1. 目的

樂衍有限公司(以下稱本公司)為確保核心資訊系統資料、系統、設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或毀損等風險，並建立資訊安全管理體系，特訂定資訊安全政策(以下簡稱本政策)，本政策未規定事項依政府其他資訊安全法規精神辦理，以符合資訊系統之機密性、完整性、可用性與法律遵循性。

2. 依據

2.1 ISO/IEC 27001:2022 (Information Security, Cybersecurity And Privacy Protection — Information security management systems — Requirements)

2.2 ISO/IEC 27002:2022(Information Security, Cybersecurity And Privacy Protection — Information security controls)

3. 名詞解釋

3.1 機密性(Confidentiality) ：確保只有經過授權的人才能存取資訊資產。

3.2 完整性(Integrity) ：確保資訊資產的完整性(Completeness)及其處理方法的準確性。

3.3 可用性(Availability) ：確保授權的使用者在需要時，可以使用資訊資產。

3.4 資通系統(資訊系統)：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

3.5 資通服務(資訊服務)：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

3.6 資通安全(資訊安全)：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

3.7 資通安全事件(資訊安全事件)：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

4. 政策聲明

4.1 為確保核心資通系統安全及建立可信賴之環境，相關使用者需經過正常程

序之申請授權，方能閱讀與存取授權範圍內之管制資訊，期間並保障資訊於處理、傳輸、儲存之過程中皆能正確無誤之使用，及避免資訊與系統被無意或惡意之竄改或變更，並確保智慧財產權及個人資料都能得到妥適的保護，避免不當的使用。

4.2 對於個人資料之蒐集、處理及利用，將依個人資料保護法及相關法令之規定，僅就其特定目的（如承辦業務及所需提供之服務時）之用，不會恣意對其他第三者揭露。

4.3 以簡單且容易記憶並符合資訊安全管理為原則，訂定資訊安全政策聲明口號：機密資料保護好，資安管理不可少，持續服務為首要，養成習慣沒煩惱。

5. 目標

5.1 依據資訊安全管理標準 ISO/IEC 27001：2022 驗證之精神與要求，建置與累積導入資訊安全管理系統(Information Security Management System，ISMS)經驗與能力，作為本公司推廣資訊安全系統建置之基礎準則。

5.2 確保本公司核心資訊系統相關平台之資料的機密性(Confidentiality) 、完整性 (Integrity) 、可用性 (Availability)，以達正常持續運作之目標。

5.3 依據 PDCA 流程模式，以週而復始、循序漸進的精神，確保本公司核心資通業務運作之有效性及持續性，並訂立資訊安全目標量測機制，期能不斷精進。

6. 作業流程執行與要求

6.1 高層支持：
推動資訊安全管理，必須由高層主管支持與參與。

6.2 政策先行：
列出優先實施範圍，逐步推廣與落實。

6.3 全體共識：
充分了解資訊安全管理制度的重要性，建立使命感。

6.4 教育訓練：
適度資訊安全教育訓練，加強資訊安全管理觀念與技能。

6.5 定期稽核：
透過稽核程序，發現資訊安全問題，提出改善建議，降低資安風險

6.6 適時改善：發生資訊安全問題，即時研商對策，謀求改善機制，健全資訊安全管理制度。

6.7 電腦病毒及惡意程式之防範：

(1) 事前預防及保護措施，防制及偵測電腦病毒及惡意程式侵入

(2) 建立個人電腦使用規範及適當宣導，促使同仁正確認知電腦病毒及惡意程式的威脅並提升資訊安全警覺。

6.8 重要資訊備份：

(1) 正確及完整的重要備份資料，除存放在主要的作業場所外，應另外存放在不同的安全場所，以防止主要作業場所發生災害時可能帶來的傷害。

(2) 不定期測試並還原重要備份資料，以確保可用性與完整性。

(3) 重要資料的保存時間，以及檔案的保存需求，由資料擁有者研提及控管。

6.9 資訊交換：

(1) 資訊資料交換應有妥善安全措施，以防止資料遭破壞、誤用或未經授權存取。

(2) 確保傳送過程中之實體媒體安全，不受未經授權的存取、誤用或毀損。

6.10 營運資訊保護：

使用辦公室電子設備 (含影印機與傳真機)，應注意資訊安全； 產出機敏性文件時，應全程監看並於產出後妥善收存。

6.11 存取控制：

(1) 訂定系統存取授權規定，並告知使用者相關之權限及責任。

(2) 人員異動或職務調整時，應依系統存取授權規定，限期調整其權限。

(3) 強化使用者通行密碼管理並定期更新。

(4) 使用機敏性媒體應於離開座位時放置安全處所，避免未授權者取閱；電腦設施亦應設置螢幕保護機制並設定密碼保護，於離開操作後限定時間內啟動。

(5) 除申請核准之事由外，不得攜帶可攜式之儲存裝置或個人筆記型電腦進入資訊機房，避免機敏資料外流。

(6) 辦公桌面、伺服器及個人電腦螢幕應保持淨空，不置放機敏性文件。

6.12 電腦網路服務的使用：

(1) 被授權的電腦網路使用者，只能在授權範圍內存取電腦網路資源。

(2) 訂定電子郵件使用規定，機敏性資料不宜以電子郵件方式傳送。

6.13 行動通訊及遠距工作：

未經授權禁止於本公司資訊機房內使用行動式通訊設備及以遠端連線方式存取本公司之資訊資產。

7. 適用範圍

樂衍有限公司核心系統暨所屬單位。

8. 溝通或傳達

為使本公司之政策、需求及目標能有效地傳達到與業務相關之關注方，將利用媒體、函文、會議、網頁、電子郵件及文宣等途徑，進行彼此關注議題討論及溝通，於必要時得邀請相關人員參與，並留存紀錄做為後續之依據。

9. 實施與修正

9.1 本政策每年如有增修需經「資通安全管理審查會」審查且留下審查紀錄，並持續改進其有效性及適切性，以符法令法規、技術及本公司營運要求。

9.2 本政策如遇組織重大改變時應立即審查，以確保其適當性與有效性。必要時應告知與業務相關之關注方，以利共同遵守。

9.3 本政策奉資通安全長核定後實施，修正時亦同。