郁天科技有限公司

文件名稱：資訊安全政策	機密等級：一般
文件編號：ISMS-1-001	制定單位：資安推行委員會

版次	發佈日期	文件增修廢之內容摘要
1	2025/04/20	新制訂。
2	2025/04/20	調整資訊安全政策內容。
3	2025/06/23	1.調整資訊安全政策之適用範圍應擴及「GotIT EIP 智慧平台」與「供應鏈管理平台」。 2.使用表單更名為「資訊安全政策公告」(ISMS-4-047)。
4	2025/12/12	各項特定主題政策內容做適切性調整。

郁天科技有限公司

文件名稱：資訊安全政策	機密等級：一般
文件編號：ISMS-1-001	制定單位：資安推行委員會

1. 目的

為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之業務持續運作環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

2. 範圍

2.1. 適用於本公司資訊資產、系統及服務之安全管理作業，涵蓋機密性、完整性和可用性。

2.2. 適用於本公司全體員工、提供資訊服務廠商及第三方人員。

2.3. 適用範圍如下：

本公司資訊安全管理活動適用於『GotIT EIP 智慧平台』與『供應鏈管理平台』，以及個人資料安全保護，包括開發、維護流程及客戶服務之資料處理。

3. 定義

所謂資訊安全係將管理程序及安全防護技術應用於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體，以確保資訊蒐集、處理、傳送、儲存及流通之安全。

4. 本公司資訊安全政策

「落實資訊安全、永續客戶信任」

落實資訊安全管理，公司能確保自身與客戶的資料安全，降低資訊風險，強化競爭力，提升企業形象，並獲得客戶長期信任。本公司透過資訊安全管理來建立長期客戶信任：

4.1. 落實資訊安全：

4.1.1. 建立資訊安全制度，確保機密性、完整性與可用性。

4.1.2. 進行風險管理與控制，防止資料外洩與攻擊。

4.1.3. 提高員工安全意識，防範內外部威脅。

4.1.4. 持續監測與改進，確保安全機制有效性。

4.2. 永續客戶信任：

4.2.1. 保護客戶資料安全，避免未授權存取。

4.2.2. 維持系統穩定性，確保服務不中斷。

4.2.3. 遵循法規合規，提升企業可信度。

4.2.4. 加強透明溝通，建立長期信任關係。

4.2.5. 善盡稽核與通報義務，落實應變聯防機制。

5. 特定主題政策

5.1. 資訊安全全景鑑別及風險評鑑：

5.1.1. 確認組織面臨資訊安全相關內外部環境議題。

5.1.2. 確認與資訊安全相關之利害關係人及其需求與期望。

5.1.3. 確認與資訊安全相關資訊資產清冊。

5.1.4. 執行風險鑑別與評估作業。

5.1.5. 依風險評鑑結果，研擬風險回應因應方案及確認殘餘風險。

5.2. 資訊資產管理：

5.2.1. 識別組織之資產並定義適切之保護責任。

5.2.2. 確保所有資產依其對組織之重要性，受到適切等級的保護。

5.2.3. 防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。

5.2.4. 資訊分類分級及處理：

5.2.4.1. 資訊標示涵蓋所有格式的資訊及其他相關聯資產

5.2.4.2. 使人員及其他關注方認知標示要求。

5.2.4.3. 提供所有人員必要之認知方法，以確保正確標示資訊並進行相對應的處理 。

5.3. 資訊安全文件與記錄管理：

5.3.1. 使資訊安全管理系統所使用之文件與紀錄表單能迅速正確流通，以確保各相關單位能適時獲得適當且有效之最新文件與紀錄表單。

5.3.2. 文件之制訂、修訂、廢止、發行、回收、保存、查詢與列印作業之管理。

5.3.3. 每年執行文件適切性審查作業。

5.4. 系統開發與維護：

5.4.1. 將安全性考量整合到軟體開發的每個階段，從需求分析、設計、開發實作、測試，到部署與維護的流程。

5.4.2. 確保本公司自主研發系統、委外開發系統，在專案開發過程中所撰寫之原始碼，及維運中的資安系統，皆不含資安弱點、惡意程式碼或其他安全威脅風險，建立弱點與源碼安全掃描的作業流程與控管規範。

5.4.3. 在採購軟體時，視其安全需求，進行供應商及軟體評估、SBOM 文件與 OWASP 分析。

5.4.4. 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

5.4.5. 資訊系統應保護資料，防止洩漏或被竄改。

5.5. 網路安全：

5.5.1. 網路使用者經授權後，只能在授權範圍內存取網路資源。

5.5.2. 對使用網路系統的電腦連接線路，應適當加以控制，以減少未經授權之系統存取或電腦設

施的風險。

5.5.3. 設定網路區隔之規劃，應遵循內外網路實體區隔規定，並應禁止個人無線網路裝置破壞內外網路實體區隔之安全機制。

5.5.4. 非經授權嚴禁使用無線網路及私有有線設備與網路介接。

5.5.5. 遵循標準作業程序進行防火牆軟體和韌體的修補，並隨時了解已知弱點，確保系統的安全性。

5.5.6. 一經發現或接獲通報發生網路安全事件(如駭客入侵、病毒或木馬等感染)，應立即通報管理代表，辨識事件等級及採取緊急應變措施處理，並將辨識結果、應變與排除方法、注意事項，皆紀錄在「資訊安全事件報告單」。

