資訊安全風險管理架構

本公司資訊安全由資訊管理處負責，訂定內部資安規範與制度、規劃暨執行資訊安全作業與資安政策推動與落實，並依需求適時調整。

內部稽核負責查核內部資安執行狀況，每年稽核一次。

資訊安全政策

1.管理階層應瞭解資訊安全目的並予支持。

2.應訂定資訊安全政策的的說明文件及資料

3.資訊安全政策應定期評估。

4.定期對單位人員及資訊設備進行安全評估，確定其遵守資訊安全政策及相關規定。

5.於委外契約中有關安全需求得依實際需要隨時修改安全控管措施及作業程序等。

建立資訊安全組織

1.指定高級主管人員負責推動、協調及監督資訊安全管理事項。

2.指定單位辦理風險評估、安全分級、系統安全控管措施。

3.單位內若開放給外單位作資料存取，應訂定控管程序。

人員安全與管理

1.依員工職務層級進行適當的資訊安全講習。

2.對員工的私人資訊設備作必要之安全控管程序。

資產分類及控制

1.資產清冊應隨時更新。

2.公司應建置資訊安全等級分賴標準。

實體及環境安全管理

1.公司對攜帶型的資訊財產應訂有安全之攜出管理規則及嚴謹的保護措施並落實執行。

通訊與操作管理

1.公司應與業者簽訂適當的資訊安全協定，賦與相關的安全管理責任，並納入契約條款。

2.公司應使用網路防火牆並定期檢討電腦網路安全控管事項之執行。

3.公司對於敏感性資訊之傳送應採取資料加密等保護措施。

4.公司對於輸出及輸入機密性、敏感性資料應有處理程序及標示。

存取控制

1.公司應依網路型態訂定適當的存取權限管理方式。

2.公司應規範於不使用時用上鎖或密碼等管制措施以不讓電腦或終端機遭非法使用。

3.公司資訊及應用系統應設有作業結束後或在一定期間未操作時即自動登出或中斷連線之保護機制，若需再登入需重新取得授權。

4.公司應依環境或業務需要於網路防火牆作適當之設定。

5.公司應管制使用者的連線功能，並針對電子郵件、單雙向檔案傳輸、互動式存取與存取時段做通盤連線控管考量。

6.公司應指定專人管理應用程式原始碼、資料庫及執行檔。

7.公司的機密及敏感性資料的處理應於獨立或專屬的電腦作業環境中執行。

系統開發與維護

1.定期對使用軟體實施病毒偵測。

永續經營管理

1.辨識關鍵性業務及執行其風險評估、衝擊影響、優先順序。

2.定期作風險估並調整永續經營政策。

內部稽查及其他

1.單位應使用合法軟體。

2.軟體之使用及資料之儲存、處理和報廢，應有適當之控制。

評估與修正

本辦法訂於每年十二月由「資訊安全處理小組」召開資訊安全顧問會議，以獨立公正客觀原則，辦理本公司資訊作業安全事項重行評估與修正事宜，以反映相關法令、資訊技術及本公司業務發展現況，俾使本辦法確實符合安全需求。