威健實業股份有限公司
資訊安全政策

民國 114 年 01 月 13 日董事會增訂通過

壹、前言

基於威健實業股份有限公司（以下簡稱本公司）的業務特性，為維護本公司及其各利害關係人(包括但不限於員工、客戶、原廠/上游供應商、股東、投資人與金融/證券機構、非原廠之供應商及政府/主管機關與社會)之權益，本公司及全體同仁有責任和義務，共同建立及維護一個安全的資訊與通訊作業環境，讓資訊安全成為企業文化的一環，特訂定資訊安全政策以明確定義安全目標與安全要求，以資遵循。

貳、目的

本公司資訊安全政策制定的目的，在提供可資依循之企業資訊安全指導大綱及方向，明確定義本公司資訊安全管理之目標，並作為本公司各事業單位規範所管轄業務安全責任之指導原則。強化資訊安全管理，確保資訊資料、系統、設備及網路通訊之安全，以有效降低因人為疏失、蓄意破壞、設備故障或天然災害等因素導致資訊資產遭竊、不當使用、洩漏、竄改、毀損或服務中斷之風險。並符合資訊安全管理制度(ISMS)要求，確保資訊資產之機密性、完整性與可用性。

一、機密性：確保被授權之人員方可合理的使用資訊，以防止資訊被不當揭露。
二、完整性：確保資訊不受未經授權的竄改與資訊處理方法及結果的正確性。
三、可用性：確保經授權的使用者，在需要時可以取得資訊，並使用相關資產。

參、依據

為反映科技和資訊安全領域不斷變化的格局，並確保組織能夠保護其資料、資訊資產和隱私資訊免於受到網路的威脅，乃依據 ISO/IEC 27001:2022 (Information technology - Security techniques - Information security management systems - Requirements)之資訊安全管理系統國際標準，以訂定本政策。

肆、名詞定義

一、機密性（Confidentiality）
　　確保只有經授權的人，才可以存取資訊。
二、完整性（Integrity）
　　確保資訊與處理方法的正確性與完整性。
三、可用性（Availability）
　　確保經授權的使用者在需要時可以取得資訊及相關資產。

伍、 適用性聲明書

為了執行 ISMS 各項控制項目，本公司已制定「適用性聲明書(ISMS-L1-01-F01)」，描述與組織之 ISMS 相關且對其適用之各項控制目標與控制措施的已文件化聲明。對於不適用之控制項目應說明其不適用理由。

陸、 資訊安全管理目標與內容

一、本公司各事業單位執行業務時必須遵守政府相關法規(如：專利法、著作權法、個人資料保護法、個人資料保護法施行細則等)之規定。

二、設置資訊安全管理委員會，負責本公司資訊安全管理系統之建立及推動事宜。

三、建立組織全景評鑑機制，以界定資訊安全的方針與資訊安全管理系統的實施範圍，並了解組織全景及關注方的需要與期望。

四、訂定文件控管作業規定，以律定資訊安全制度相關文件之制定、修改、編碼、發行等管理原則。

五、建立資訊資產之管理機制，以統籌分配、有效運用有限資源，解決關鍵安全問題。

六、建立風險評鑑管理辦法並識別出各類資產的風險，以採取適當之風險處理措施，加以管控、降低風險至可接受之程度。

七、定期實施業務相關之資訊安全教育訓練，宣導資訊安全政策及相關實施規定。

八、建立機房實體及環境安全防護措施，並定期施以相關保養維護。

九、明確規範資訊系統、網路服務、敏感資訊之使用權限，防止未經授權之存取行為。

十、建立資訊系統獲取、開發及維護作業流程，明確規範系統於開發及委外相關遵循之依據，且資訊系統或服務應於建置或推出前，應將資訊安全相關議題納入，以防範危害系統安全之情況發生。

十一、訂定及執行資訊安全內部稽核活動，以落實資訊安全管理制度，針對未盡事項執行矯正措施。

十二、訂定資訊安全之營運持續計畫並實際演練，確保本公司遭受突發事故時業務得以持續運作。

本公司所有人員皆負有維持資訊安全之責任，且應瞭解及遵守相關之資訊安全管理規定，並於工作職責中落實。

柒、 修訂與公告

本政策由「資訊安全管理委員會」每年定期審議，另組織、業務、法令或實體環境等因素之變迭時，予以適當修訂。本政策經「董事會」核定後公布施行，修正時亦同。