東捷資訊服務股份有限公司

資訊安全管理系統

資訊安全政策

本公司已通過 ISMS ISO27001:2022 版認證，證書有效期為 2025 年 1 月 14 日至 2028 年 1 月 13 日止。

資訊安全政策

1. 目的

東捷資訊服務股份有限公司(以下簡稱本公司），為維護本公司業務之永續經營，強化資訊安全管理制度，確保資訊資產之機密性、完整性、可用性之要求，增進資訊處理設施與網路系統之可靠性以及同仁對資訊安全之認知，期以有效及合理地降低企業營運風險，特訂定本政策作為資訊安全管理之準則。

2. 目標

適用於本公司資訊安全管理制度相關文件、外來文件與紀錄之管控。維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

2.1. 執行客戶委託業務的營運持續計畫與演練，確保本公司資訊安全系統運作持續正常。

2.2. 建置資訊安全監控中心，確保電腦機房之網路及設備不因意外或錯誤造成無法使用。

2.3. 將安全性要求及個人資料蒐集與利用之相關資料納入所有的專案契約，確保重要資訊系統不因資訊安全事件造成機敏性資料外洩或終止服務。

3. 定義

3.1. 資訊安全：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，以確保公司資訊資產受到妥善保護。

3.2. 資訊資產：凡本公司資產，如人員、文件、電子文件、服務設施、軟體、硬體、媒體、建築保護設施等皆屬之。

4. 適用範圍

資訊安全管理涵蓋訊安全管理涵蓋本公司所提供之資訊委外服務、ERP 整合規劃服務、顧客關係管理服務、郵件資料整合服務、雲平台系統服務、業務行銷服務和與其相關之支援服務等營運作業相關之管理活動。為避免因人為疏失、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，對本公司帶來可能之風險與危害，本公司制定以下特定主題規範，據以實施、定期評估實施成效及持續改善：

4.1. 資安組織及管理審查程序

4.2. 文件與記錄管理

4.3. 資安目標與績效評量

4.4. 風險管理

4.5. 資訊安全內部稽核

4.6. 持續改善

4.7. 人力資源安全管理
4.8. 資產管理
4.9. 存取控制管理
4.10. 實體與環境安全管理
4.11. 運作安全與密碼學
4.12. 通訊安全管理
4.13. 系統獲取、開發與維護管理
4.14. 供應商管理
4.15. 資訊安全事故管理
4.16. 營運持續管理

5. 責任

5.1. 本公司的管理階層建立及審查此政策。
5.2. 資訊安全管理者透過適當的標準和程序以實施此政策。
5.3. 所有人員、委外服務廠商與訪客需依照相關安全管理程序以維護資訊安全政策。
5.4. 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
5.5. 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行懲處。

6. 審查

本政策應至少每年審查乙次，以反映資訊安全管理政策、法令、技術及業務等最新發展現況、以確保資訊安全實務作業確實遵守資訊安全政策，以及確保資訊安全實務作業之可行性及有效性。

7. 資訊安全政策之核准

7.1. 資訊安全政策配合資訊安全委員會之管理審查進行資訊安全政策審核。

7.2. 資訊安全政策經總經理核准後實施，修訂時亦同。