A. 資訊安全風險管理架構：

- 資訊安全之權責單位為資訊中心，負責評估規劃、執行及推動資安管理事項，並向同仁不定期宣導資訊安全意識。
- 稽核室為資訊安全監理之查核單位，定期查核執行缺失，要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，降低內部資安風險。
- 運作模式每年採循環式管理，確保資安可靠度之達成且持續檢討改善。

B. 資訊安全管理方案：

資訊安全管理方案		
類別	**說明**	**相關措施**
權限管理	人員帳號、權限管理與系統操作行為	• 人員帳號權限管理與審核 • 人員帳號權限定期盤點
存取管控	人員存取內外部系統及資料傳輸管道之控制措施	• 內/外部可存取範圍定義管控措施 • 操作軌跡記錄
外部威脅	內部潛在弱點、中毒管道與防護措施	• 主機/電腦弱點檢測及更新措施 • 檔案與信件病毒防護與惡意程式檢測 • 防火牆防護與惡意程式檢測
系統可用性	系統可用狀態與服務中斷時之處置措施	• 系統/網路可用狀態監控及通報機制 • 資訊備份措施、本/異地備援機制 • 定期災害復原演練
教育訓練及宣導	不定期資安風險案例宣導	• 不定期資安風險案例宣導

C.資訊安全政策：

宏泰電工秉持維護公司之資訊安全理念，對於公司所儲存或傳遞之資料應作周全保護與防範，以杜絕毀損、電腦病毒、洩漏、濫用與侵權等事件。本公司資訊安全政策如下：

1. 資訊安全措施，應符合政府法律之規範與公司資訊安全政策及內控管理辦法之相關要求；所有資訊安全控制或程序之開發、修改及建置，須符合並遵循資訊內控管理辦法之機制。
2. 公司所有人員和供應商、客戶，如需公司提供資訊服務，均須依規定程序及指定措施辦理資訊業務，以維護本政策。
3. 本公司各單位資訊資產管理者，必須對其所負責領域或持有之資訊資產，建置使用狀況之監控程序，以隨時發掘系統或單位資訊遭濫用的潛在風險，加強資料之機密性、可用性及完整性。
4. 所有人員對於發生安全事件、安全弱點及違反安全政策與程序之虞者，應透過適當通報機制，報告資訊安全事件及資訊安全弱點。
5. 工作分派應考量職責分離，職務與責任範圍應予區分，以避免資訊或服務遭未授權修改或誤用。
6. 公司嚴禁所有人員於公司資訊設備上安裝、使用、下載非法或未授權之軟體。
7. 本公司將定期修訂資訊安全政策，並貫徹執行，以提昇各資訊系統所有作業之安全。
8. 任何危害資訊安全之行為人，視情節輕重追究其民事、刑事及行政責任與相關懲處。

項目	說明
資安專責人員	已配置資安專責人員兩名。
外部防火牆	強化對外閘道安全，對外網路閘道端採用新世代 Layer7 防火牆。
對外上網線路	強化線路安全，對外上網線路依其服務差異及重要性，已向中華電信申請共 13 條線路之資安服務，與新世代防火牆搭配使用，達到外部雙層防禦效果。
微軟更新	配置 WSUS 更新系統，確保電腦之安全性漏洞補強可即時到位，也避免微軟發佈更新若出現異常時進行控管避免災難發生。
防毒系統	配置趨勢科技最新版本 ApexONE 防毒系統，除一般系統病毒偵測及清除外，強化網頁信譽評等、可疑連線偵測阻擋、行為監控及周邊設備存取控管..等等防禦。
終端電腦 (PC、NB)	強化終端電腦安全性管理，逐步汰換早期作業系統電腦，目前 99% 以上終端電腦皆為 Windows 10 (含)以上作業系統。
資安方案	針對災難備援 3-2-1 架構增設第二實體備援完成，並同步評估離線雲端備援機制並會同中華電信 POC 完成測試，準備進行導入。
教育訓練	針對資安人員外訓報名台灣金融研訓院線上課程，分別為資訊安全意識、必備知識與責任(120 分鐘)、資安事件說明及預防措施(150 分鐘)及上市上櫃公司資通安全管控指引說明(90 分鐘)；另針對同仁舉辦年度資安通識宣導教育訓練課程(120 分鐘)。