杏昌生技股份有限公司
資通安全管理策略與架構

本公司為確保資訊安全及營業秘密保護，設有資通安全組織，並依據內部實際需求制訂資通安全政策及具體管理方案，並投入資通安全管理之資源，以強化資通安全事件應變能力及提升資安意識。

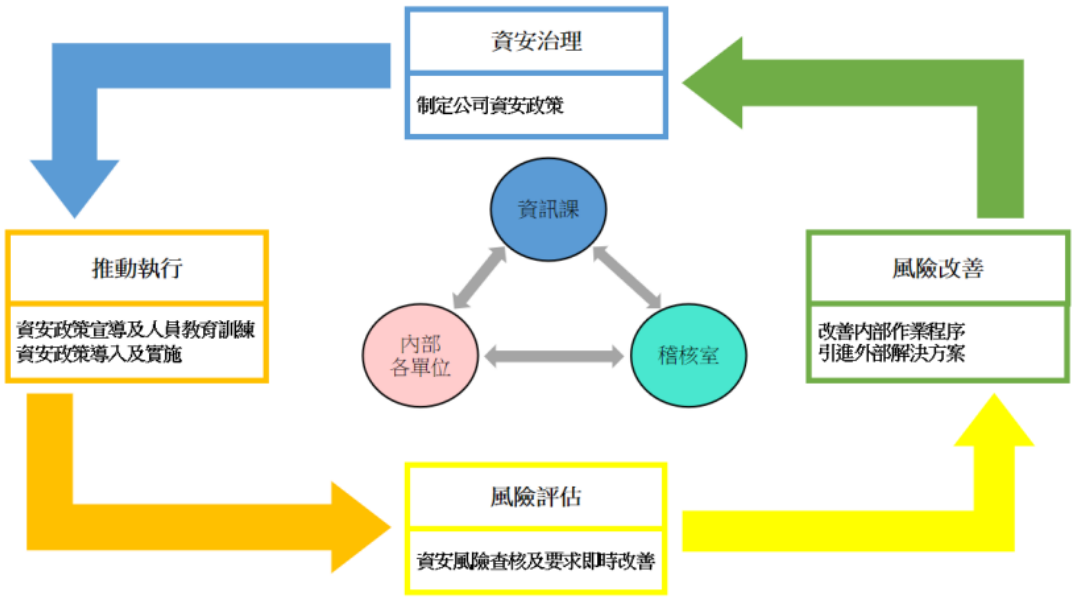
資通安全管理策略與架構

由總經理負責制定資訊安全管理政策，下轄「資通安全小組」及「資通安全監督單位」擬定並執行資訊安全具體管理方案，加上資訊安全稽核單位，進行管理制度內部查核、資訊安全預防及危機處理等監控作業，持續精進內部異常偵測與防護方法，以降低企業資安風險。

1.本公司資通安全小組由資訊課主管擔任資安專責主管及兩名資安人員，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業程序與資安政策推動與落實。

2.本公司稽核室為資通安全監理之督導單位，該室設置稽核主管，與專職稽核人員，負責督導內部資安執行狀況，若有查核發現缺失，立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。

3.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。



資通安全政策

1.確保公司主機、網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資通安全管理規範。

2.確保公司業務資訊之機密性、完整性與可用性。

機密性：確保被授權之人員才可使用資訊。

完整性：確保使用之資訊正確無誤、未遭竄改。

可用性：確保被授權之人員能取得所需資訊。

說明如下:

