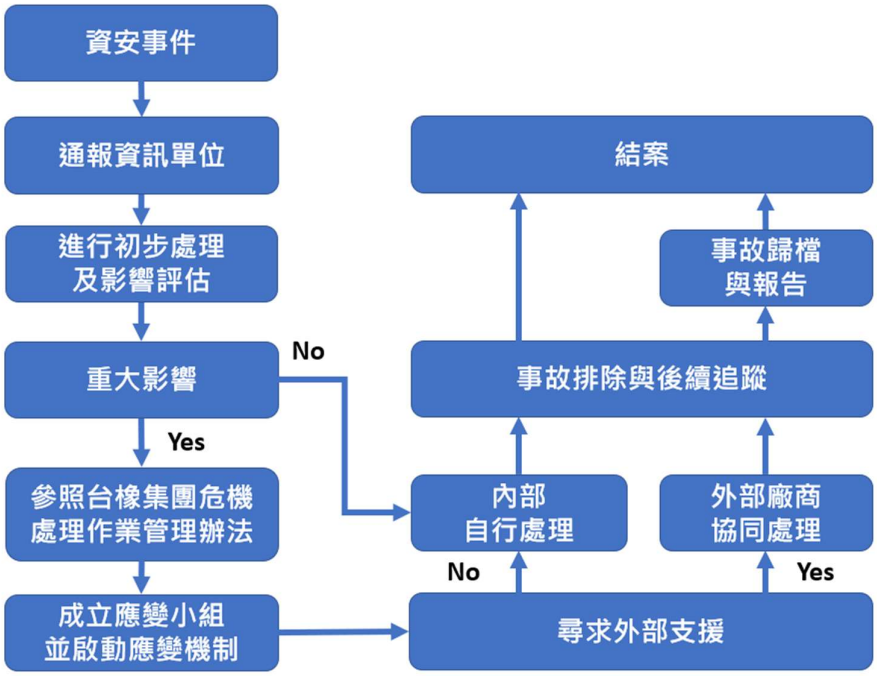
(2) 終止或結束後: 確保資訊資產返還或銷毀，移除存取權限。

2.5.5 其他控管

系統安全驗收、服務變更管理、第三方服務審核

2.6 資安事件應變

本公司資安事故之通報及處理，皆遵守下列資安事件應變程序進行



2.7 營運持續管理作業辦法

為降低資訊系統突發事故衝擊，依營運與 ICT 持續要求，制定應變策略與處理計畫，確保關鍵業務不中斷。

2.7.1 營運衝擊分析

(1) 填寫「業務營運衝擊分析表」，辨識關鍵業務，設定 RTO、RPO、MTPD

(2) 評估資訊安全水準、復原所需資源與預算

(3) 依成本效益分析，制定備援機制與持續計畫

2.7.2 業務營運持續計畫

(1) 內容包含：衝擊分析、復原計畫、測試演練

(2) 明確通報機制、職務分工與聯絡清單、復原場所與程序

2.7.3 計畫更新與維護

(1) 異動時隨時更新，至少每年確認聯絡清單與復原程序

(2) 每年測試至少一個核心系統，三年內完成全部系統測試

(3) 檢討修訂並報資訊安全管理小組核備

2.8 人員訓練

2.8.1 新進員工教育訓練 - 加強資訊安全政策宣導，以確保新進員工了解並遵守公司一切資安相關規定

2.8.2 資安教育訓練 - 針對所有員工每年定期舉辦資訊安全教育訓練課程並於每季以郵件發送資訊安全宣導，以提升同仁資安防護意識