我樂活科技股份有限公司

資訊安全政策

機密等級：內部使用

文件編號：IS-001

版　　次：1.0

發行日期：113 年 12 月 16 日

修　訂　紀　錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	113 年 12 月 16 日		資訊安全小組	初版

目錄

文件編號	IS-001		保密區分	內部使用
版　　次	V1.0		發布日期	113/12/16

1. 目的

確保本公司所屬之資訊資產的機密性、完整性及可用性，並符合 ISO 27001 及相關法規的要求。透過有效的風險管理和控制措施，防範內部與外部的蓄意、意外威脅，保護資訊資產免受未經授權的存取、洩露、竄改或破壞，以保障公司營運的持續性和穩定性。

2. 範圍

2.1 本資訊安全政策的範圍涵蓋公司所有核心資訊系統、軟體開發專案、維運服務及機櫃設施，並包括相關利害關係者的需求及期望。

2.2 管理範圍以保護資訊資產的機密性、完整性及可用性為目標，確保資訊資產免於人為疏失、蓄意攻擊、天然災害或其他外部威脅的影響。

2.3 為有效應對可能的風險，應採用組織、人員、技術與實體層面的多層次控制措施。

2.4 管理範圍將根據公司業務需求與法律合規要求進行定期審查與調整，確保資訊安全管理制度的持續適用與改善。

2.5 資訊安全管理系統之管理事項如下：

2.5.1 資訊安全管理
2.5.2 資訊安全政策管理。
2.5.3 資訊安全組織管理。
2.5.4 人力資源安全管理。
2.5.5 資訊資產管理。
2.5.6 存取控制管理。
2.5.7 密碼管理。
2.5.8 實體與環境安全管理
2.5.9 作業安全管理。
2.5.10 通訊安全管理。
2.5.11 資訊系統獲取、開發及維護管理。
2.5.12 供應商關係管理。
2.5.13 資訊安全事件管理。
2.5.14 業務持續管理。
2.5.15 遵循性（適法性）管理。
2.5.16 資料安全管理。
2.5.17 變更與組態管理。
2.5.18 雲端服務管理。

3. 權責

3.1 資訊安全委員會

3.1.1 資訊安全委員會是本公司資訊安全管理的最高決策機構。

3.1.2 負責資訊安全管理制度的規劃、建立、實施、維護、監控、審查與持續改善。

3.1.3 委員會的成員應包含高階管理層和與資訊安全相關的關鍵人員，確保政策與策略的執行符合公司營運需求和法規要求。

3.2 公司同仁、資訊系統服務使用者、委外人員

3.2.1 配合資訊安全管理制度作業。

3.2.2 遵守相關資訊安全管理制度規範。

4. 定義

4.1 資訊安全

4.1.1 資訊安全是指保護資訊的機密性、完整性及可用性，防範未經授權的存取、洩露、竄改或破壞。

4.1.2 資訊安全包含鑑別性、可歸責性、不可否認性及可靠性，確保資訊資產的正確性與追溯性。

4.2 機密性

確保僅有獲得授權的人員能夠存取資訊，防止未經授權的洩露或公開。

4.3 完整性

保障資訊的正確性及完整性，防止資訊在傳輸、處理或儲存過程中遭到未經授權的修改或損毀。

4.4 可用性

確保資訊及相關資產能夠在需要時被合法存取與使用，避免因系統故障或其他干擾導致資訊無法被利用。

4.5 鑑別性

確保系統能夠正確鑑別使用者或設備，確認其合法身份，以防範未經授權的存取。

4.6 可歸責性

透過稽核與記錄，確保能夠追溯資訊操作的過程及行為，並能確認行為責任歸屬。

4.7 不可否認性

確保已進行的操作無法被合法地否認，並能提供相關證據支持操作的真實性。

4.8 可靠性

保障系統和資訊的穩定性及運行的可靠性，確保其能持續運作並提供預期的服務水準。

5. 作業內容

5.1 原則

5.1.1 依據相關法律法規、營運需求及風險評估結果，制定「資訊安全管理程序」作業標準並實施適當的資訊安全管理措施，以保障資訊資產的機密性、完整性與可用性。

5.1.2 所有資訊安全措施應經過風險評估，確保其與風險程度相符，並依據實際業務需求動態調整。

5.1.3 基於角色與職能建立權限管控機制，遵循最小權限原則，確保權責分明並定期審查，避免權限濫用。

5.1.4 所有員工應參加定期的資訊安全教育與訓練，提升安全意識並強化對相關政策的理解與遵循能力。

5.1.5 建立有效的資訊安全事件管理程序，確保事件發生時能迅速回應、妥善處理及降低影響，並透過定期演練測試業務持續計畫的有效性，確保在突發狀況下公司業務的連續性與穩定性。

5.1.6 遵循個人資料保護法及智慧財產權法之相關規定，妥善處理與保護個人資料與智慧財產，防止不當使用或洩露。

5.1.7 定期進行資訊安全稽核，檢查現行安全措施的有效性與合規性，並根據稽核結果持續改善。

5.2 瞭解組織及其全景

5.2.1 依營運目的，針對內部和外部的環境因素，全面鑑別會影響資訊安全管理系統（ISMS）的相關議題，包括法律法規、主管機關政策、技術趨勢、市場變化及利害關係者的需求與期望。

5.2.2 建立「組織全景鑑別表」，作為鑑別內外部議題的依據，該表得於遇到重大變更時進行即時修訂，確保資訊安全管理系統的範圍與防護措施能隨業務需求和風險情況進行調整。

5.2.3 持續監控技術發展和安全威脅趨勢，及時調整相關防護策略，以維持安全管理系統的有效性和防禦能力。

5.3 目標

5.3.1 根據具體業務需求及風險評估結果制定所有資訊安全目標，並與公司整體策略及合規要求保持一致。

5.3.2 致力於維護資訊的機密性、完整性及可用性，並遵循相關法規以保障個人資料隱私。

5.3.3 採取有效措施防止未經授權的存取、修改或洩露，確保業務資訊的正確性與完整性。

5.3.4 為確保資訊系統和服務的持續運作，應建立資訊業務持續性計畫，並定期進行演練與測試，確認其有效性。

5.3.5 每年應根據上述目標制定具體的量化衡量指標，並記錄於「目標管控及量測表」，定期檢視其執行情況，確保資訊安全目標能夠實際達成且持續改善。

5.4 審查

5.4.1 本資訊安全政策應至少每年檢討一次，以確保其符合最新的法律法規、主管機關政策、技術變革及組織業務需求。

5.4.2 審查應包括對現行資訊安全措施的有效性評估，並根據審查結果進行必要的修訂。

5.4.3 審查過程中應特別關注資訊安全風險評估的更新，確保風險管理策略能夠適應內外部環境變化。

5.4.4 若發生重大安全事件或組織結構變動，應即時進行額外的審查和修訂，確保政策的持續適用性。

5.4.5 本政策須以書面、電子或其他形式通知全體同仁、相關廠商及利害關係者，以確保其對最新資訊安全要求的知悉與遵循。

5.5 實施

本政策經資訊安全委員會核定後實施，修訂時亦同。

6. 附件：

6.1 IS-001-01 目標管控及量測表。