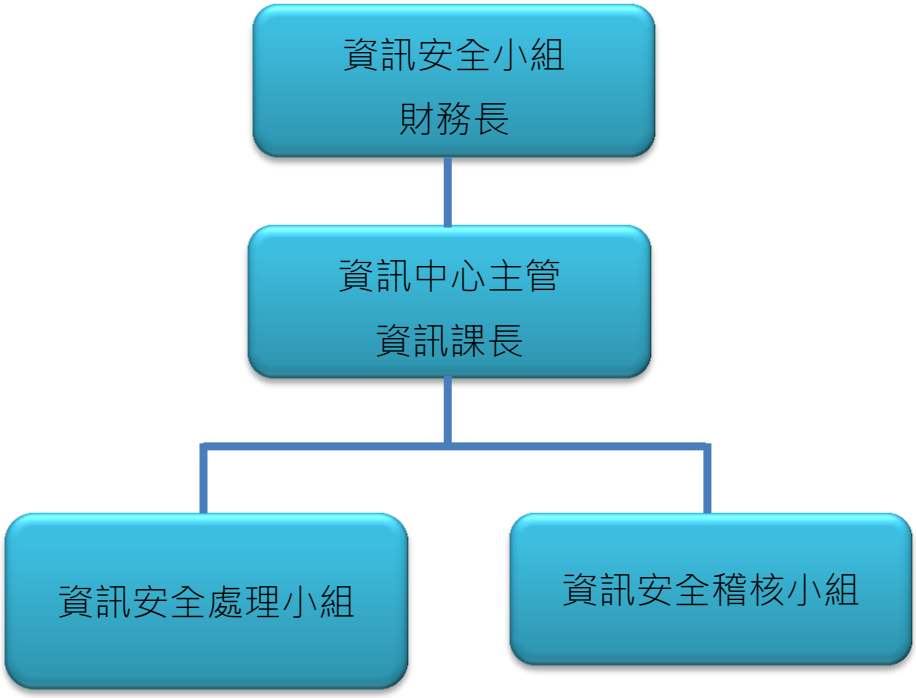
育富電子資訊安全風險管理架構

一、 組織架構

有鑒於本公司應用於網路之服務不斷增加，為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立資訊安全小組。委員會由財務長為召集人，資訊中心主管負責執行並每年一次向董事會報告。組織包含資訊安全處理小組與資安稽核小組；資訊安全處理小組執行資訊安全系統建置與資安問題排除；資訊安全稽核小組配合公司稽核單位進行資訊安全稽核工作。



二、資訊安全風險管理機制:

執行資訊機房、電腦資訊檔案安全、網路安全、郵件安全管理、資訊系統控制存取等管理。

三、資訊安全政策:

I. **資訊安全之目標：**

建立安全及可信賴之電腦化作業環境，確保本公司資料、系統、設備及網路安全，以保障公司利益及各單位資訊系統之永續運作。

II. **資訊安全之範圍：**

1. 人員管理及資訊安全教育訓練。
2. 電腦系統安全管理。
3. 網路安全管理。
4. 系統存取管制。
5. 系統發展及維護安全管理。
6. 資訊資產安全管理。
7. 實體及環境安全管理。
8. 資訊系統永續運作計畫管理。
9. 資訊安全稽核。

III. **資訊安全的原則及標準：**

1. 定期辦理資訊安全教育訓練及宣導，包括資訊安全政策、資訊安全法令規定、 資訊安全作業程序、以及如何正確使用資訊科技設施等，促使員工瞭解資訊 安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，並遵守資訊安全規定。
2. 為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒應採取偵測及防範措施，對入侵及惡意攻擊應建立主動式入侵偵測系統，以確保電腦資料安全之要求。
3. 為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。

IV. **員工應遵守之相關規定：**

1. 申請公司系統及網路相關權限需填寫資訊服務需求單，經單位主管及資訊單位核可後使得建立相關的帳號及權限。
2. 電腦資料及設備，不得任意破壞、攜出、外借、不正當修改，以維護資料完整性，若業務需求時，應提出申請並依循安全保密協定，保護公司機密資料。
3. 安裝軟體需經資訊人員核可，禁止使用無版權軟體。

4. 登入電腦設備後，若離開位置或長時間不使用主機時應登出，以資料機密外洩，為別人所破壞或造成當機之困擾。

5. 離職或新舊職務交接時，需經資訊單位審核及會簽資料安全相關事項，並且移除該員所有系統相關的權限，或更改密碼。

6. 電腦設備使用出現異常時，使用者應立即通知資訊單位，以便檢查或維修。

四、資訊安全具體管理方案:

管理項目	管理方式
防火牆防護	防火牆設定連線規則。
	如有特殊連線需求需額外申請開放。
使用者上網控管	即時依資訊安全資訊通報檢測並宣導安全上網行為。
	自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。
防毒軟體	使用中央控管防毒軟體，並由伺服器自動更新病毒碼。
系統更新	作業系統設置自動更新，因故未更新者，由資訊部協助更新。
郵件安全控管	設置有接收外部郵件自動掃描威脅，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。
	個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
資料備份	重要資料依其特性設定備份週期，並設置異地備份機制。
資安保險	本公司客戶主要為企業客戶，無消費者個資保管風險，於評估市面資安險種保險範圍、適用行業等項目後，暫不投保資安險，但因應資訊安全所面

	臨的挑戰，已導入相關軟硬體,例如防火牆、防毒、入侵防護系統…等，並持續關注資訊環境變化趨勢，並強化公司同仁資安危機意識及資安處理人員應變能力。

五、緊急通報程序

當發生資訊安全事件時，發生單位通報資訊安全處理小組，判斷事件類型並找出問題點，即時處理並留下紀錄，針對問題點提出改善方案，以防再次發生。