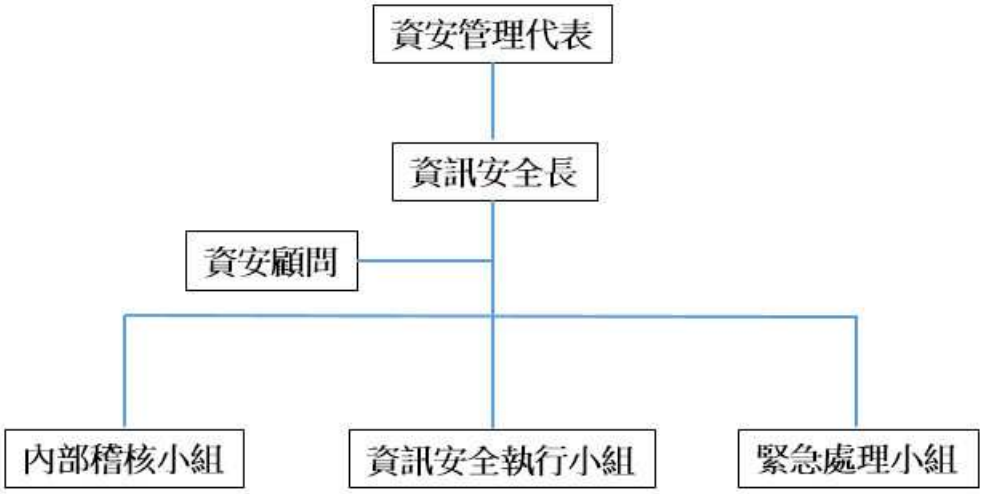
資訊安全組織架構



資安管理代表：

負責核准資訊安全管理系統之範圍、政策與高階管理階層決策

資訊安全長：

由資安管理代表指派資訊部門人員擔任。

資訊安全執行小組：

負責規劃及執行各項資訊安全作業。

緊急處理小組：

各關鍵業務流程負責人擔任組員。

內部稽核小組：

檢查資訊安全管理系統及所有控制措施之管理，提出稽核報告，追蹤改善情形。

資訊安全政策

一.目的

超豐電子股份有限公司（以下簡稱本公司）為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司資訊業務運作所需之環境與架構，使其免於遭受內、外部的蓄意或意外之威脅，特制定此政策規範。

二.適用範圍

舉凡本公司所有同仁及與本公司有業務往來之廠商、訪客等，皆應遵守本政策。

三.定義

資訊資產：收集、產生、運用之資料，以及為完成以上工作所需使用之相關資產，包括人員、設備、系統、資訊、資料及網路等等安全。

- 機密性(Confidentiality)：確保只有經過授權的人才能存取資訊資產。
- 完整性(Integrity)：確保資訊資產其處理方法的準確性及完整性。
- 可用性(Availability)：確保授權的使用者在需要時，可以使用資訊資產。

四.責任

1.本公司成立資安委員會統籌管理制度相關事項之推動。

2.管理階層應積極參與及支持管理制度，並透過適當的標準和程序以實施本政策。

3.本公司全體人員、委外服務廠商與訪客等皆應遵守本政策。

4.所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。

5.任何危及資訊安全與個人資訊保護之行為，將視情節輕重追究其民事、刑事及行政責任之相關規定議處。

五..資安政策之評估與審查

1.資訊安全政策得以電子檔公告於公司內部網站、公告周知。

2.為確保資訊安全管理制度實務運作之可用性、安全性及有效性。本政策應每年至少評估一次，以符合相關法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

資訊安全管理措施

一、公司為管理資訊安全之風險，已訂定資訊安全政策與資訊安全管理措施，並與母公司力成共保企業資訊安全風險管理保險。

二、電腦設備安全管理

1.本公司電腦主機、各應用伺服器等設備均設置於專用機房，機房門禁採用感應刷卡進出，且保留進出紀錄存查。

2.建置異地備援架構。

3.與設備廠商簽維護合約，確保零件故障，可在約定時間內更換。

4.機房主機配置不斷電與穩壓設備，並連結公司自備的發電機供電系統，避免台電意外瞬間斷電造成系統當機，或確保臨時停電時不會中斷電腦應用系統的運作。

三、網路安全管理

1.與外界網路連線的入口，配置防火牆，阻擋駭客非法入侵。

2.同仁由遠端登入公司內網存取 ERP 系統，必須申請 VPN 帳號，透過 VPN 的安全方式始能登入使用。

四、病毒防護與管理

1.伺服器與同仁終端電腦設備內均安裝有端點防護軟體，病毒碼採自動更新方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。

2.建置垃圾郵件過濾機制，防堵病毒或垃圾郵件進入使用者端的 PC。

五、系統存取控制。

1.同仁對各應用系統的使用，透過公司內部規定的系統權限申請程序，經權責主管核准後，由資訊部建立系統帳號，並經各系統管理員依所申請的功能權限做授權方得存取。

2.帳號的密碼設置，規定適當的強度，並且必須文數字、特殊符號混雜，才能通過。

3.同仁辦理離職手續時，系統會 Auto mail 相關人員，由資訊部進行各系統帳號的刪除作業。

六、確保系統的永續運作。

1. 系統備份：建置備份管理系統，採取日備份機制，並建置異地備援。
2. 災害復原演練：每年實施一次災害復原演練。

七、資安宣導與教育訓練

1.定期宣導。每季要求同仁定期更換系統密碼，以維帳號安全。

2.定期實施資訊安全教育訓練宣導，資訊安全政策及相關實施規定。