東元電機股份有限公司

資訊安全政策

1、 目的

東元電機股份有限公司（以下簡稱本公司）為強化資訊安全管理與維護本公司之永續經營，遵循相關法令法規並保護本公司之資訊資產(包括文件、資料、軟體、硬體、人員等）與服務，免於因外在之威脅，或內部人員不當之管理與使用，致遭受竄改、揭露、破壞或遺失等風險，以確保資訊資產之機密性、完整性、可用性保護之要求，並建立資訊安全管理體系與資訊安全管理準則，期有效及合理地降低本公司營運風險，持續強化同仁對資訊安全之認知，特訂定資訊安全政策（以下簡稱本政策)。

2、 適用範圍

本政策適用於本公司各單位之全體同仁、委外廠商、供應商、第三方人員以及所有相關資訊資產之安全管理。

3、 名詞定義

3.1 資訊安全(information security)

避免因人為疏失、蓄意或自然災害等風險，運用系統化之控制措施，包含政策、實施、稽核、組織和軟硬體功能等，以保護公司資訊資產的機密性、完整性、可用性之安全；此外，亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質；等同本公司所謂之資訊安全或資安。

3.2 資訊資產

凡本公司資產，如文件、資料、軟體、硬體、人員，等皆屬之。

3.3 機密性（confidentiality, C）

確保只有獲得授權的人員及程式才能存取資訊。

3.4 完整性（integrity, I）

確保資訊與處理方式精確性及完整性。

3.5 可用性 （availability, A）

確保獲得授權的使用者在需要時可使用相關資訊資產。

3.6 個人資料

係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性取向、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

4、 作業流程

4.1 為達成本公司之任務目標及最高管理階層對資訊安全之期許與要求，確保本公司資訊資產之安全，依照 ISO/IEC 27001：2022 標準之要求建立、記載、實施及維護資訊安全管理制度，並持續改進系統的有效性。資訊安全政策訂為:

4.1.1 確保本公司相關業務資訊之機密性安全，防止本公司機敏性資訊免於因內部或外部、蓄意或意外之各種威脅與破壞，致業務資訊遭受竄改、揭露、破壞、遺失或終止服務等風險。

4.1.2 確保本公司相關業務資訊之完整性與可用性，並正確執行本公司作業與各項業務，以保護本公司之資訊資產安全，確保本公司之設備及網路，不因各種威脅與破壞，而造成服務錯誤或中斷無法使用。

4.2 為達成上述資訊安全政策目的，將相關目標訂定如下：

4.2.1 確保相關資訊安全措施或規範符合資訊安全政策與現行法令之要求，每年至少進行一次資訊安全稽核。

4.2.2 每年至少進行一次營運持續計畫之測試及檢核。

4.2.3 確保資訊資產經風險評估後，受到適當之保護，防止未經授權或因作業疏忽對資產所造成之損害。

4.2.4 確保所有資訊安全事件或可疑之安全弱點，皆依適當通報程序反應，並予以適當調查及處理。

4.2.5 確保本公司資訊安全管理制度運作持續正常，並通過第三方驗證。

4.2.6 定期實施資訊安全教育訓練，並視情況實施不定期教育訓練。

4.3 本政策及目標應充分與各關注方溝通，溝通方式包括公開宣告於本公司網頁、紙本或電子檔案等型式。

4.4 基於此目標，本公司資通安全政策聲明為：

「落實資安防護要求確保資訊安全，建立安全可信賴之營運服務環境。」

4.5 資訊安全管理措施

資訊安全管理依照 ISO/IEC 27001：2022 標準涵蓋 4 大控制措施，避免因人為疏失、蓄意或天然災害等因素，導致資訊不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。管理措施如下：

4.5.1 組織控制措施

4.5.2 人員控制措施

4.5.3 實體控制措施

4.5.4 技術控制措施

4.6 運作機制

本公司依照 ISO/IEC 27001：2022 標準，採用"Plan-Do-Check-Act"（PDCA）之循環運作模式，建立與實施資訊安全管理系統，並維繫其有效運作與持續改進。

4.6.1 規劃與建立(Plan)：依據本公司整體策略與目標，藉由成立資訊安全管理組織，控制潛在之威脅及漏洞，規劃風險評鑑、設計與建置控管機制，以建立資訊安全管理系統。

4.6.2 實施與運作(Do)：依據評估規劃之結果，建立或修正應有之管控機制。

4.6.3 監督與稽核(Check)：監督資訊安全管理系統各項作業之落實執行，並評估及稽核其有效性。

4.6.4 維護與改進(Act)：根據監督稽核之結果與建議，執行矯正措施，改善並執行應有之控管機制，以持續維護資訊安全管理系統之運作。