資訊安全政策

1 目的

建立裕融企業股份有限公司（以下簡稱本公司）資訊安全政策作為實施各項資訊安全措施之標準，為強化資訊安全管理，保護本公司資訊資產，免於遭受內外蓄意或意外之破壞。

2 範圍

本公司資訊安全管理皆應遵循本政策。

3 權責

資訊安全推動小組召集人：審查並核准本政策。

4 定義

4.1 資訊安全目標

4.1.1 確保本公司重要資訊資產之機密性，降低不當存取之風險。

4.1.2 確保本公司重要資訊資產之完整性，降低未經授權修改之風險。

4.1.3 確保本公司資訊作業持續運作。

4.1.4 確保本公司資訊作業均符合相關法令規定、契約要求。

5 作業規範

本公司資訊安全作業規範如下:

5.1 人員管理及資訊安全教育訓練

5.1.1 辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升公司資訊安全水準。

5.1.2 負責資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責。

5.2 電腦與網路安全管理

5.2.1 採行必要的事前預防及保護措施，偵測及防制電腦病毒，確保系統正常運作。

5.2.2 以防火牆控管外界與內部網路之資料傳輸與資源存取。

5.3 系統存取控制

5.3.1 賦予人員必要的系統存取權限；公司員工之系統存取權限，以執行業務所必要者為限。

5.3.2 取消離職人員使用公司內各項資訊資源之權限，並列入公司人員離職之必要離職人員手續。公司人員職務調整及調動，應依系統存取授權規定，調整其權限。

5.3.3 建立系統使用者帳號及權限管理制度，加強使用者通行密碼管理，並要求使用者定期更新。

5.3.4 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，事前簽訂契約或協定，明定其應遵守之資訊安全規定及應負之責任。

5.3.5 建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

5.4 應用系統開發及維護安全管理

5.4.1 自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量。

5.4.2 系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免未經授權之異動。

5.5 資訊資產安全管理

5.5.1 建立與資訊系統有關的資訊資產目錄。

5.5.2 建立資訊安全等級之分類標準及適當的標示識別方式、相對應的保護措施。

5.5.3 依據資訊資產目錄鑑別其可接受之資訊安全風險等級，並留存相關紀錄。

5.6 實體及環境安全管理

5.6.1 就設備安置、周邊環境及人員進出管制等，訂定妥善之實體及環境安全管理措施。

5.7 業務永續運作計畫之規劃與管理

5.7.1 訂定業務永續運作計畫，評估各種人為及天然災害對公司正常業務運作之影響。

5.7.2 訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

5.7.3 建立資訊安全事件緊急處理機制，在發生資訊安全事件時，依規定之處理程序，立即向權責主管單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。

5.7.4 訂定資訊安全訊息通報機制，針對與資訊系統有關之資訊安全事故，採取適當矯正程序，並留存紀錄。

5.8 資訊安全政策之審查及修訂

5.8.1 本政策應至少每年或內外部環境發生重大變更時，於資訊安全管理審查會議進行審查，以反映相關法令、技術及本公司業務等最新發展現況，並予以適當修訂。

5.8.2 本政策經資訊安全推動小組召集人核准，於公告日施行，並以電子郵件或其他方式通知本公司所有內部與外部人員，修正時亦同。