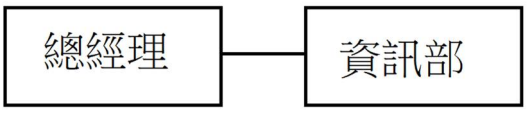
資訊安全管理及執行情形

旭東資訊安全管理及執行情形如下，並擬提報2022年8月5日董事會：

一、 管理架構

由總經理所管轄資訊部負責統籌並執行資訊安全政策，由稽核室擬定相關內部控制程序管理每年進行內部稽核。此外會計師事務所每年依據公司現行資訊作業方式及財務報表簽證之查核需求，考量風險管理等因素，進行資訊環境風險評估與必要之控制測試，以評估公司資訊作業內部控制之有效性。



二、資訊安全政策

1. 維持各資訊系統持續運作

2. 防止駭客、各種病毒入侵及破壞

3. 防止人為意圖不當及不法使用

4. 防止機敏資料外洩

5. 避免人為疏失意外

6. 維護實體環境安全

三、具體管理方案及投入資通安全管理之資源

1. 為因應在有重大災害及突發狀況發生，而危及、阻斷資訊系統及人員的正常運作時，能有效地讓資訊系統繼續運作，以確保公司業務持續營運，訂定了「系統備援及回復計劃」程序，以降低事故衝擊損害。
2. 定期針對ERP系統進行資料還原演練測試，並評估是否合於現況及本公司之營運需求。
3. 建立資訊安全事件通報機制，回應解決資安事件。
4. 使用防火牆設備控管外界與內部網路之資料傳輸並定期檢視相關日誌。
5. 定期對內部資訊設備進行防毒查核並持續進行防毒系統病毒碼與作業系統安全性更新。
6. 使用備份系統進行資料本地與異地端備份。
7. 資安防護機制持續優化，保護公司重要系統與資料安全。
8. 隨時宣導資訊安全訊息，提升員工資安意識。
9. 因資訊安全管理的落實，截至2022年6月底未發生重大資安事件。