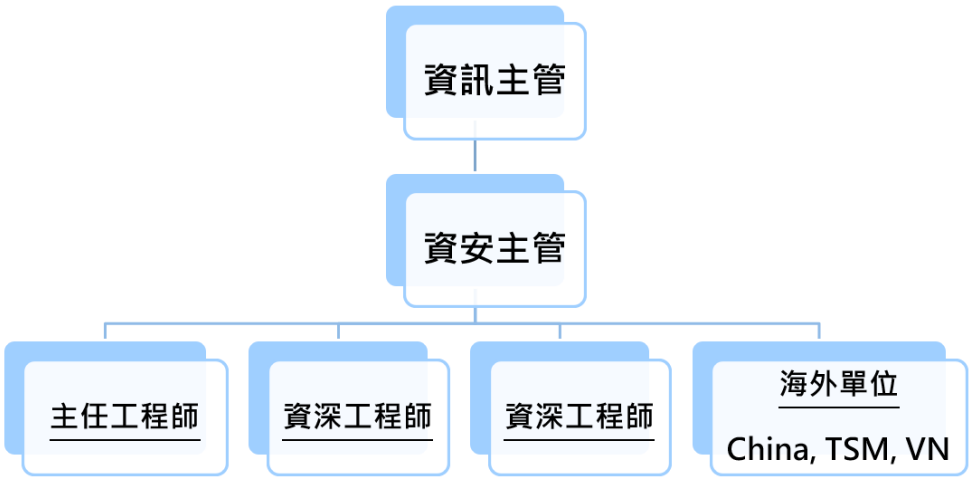
台橡股份有限公司
TSRC CORPORATION

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，該組織設置資訊主管乙名，資安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

本公司及子公司 (以下個別或統稱「公司」) 內部人員不法、不誠信或不道德行為之檢舉與處理，適用本辦法。

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。

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

辦理資訊作業委外前，依據公司資訊安全政策，檢視各類委外作業型態，於資訊委外各階段(事前規劃、事中招標、事後維運)，訂定相關的資訊安全需求，以監督各項資訊作業委外安全之進行，預防資訊安

全事件發生。

2.5.1 事前規劃

(1) 需求評估階段- 資訊解決方案需將資訊安全納入考量

(2) 決定解決方案- 委外建置的資訊安全管理措施

2.5.2 事中招標

(1) 採購階段 - 保密合約與服務水準協議

(2) 履行階段 - 進行資訊安全相關驗證

2.5.3 事後維運

(1) 資訊安全測試

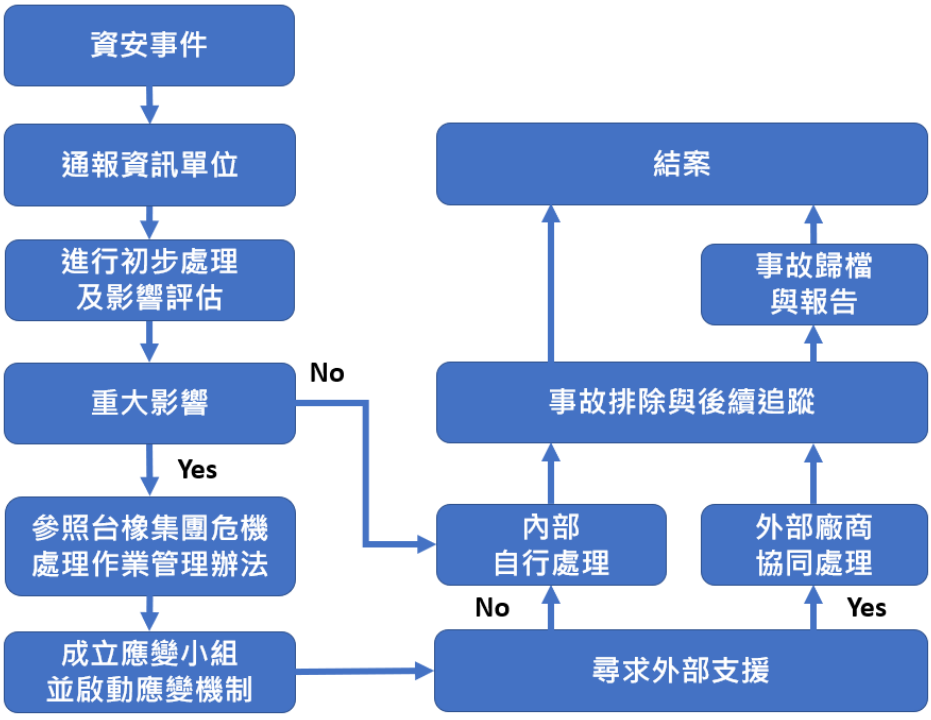
(2) 系統維護

(3) 安全控制與存取管理

(4) 異常事件處理

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 電腦系統復原及作業辦法

為確保公司之電腦系統在發生損毀後，能迅速復原維持資料的完整性

2.7.1 伺服器及主機將區分為三等級，實施不同等級的備份機制

(1) 第一級伺服器為:對公司業務有重大影響，若損壞將影響公

司業務

(2) 第二級伺服器為:對公司業務無直接影響，但對公司內部流程有明顯影響

(3) 第三級伺服器為:對公司業務無影響，只影響少部分公司內部流程且對於公司同仁日常作業無明顯影響

2.7.2 每年依據主機等級進行系統復原驗證測試

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