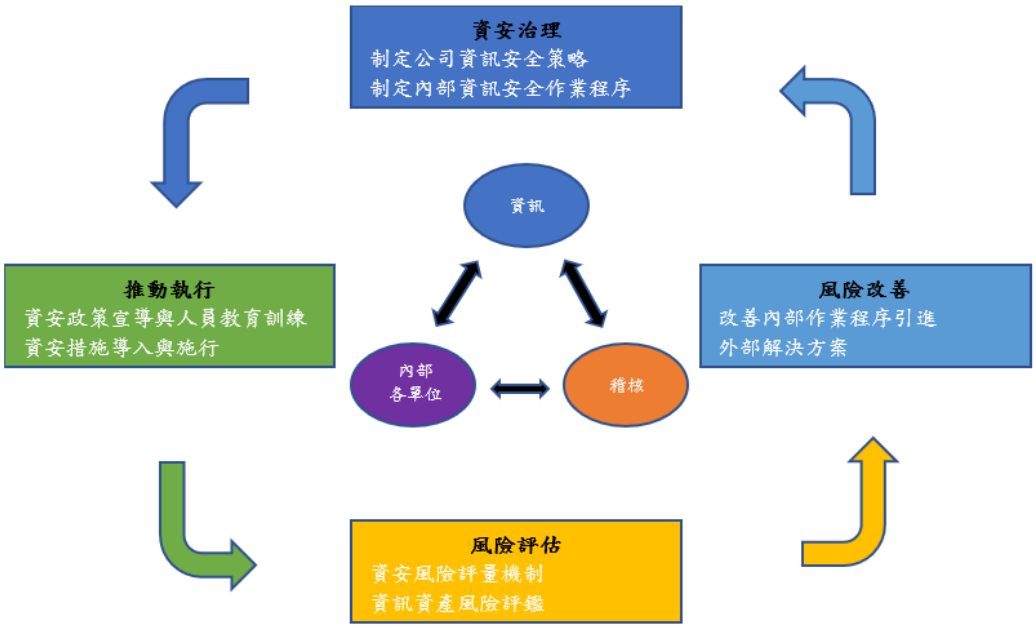
總太地產開發股份有限公司

資訊安全政策及管理方案

資訊安全管理

資訊安全風險管理架構

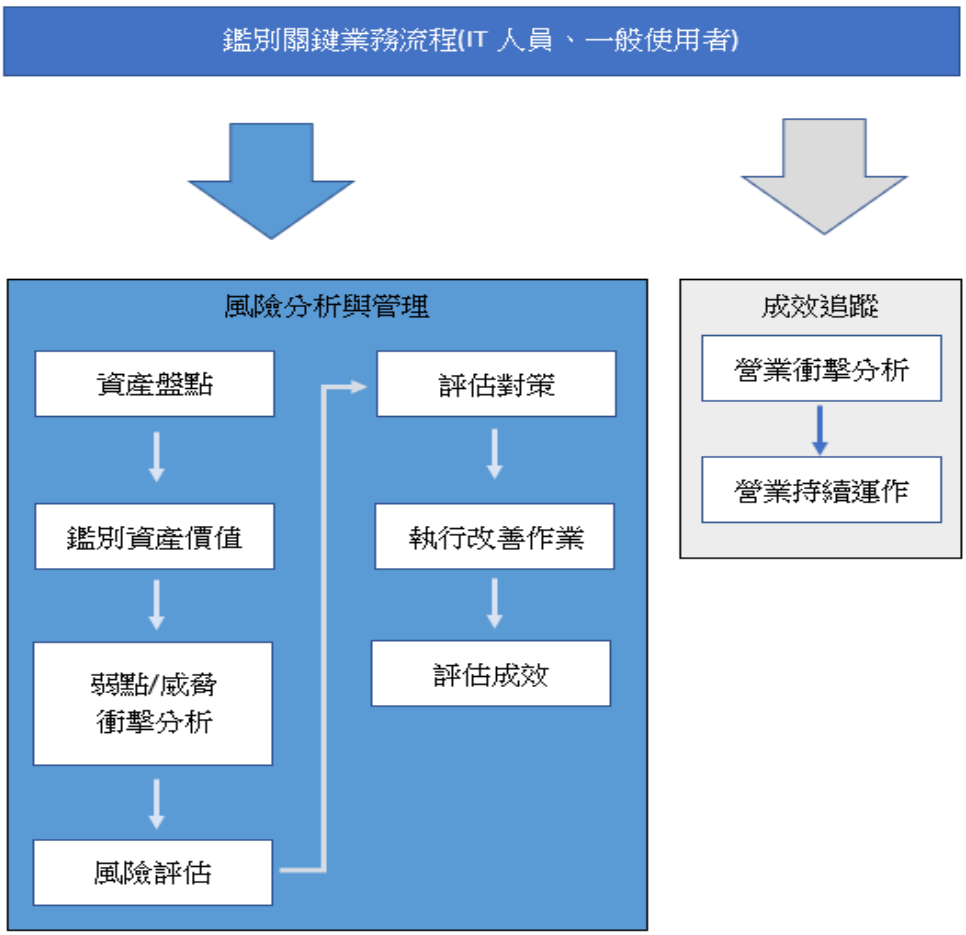
- 本公司資訊安全之權責單位為資訊部，該部設置資訊專員乙名，並與勤業眾信合作，負責研擬內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實，已於 111 年 3 月 15 日於董事會報告。
- 資安政策之評估與審查至少每年評估及審查一次，以反映管理政策、政府法令、公司業務等之最新發展現況，確保資訊安全管理制度的可行性及有效性，以維持營運和提供適當服務的能力
- 本公司稽核室為資訊安全監理之督導單位，該室設置稽核乙名，並與勤業眾信合作，負責督導內部資安執行狀況，若有查核發現缺失，旋即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。
- 組織運作模式-採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。



