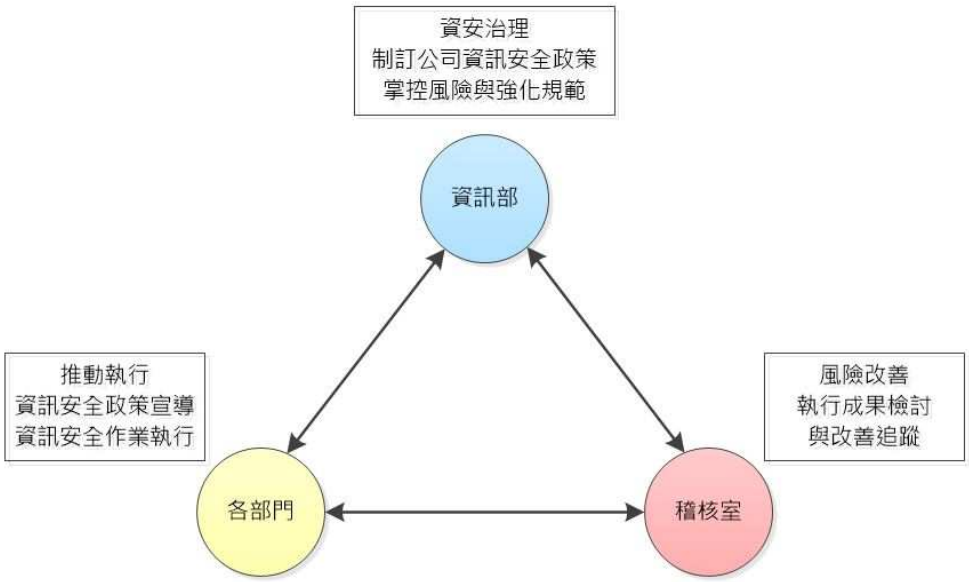
資通安全風險管理及因應措施

（一）資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源

1. 資通安全風險管理架構：本公司董事會已於 112 年 5 月 10 日指派具有資安背景之資訊安全主管。負責資通安全事務，評估公司所面臨之資訊安全風險及需求，強化公司資訊安全管理機制及其有效性，了解組織內資訊安全管理體系該年度之精進與作為，並定期報告至總經理與董事會。
2. 資通安全政策：本公司成長的過程中資訊安全及機敏資料保護對於社會、股東及商業夥伴的承諾。為確保公司內部資訊及資訊系統獲得適當保護，遵照國際標準之要求推動及強化資訊安全管理系統，透過持續提升系統之有效性，提供更安全及穩定的資訊服務。



3. 資通安全管理方案：透過規劃及評估、建置與執行、檢視及覆核、追蹤與持續改善的資訊安全管理方式。加強資安技術發展規劃，如：強化資安攻擊防護、即時偵測外部威脅並有效阻斷、降低機敏資料外洩風險，做為資安發展重點。

(1)遵照國際標準要求推動及強化資訊安全管理系統，加強資訊安全教育訓練。

(2)執行核心業務系統災難復原作業，以確保備援程序與資料備份的有效性，透過實際演練確保資訊系統服務能順利銜接，以預防災難發生的風險。

(3)針對所有資料進行分級分類，並對於所儲存或傳遞之機敏資料採取嚴格的資料外洩防護措施與監控，以確保營業秘密安全。

(4)降低發生毀損、失竊、洩漏、竄改、濫用與侵權等資通安全事件時之衝擊。

(5)續提升各資訊服務系統所有作業之機密性、完整性與可用性。

(6)設置資安事件通報程序，確保資安事件發生時能即時且有效實施因應措施，降低資安事件造成企業團之損失風險。

管理事項	作業說明
1.資訊資產管理	・資產清冊每年定期盤點。 ・重要資產簽訂更新維護保固作業。 ・重要系統及資料進行備份機制。
2.人員管理及教育訓練	・持續建立、宣導及推廣員工資訊安全認知，以提升資訊安全 ・同仁資訊安全宣導訓練。 ・不定期各類資訊安全宣導。
3.實體及環境安全管理	・資訊機房設置有門禁控制，確保只有經過授權人員才可進入。 ・資訊相關設備，應適當地進行安置、保護、監控，以降低環境威脅所造成的損害。
4.電腦系統及網路安全	・網路安全防護與使用軟體控管 ・使用專業防毒軟體並自動更新。 ・網路防火牆設定連線規則，確保使用安全。 ・垃圾郵件過濾、病毒威脅防護及主機重大修補程式更新。
5.系統存取控制安全	・系統權限依員工職務職能以經權限申請作業後存取。 ・每年定期進行權限覆核作業。
6.營運持續運作	・系統服務中斷之應變措施。 ・定期災害復原測試。
7.資訊安全事件管理	・資訊安全事件通報與處理記錄。

4. 投入資通安全管理之資源：

(1)資安強化控管：本公司非常重視的資安議題，因應遠端辦公需求，重視遠端辦公連線安全、資料存取安全及實體環境控管。遠距工作需求增多，強化遠端工作連線安全，導入 VPN 軟體式認證，透過密碼，以防密碼外洩遭駭客入侵，有效解決帳號、密碼被盜的問題，確保組織內部網路的安全性。

(2)資通安全意識強化：有了良好的資訊安全環境，同仁資訊安全意識更是不可或缺，為了持續加強並提升員工資訊安全意識，由資訊部發起舉辦資訊安全教育訓練，宣導基本資訊安全概念、最新的資訊安全趨勢以及最新的駭客攻擊手法，定期更新的資安新聞事件、攻擊手法，讓同仁隨時可以接收到資安相關資訊，並透過不定期信件發送資安公告，提醒資安規則調整及可能存在風險之行為，以降低資訊安全事件發生之機率。

(3)防護機制建構：以縱深防禦概念建構由外而內、由內而外的資安防護機制，致力避免各面向之攻擊影響公司營運系統穩定運作，透過教育訓練與定期公告建立員工資安意識，並定期評估資訊安全政策與作業之妥適性與有效性，擬定專案計畫持續強化保護措施，以降低資訊安全風險，