1.制度規範：訂定公司資通安全管理制度，規範人員作業行為，每年定期檢視相關制度是否符合營運環境變遷，並依需求適時調整。

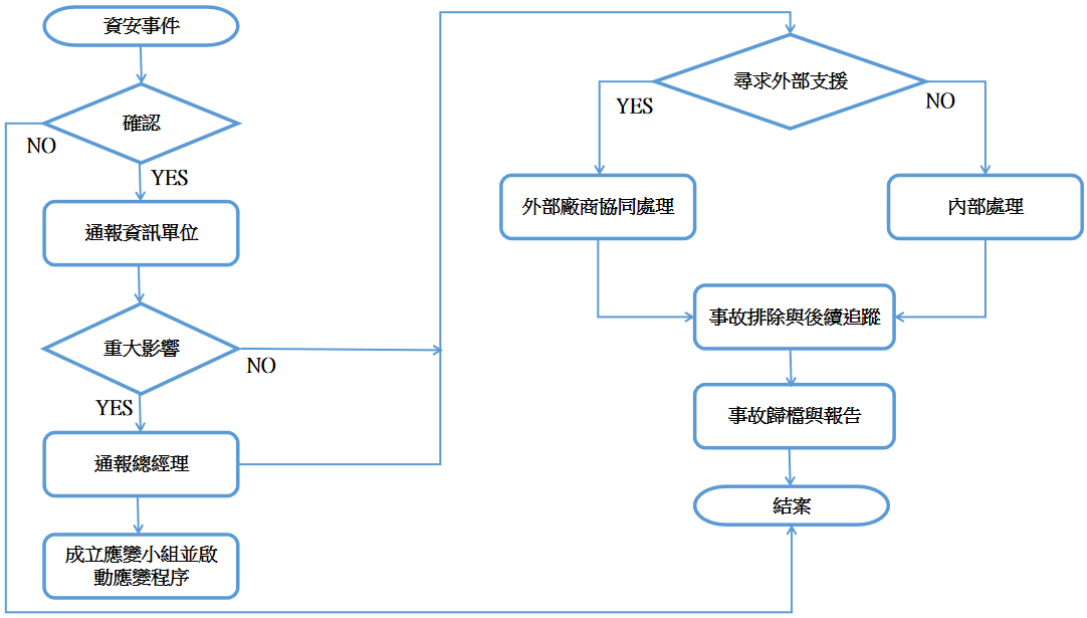
2.系統防護：建置資通安全管理系統，落實資安防護管理措施，以確保電腦資料安全之要求，以提昇整體資訊環境之安全性。

3.人員訓練：進行資通安全教育訓練，提昇全體同仁資安意識，不定期實施資通安全機會宣導，藉以提昇公司同仁資安知識與專業技能，並遵守資訊安全規定。

具體管理方案

類別	**說明**	**相關措施**
權限管理	人員帳號, 權限管理, 系統操作	人員帳號權限管理與審核 人員帳號權限定期盤點
存取管制	人員存取內外部系統, 資料傳輸管道安全措施	內/外部存取管控 資料外洩管控 操作行為軌跡紀錄
外部威脅	網路安全, 防毒防駭的保護措施，委外協力廠商	網路安全維護 防毒防駭程式偵測 訂簽保密協定
系統可用	系統可用狀態與服務中斷時的處置措施	定期資料備份與系統備援機制 定期災害還原演練

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。



投入資通安全管理之資源：

1.防堵外部資安攻擊：建置如防火牆、防毒軟體等安全機制。

2.提升員工資安警覺性：如資安正確觀念宣導、現行資安議題、經典案例分享等，加強員工對於來源不明的資料及郵件的處理。

3.防範內部資安威脅：如員工簽訂保密條款、資料存取及郵件發送均於伺服主機端留存紀錄以供查核、使用者帳號、權限均由各級主管依工作需求核定。

4.資料保全設計：重要資料均定期自動備份，並不定期演練備援回復作業。

5.投入人力：如每日主機伺服器及各系統狀態檢查、定期備份及備份媒體異地存放之執行、定期資安宣導、災難復原執行演練、權限覆核、每年對資訊循環之內部稽核、會計師稽核、...等。

6.資安人力: 資通安全小組由資訊課部門主管擔任資安專責主管及兩名資安人員，負責統籌、計畫、執行及分析資安事件。

7.本公司已成為台灣電腦網路危機處理暨協調中心(TWCERT/CC)會員，該中心可提供資安事件諮詢及協調協處服務，使公司有效接收及傳遞資安情資。

8.資訊公告不定期以 email 方式告知內部同仁宣導資訊相關議題來傳達資安防護重要性。

本辦法於 2023 年 10 月 15 日訂定。