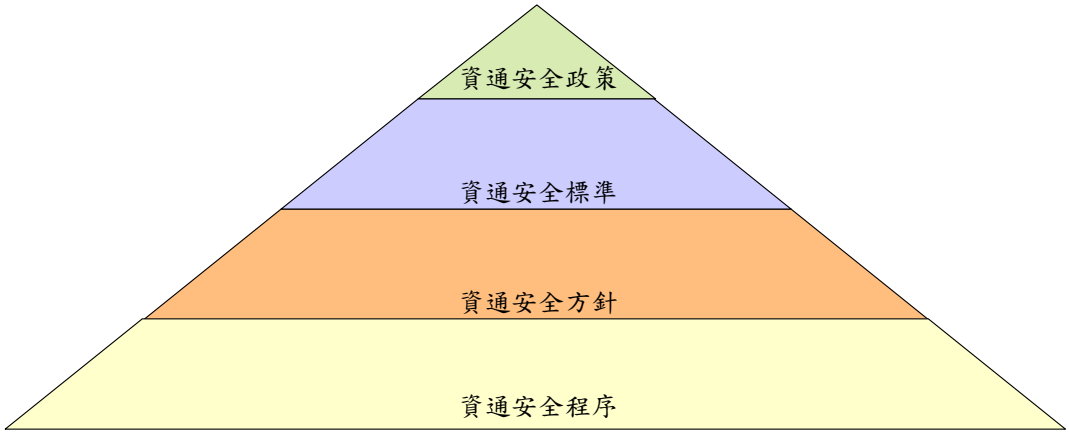
資通安全風險管理架構：



一、設置資訊安全長及成立資安專責單位:資訊安全部，單位配置 1 名資安專責主管及 2 名專責人員，專門負責公司資通安全相關工作，並排定每月定期舉行部門會議，檢視資通安全政策推行狀況。

二、資通安全政策：由資訊安全部召集企劃部門、電算部門、人事部門等相關部門主管，共同商討制定資通安全政策後核定實施，同時揭露於公司電子公佈欄並適時更新政策內容。

三、資通安全標準：遵循「AEO（Authorized Economic Operator）制度」與「上市上櫃公司資通安全管控指引」所規範之標準。

四、資通安全方針：

1. 員工管理及資通安全教育訓練(門禁系統、每年定期各單位資通安全教育訓練、每年定期電子郵件社交工程演練)
2. 電腦系統安全管理(防毒防駭機制、密碼管理、定期與不定期弱點掃描)
3. 網路安全管理(防火牆建置、應用程式防火牆設置、入侵偵測機制、APT 攻擊防禦系統)
4. 情資共享與聯合防禦(MDR 端點聯防、加入 TWCERT/CC 會員)
5. 系統存取控制(系統權限授權定期檢視、線上授權)
6. 系統發展及維護安全管理(系統發展 SOP 建立、密碼管理)
7. 資訊資產安全管理(資產管理電腦化、公物攜出電腦化管理)
8. 實體及環境安全管理(每年定期 AEO 宣導與教育訓練)
9. 資訊系統備援環境建置(HA 系統建置與第一備援中心建置)
10. 個資安全管理(個資存放加密、部分呈現、資料庫防火牆設置)
11. 員工到職、在職及離職管理程序(簽署保密協議明確告知保密事項)

五、資通安全程序

1. 依據資通安全方針制定實施細節
2. 資訊系統備援環境演練
3. 定期舉辦人員資通安全教育訓練
4. 定期辦理電子郵件社交工程演練

5. 資訊安全部之主管及人員，定期接受資安專業課程訓練
6. 落實資通安全控制程序

資通安全宣言：

「遵守業務資訊不外洩 維護資訊安全與穩定」

為強化資通安全之風險管理，本公司訂定資通安全具體管理方案及因應措施如下：

1. 公司已建置資訊設備防毒防駭機制與資訊設備備援環境，每年定期實施資安滲透測試、弱點掃描及自主網路與電腦設備安全查核，提早發現可能的問題和執行漏洞修補，並定期由資訊安全長向董事會報告資通安全防護現況與因應計畫。
2. 內部稽核人員均依稽核計畫每年稽核資通安全檢查作業控制情形，做成稽核報告，並向董事會報告執行結果。
3. 針對新進人員及新晉升主管安排公司依資通安全規範之教育訓練課程，且各單位每年排定並執行資通安全教育訓練課程，資訊安全部亦不定期透過e-Mail、公佈欄及公司經營會議加強資安宣導及案例分享。
4. 公司每三年需申請AEO校正作業(每年辦理自我評估檢查及上傳作業)，並辦理各項安全審查項目(包括實體安全、程序安全與資訊安全)，經實地驗證通過後，始能獲得AEO續證資格，最近一次續證效期為110年～112年。
5. 加入資安情資分享組織「臺灣電腦 網路危機處理暨協調中心(TWCERT/CC)」，取得資安預警情資、資安威脅與弱點資訊。
6. 發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」或「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。