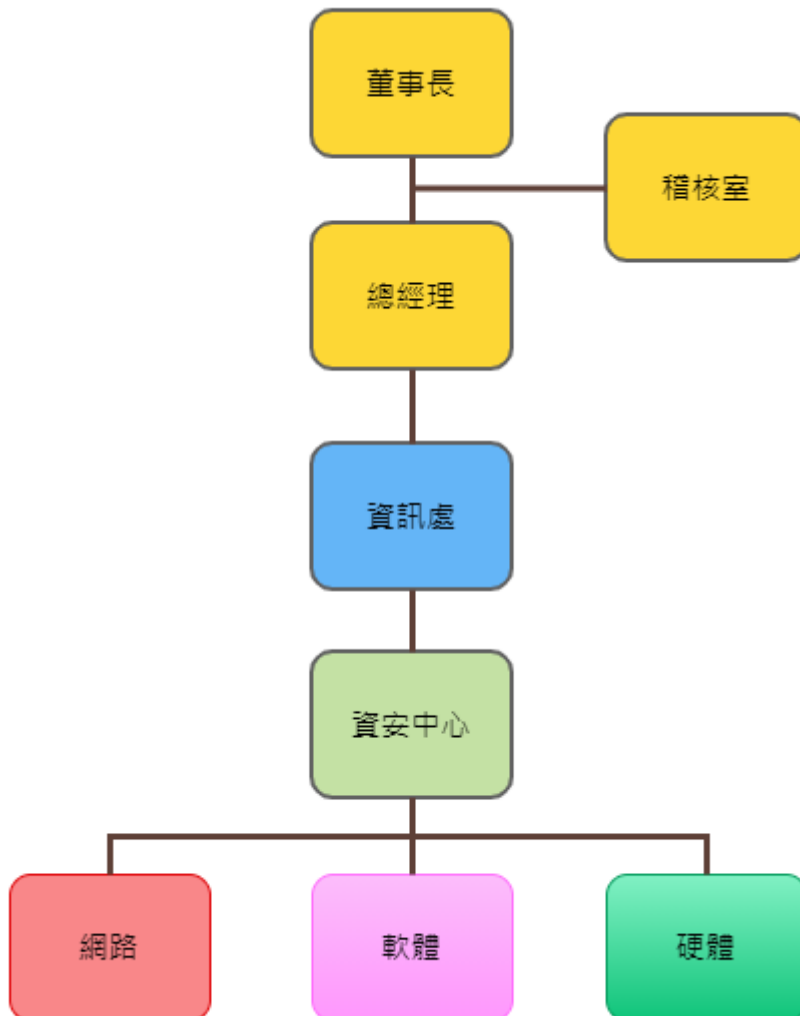


公司資訊安全管理架構

本公司專設資安中心，協助公司的資安規劃與政策推行，對外抵禦駭客及病毒的威脅入侵，對內宣導資安訊息與資安演練提升同仁資安意識。



網路：網路架構/網路 等 設備管理

硬體：PC/Server/Nas/Storage 等 資訊硬體設備管理

軟體：OS/防毒/AD/郵件 等 資訊軟體管理

資安管理原則

公司遵循內部資訊控制辦法，規範公司內部之資訊作業需依據相應權限、存取範圍進行操作。個人權限均以最小單位為主進行管控，公司目前電商服務尚無被駭客入侵個資被盜情事。

網路安全

- 一、利用 AD 控管人員之電腦權限，個人權限均為最小權限為主，密碼均要求複雜度與強制定期變更。
- 二、減少對外服務之設立(例: http/https/ftp..)，必要之對外服務均需受控於防火牆內，並只開啟相應的服務協定與埠號。
- 三、公司電腦均安裝有合法之防毒軟體並有控制中心統一管理病毒碼更新及查看電腦受控狀態。
- 四、郵件均委由中華電信、微軟 M365、Gmail 專業廠商代管，均有標準以上之入侵防護。
- 五、VPN 均整合 AD 帳密之登入，需帳密才可連接公司電腦。使用範圍依照資安管理原則。

資料安全

- 一、人員使用 ERP、電子表單或相關之系統服務，均需提出資訊申請單，依核決權限核准後，才能夠建立相應之權限。
- 二、針對財務、內部服務之資料庫，以及公用資料匣內檔案均有建立備份機制，每日均有專人檢查。

資訊作業規範

- 一、資訊機房配有磁卡式門禁，需設有門別權限同仁才得以進入。廠商進入機房需由專人陪同且需登記。
- 二、人員到離職程序設有資訊確認一環，異動人員均需被確認或取消相應之系統服務、Email、網路、公用資料匣、AD 之授權後，才可繼續作業。
- 三、資訊機房每日有專人巡查主機狀態、機房溫濕度之狀態，每週記錄將寄給管理人審閱與回覆。
- 四、每年公司內部稽核單位針對資訊作業、權限管控、機房管理進行資通安全查核，以確認內部規範為有效實施。