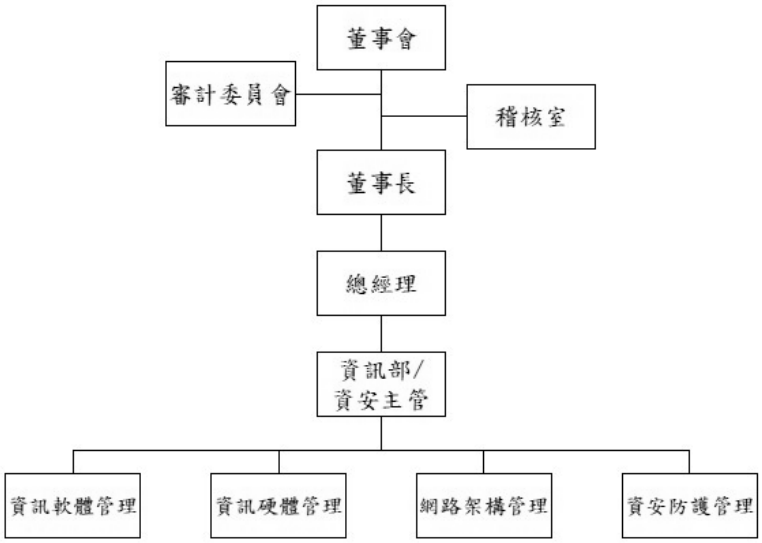
資通安全管理

一、資通安全風險管理架構：

(1)本公司設立資訊部門並由其專責資通安全管理，負責資安規劃及推動執行，以建構集團資安防禦能力及同仁良好之資通安全知識。

(2)為強化公司資訊安全管理機制，本公司設置資安專責主管及資安專責人員負責相關事務。



二、資通安全管理原則：

以所有資訊作業符合國內外法令的要求為目標，到目前為止從外部夥伴及客戶的回應，沒有發現侵害顧客隱私或遺失資料事情生。

三、資通安全政策：

(1)以減少被攻擊的機率及提高入侵難度為主要手段。

(2)以資料備份為基礎，加以管理措施減少資料外流的機會。

(3)對各種作業流程建立內部稽核機制。

四、具體管理方案：

(1)減少不必要的被攻擊的標的：盡量減少放置在 Internet 的服務，比如 FTP 或是網站等。企業網站交由專業服務商代管，避免成為吸引企業網路被攻擊的標的。

(2)建立從外部防火牆到內部防毒軟體、加密線路等的防禦機制，提高入侵難度

a. 不同地點的辦公室，採用硬體 Site to Site IPSec VPN 作為網路連線的方式，提高不同地點資料交換的安全性。

b. 在各營業據點架設防火牆，區隔內部跟外部網路。

c. 建立內部網路防毒管理中控台，監控網域內電腦防毒軟體更新及部屬的情況，監控電腦中毒情況並即時採取必要的行動，避免災情擴大。

d. 郵件伺服器中建立 Mail SPAM 機制，並依實際情況做調整，建立 DNS SPF 規則，減少電子郵件網路詐騙發生的機率。

e. 建立 WSUS 機制，保持區網內作業系統更新狀況良好。

(3)建立完整備份機制，分別針對 File server、DataBsase、重要相關服務建立

備份還原機制以及異地備份。

(4)以權限的方式管理使用者的網路使用，包含 Email、即時通訊、一般網路瀏覽均需申請經過核決流程後，方得開放使用權限，並同時監控、記錄使用者的網路行為。

(5)針對網路使用者做相關的教育訓練，若牽涉到個人資料部份，會進行個資法宣告，並經使用者確認無誤後，始得放行。

(6)包含機房人員進出管制、伺服器維護紀錄、網路帳號及各系統使用帳號權限申請、離職取消機制等，除年度內部稽核對資通安全項目進行查核，確認設備資安控制及系統復原測試執行是否確實，以確認各項機制可有效實施。

(7)強化帳號密碼之安全性，密碼長度、最長使用期限、歷程次數記錄，嚴格執行套用並於全體適用。

五、投入資通安全管理之資源：

(1)民國 114 年為完善端點防護，對於端點防護平台(EPP)之作業系統提升及版本升級並將部屬於端點，提供了更全面、更主動的資安威脅防禦，對已知的威脅和異常採取行動，並且能在發現的威脅與資料庫相符時能反應並發出警報。

(2)規劃導入內部防火牆，將伺服器群與其他辦公電腦做區隔減少服器群暴露的風險，並其韌體更新為新版本解決漏洞問題。

(3)已導入新伺服器及 VMware，階段性將原舊版本 Server 的服務逐漸移轉至新版本實體虛擬主機上繼續相關服役，減少系統漏洞攻擊事件發生。

(4)114 年同仁參加資安及資訊相關教育訓練課程 9 人次共 52 小時。

六、資通作業規範：

對各種作業流程建立內部稽核機制，包含機房人員進出管制、伺服器維護紀錄、網路帳號及各系統使用權限申請\取消機制等，除年度內部稽核對資通安全項目進行查核，確認設備資安控制及系統復原測試執行是否確實，將查核結果報告董事會(114.11.07)。