資訊安全政策及具體管理方案

1. 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，且保留進出紀錄存查。
   (2)機房內部備有獨立空調，維持電腦設備於適當的溫度環境下運轉；並放置藥劑式滅火器，可適用於一般或電器所引起的火災。
   (3)機房主機配置不斷電與穩壓設備，並連結公司大樓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。
2. 網路安全管理
   (1)與外界網路連線的入口，配置企業級防火牆，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，且均留有使用紀錄可稽查。
   (3)配置上網行為管理與過濾設備，控管網際網路的存取，可屏蔽訪問有害或政策不允許的網路位址與內容，強化網路安全並防止頻寬資源被不當占用。
3. 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，由資訊室建立系統帳號，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)同仁辦理離(休)職手續時，必須會辦資訊室，進行各系統帳號的刪除作業。
4. 確保系統的永續運作。
   (1)系統備份：建置雲端備份系統，採取日備份機制，以確保系統與資料的安全。
   (2)災害復原演練：各系統每年實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機，再由使用單位書面確認回復資料的正確性，確保備份媒體的正確性與有效性。
   (3)租用電信公司兩條數據線路，透過頻寬管理設備，兩線路並聯互為備援使用，確保網路通訊不中斷。
5. 資安宣導與教育訓練
   (1)提醒宣導：要求同仁定期更換系統密碼，以維帳號安全。
   (2)講座宣導：每年對內部同仁實施資訊安全相關的教育訓練課程。

本公司資訊風險評估程序如下：



本公司實施之資訊安全管理措施，包含如下：

資訊安全管理措施		
類型	說明	相關作業
權限管理	● 人員帳號 ● 權限管理 ● 系統操作行為之管理	● 人員帳號權限管理與審核 ● 人員帳號權限定期盤點
存取管理	● 人員存取內外部系統 ● 資料傳輸管道管控措施	● 內/外部存取管控措施 ● 資料外洩管道控制措施 ● 操作行為軌跡紀錄分析
外部威脅	● 內部系統潛在弱點 ● 中毒資訊與防護措施	● 主機/電腦弱點檢測及更新措施 ● 病毒防護與惡意程式偵測
系統可用性	● 系統可用狀態 ● 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 ● 服務中斷之應變措施 ● 資料備份備援措施 ● 本/異地備援機制 ● 定期災害還原演練

資安事件通報程序

本公司資通安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行。