第一條 目的

友訊科技股份有限公司(以下稱本公司)為強化資訊安全管理，確保重要資訊資產免受內外部蓄意或意外之威脅，以維護資訊之機密性、完整性與可用性，特訂定本政策。

第二條 作業依據

本政策係參酌 ISO/IEC 27001：2022 資訊安全管理系統國際標準訂定。

第三條 效力

本政策之效力優於本公司相關資訊安全政策。

第四條 資訊安全管理目標

本公司資訊安全管理目標為保護資訊資產之機密性、完整性與可用性。

機密性（Confidentiality）:確保只有經授權的員工才能存取資訊。

完整性（Integrity）:保護資訊與處理方法的正確性與完整性。

可用性（Availability）:確保經授權的使用者在需要時可以取得資訊與使用相關設備。

第五條 資訊安全組織

本公司為確實掌握資訊及通訊安全，參酌 ISO/IEC 27001：2022 資訊安全管理系統國際標準及公開發行公司建立內部控制制度處理準則，以資訊技術暨安全部為資訊安全管理專責單位，成立「資訊安全管理委員會」，由執行長擔任召集人，資訊技術暨安全部主管擔任資訊安全管理代表，各資安業務相關單位(產品、個資、隱私等)指派資訊安全代表，定期召開資安管理會議，討論相關資訊安全政策及其他資安相關重大議題，執行長定期向董事會報告資安治理概況，完善資安監督治理之責。

第六條 定期檢討

本政策應至少每年評估一次，以反映政府法令、資訊技術、內外部威脅及業務需求等最新發展現況，確保資訊安全管理實務作業之有效性。

第七條 資訊安全管理原則

本政策之管理原則主要是依據 ISO/IEC 27001：2022 的管控要項條文而訂定的。

一、資產管理

為保護本公司資訊資產安全，應建立資訊資產清冊，並訂定資訊資產分類、分級及管控措施原則。

二、人員安全

為降低公司內員工人為因素影響本公司資訊安全，應視需要實施適當資訊安全教育、訓練及宣導，以提高人員對資訊安全之認知。

三、實體與環境安全

為確保機房及相關設備之安全，應訂定電腦機房門禁、設備檢查及管理原則及一般資訊設備使用、管理及報廢原則。

四、通訊與作業管理

為確保正確、安全地操作資訊設備，應訂定資訊設備及網路使用規範，並建立惡意程式、木馬程式與勒索病毒之防範機制。

訂定資料備份作業之管理原則。

訂定網路安全控制機制及監督系統使用狀況軌跡，以維護網路安全。

五、存取控制

確保資訊系統之存取，訂定使用者密碼、註冊、變更、刪除及定期審查機制；訂定網路安全服務機制，區隔內部網路及聯外方式，管控遠距工作及雲端服務之使用，以維護網路及資料安全。

六、密碼與金鑰管理

為確保公司的系統運作與各類帳戶的機密性，公司應進行必要的密碼與金鑰管理，將外洩風險降至最低，適當保護本公司之機敏性資訊。

七、資訊系統取得、開發及維護

為確保應用系統開發管理、測試、驗收、上線、維護作業之安全，應訂定標準管制程序。

八、資訊安全事件管理

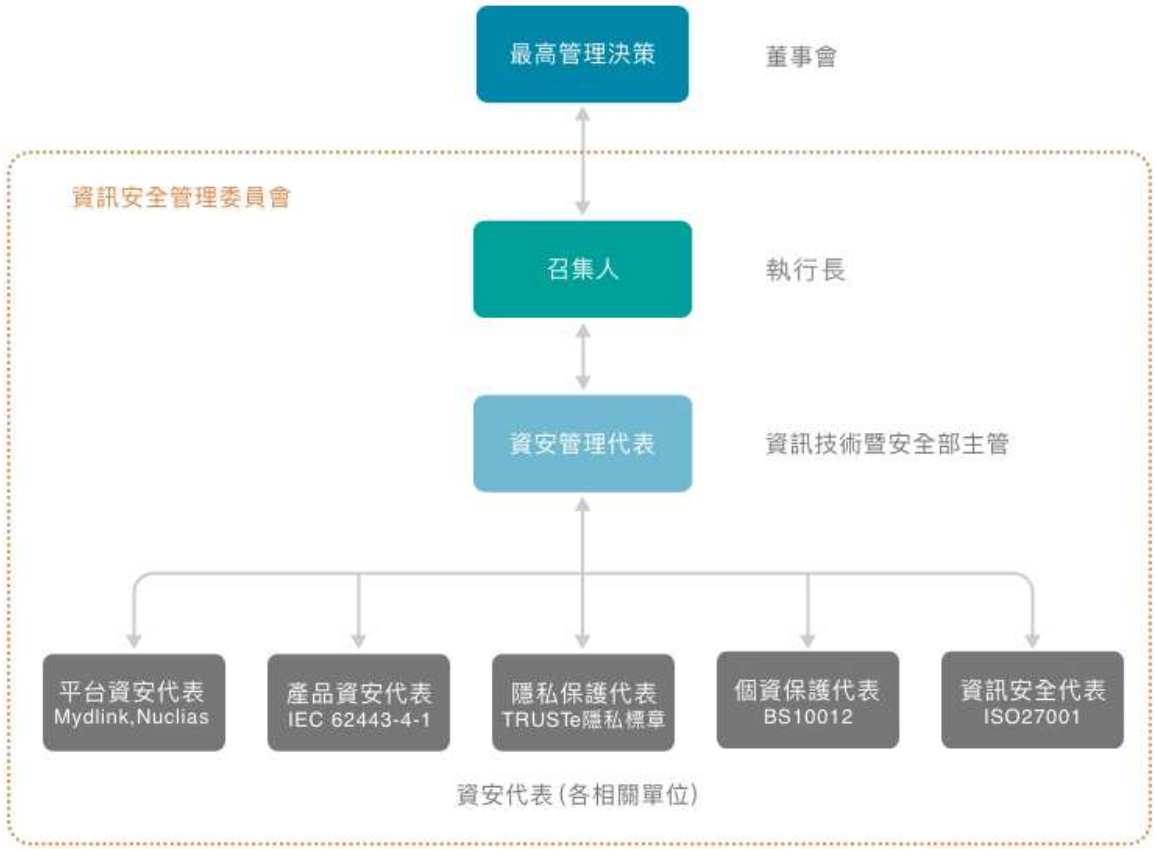
為降低資訊安全事件造成之損害，應建立資訊安全通報及處理程序。

九、營運持續管理

為確保本公司業務持續運作，應建立重要系統之業務持續運作計畫並落實每年定期演練。

第八條 附則

一、 友訊科技資訊安全組織圖



二、 本政策經董事會決議通過後公佈實施，其修訂時亦同。

三、 本政策訂立於中華民國一一一年二月廿二日。

四、 本政策修訂於中華民國一一三年十一月十三日。

五、 本政策修訂於中華民國一一四年八月十三日。