5.6. 電子傳輸：

5.6.1. 確保資料傳送可追溯性及不可否認性。

5.6.2. 維持傳送作業之可靠性及可用性。

5.6.3. 實體傳送使用破壞存跡或抗破壞之控制措施。

5.6.4. 使用規定之電子傳輸媒體傳遞資料，不可因貪圖方便而任意使用非法與不當之傳輸媒體。

5.6.5. 不得利用任何傳輸媒介透過資料傳遞、訊息傳送、發言或視訊等方式透露機密或敏感性資訊給其他組織或人員。

5.6.6. 內部資訊網站須依權責及工作需求核發適當權限，以管制相關文件之存取。

5.7. 資料備份：

5.7.1. 依照資訊之機密性、可用性及完整性需求，制定核心資訊資產備份週期、方式及保存期限，並測試其有效性。

5.7.2. 遵循 3-2-1 備份原則來建立具備彈性與安全性的多重備份機制，降低資料遺失導致營運業務中斷風險，並符合 ISO27001 備援與資訊保護相關要求。

5.7.3. 依照備份資料之機密性需求加強防護，避免衍生之其他資安事件。

5.8. 實體安全：

5.8.1. 本公司一般區域及管制區域之組織資訊及資訊環境設施遭未經授權之實體存取、損害及干擾。

5.8.2. 防止資產之遺失、損害、遭竊或破解，並防止組織運作中斷。

5.8.3. 訪客/廠商進出管理。

5.8.4. 管制區域設置監視系統，並保留監視影像紀錄至少 60 天。

5.8.5. 重要資訊設備安置預備電源，並使用不斷電系統。

5.8.6. 網路通訊線路佈纜安全。

5.8.7. 移轉資產、資訊設備送修、報廢與銷毀之安全管理

5.8.8. 場所外資產(例如雲端服務、第三方資料中心或員工遠距工作所使用的裝置)，確保這些資產的機密性、完整性和可用性。

5.8.9. 設備於場所外發生遺失、遭竊、實體損毀，或遭受可疑網路攻擊時，資產保管人應即時通報並進行緊急應變措施。

5.9. 資訊安全法規鑑別：

5.9.1. 取得及辨識可施行於本公司資訊安全相關之法規並辨識與資訊安全有關的法規及法規變更及將法規有關的資訊傳達給相關人員。

5.9.2. 落實法規宣導，常態性辦理相關宣導課程及資安公告。

5.10. 營運持續：

5.10.1. 維護資訊系統關鍵業務無法持續運作時，執行必要之替代方案，並安全的回復，確保員工安全與關鍵性業務的持續運作，降低事故所造成的損失。

5.10.2. 定期測試與檢討現有之業務持續計畫，依測試結果修訂計畫內容，以維持有效性。

5.10.3. 審核業務持續計畫內容之適當性與演練測試結果。

5.11. 存取控制：

5.11.1. 本公司同仁註冊與權限申請、特權帳號、遠端連線權限及遠距工作管理。

5.11.2. 本公司同仁異動交接管理。

5.11.3. 第三方存取之安全控管。

5.11.4. 客戶資訊安全管理責任與義務：如最高存取權限自行控管、帳號權限清查義務、管理員權限應設置安全防護、端點安全責任應確保具備防毒與漏洞修補、提供安全遠端連線環境、維護自身內部網路的安全邊界、法規遵循與隱私保護義務、稽核與通報義務。

5.11.5. 存取控制規範與系統存取責任之制定，如使用者密碼原則、雲端存取權限之檢討評估。

5.11.6. 無人看管或暫不使用設備之安全管理。

5.11.7. 軟體安裝之限制，如確認軟體版本與更新、合法授權、及無安全問題後始得安裝。

5.12. 行動媒介管理：

5.12.1. 可攜式行動資訊設備(如：平板電腦、筆記型電腦、隨身碟、隨身硬碟、智慧型手機、電腦周邊設備)之使用安全控管。

5.12.2. 使用可攜式行動資訊設備之人員(含本公司同仁、訪客及廠商)之行為管理，例如未經本公司授權同意時，不得於本公司管制區域內行使資料傳輸、拍照、錄音及錄影等行為。

5.12.3. 設備借出登記與歸還審核機制，並嚴格檢視設備未被惡意竄改或植入木馬、軟體與資料被竄改、帳號權限審查等。

5.12.4. 設備於場所外發生遺失、遭竊、實體損毀，或遭受可疑網路攻擊時，資產保管人應即時通報並進行緊急應變措施。

5.13. 委外資訊服務：

5.13.1. 確保本公司所屬資訊資產及個人資料之委外服務作業品質與效率，並能符合內部作業流程安全之要求。

5.13.2. 供應商安全協議簽訂事宜。

5.13.3. 廠商及其服務人員名冊建檔事宜。

5.13.4. 管制承包廠商服務人員在維修服務時，應依「實體安全管理程序」執行相關管制措施。

5.13.5. 委外資訊安全事件管理。

5.13.6. 系統委外開發及維護、服務變更之相關規定。

5.13.7. 承包廠商監督與稽核

5.13.8. 雲端服務之資訊安全管理。

5.13.9. 罰則與追責。

5.13.10. 即時補救措施與應變責任。

5.14. 人力資源與訓練：

5.14.1. 建立人力管理原則，說明資訊安全相關工作人員於任用、工作、解職期間之安全規範與訓練，以確保具備專業能力並能持續滿足其工作要求。

5.14.2. 資訊委外廠商任用、聘雇期間、聘雇終止或變更期間之資訊安全管理。

5.14.3. 人員之內部或外部教育訓練計劃、施行、成效評核與追蹤等管理。

5.14.4. 人員成功溝通要素規劃，包含：溝通內容、對象、時機、方式、流程、通報管道。

5.14.5. 違反資訊安全規範罰則之擬訂。

5.15. 資訊安全績效：

5.15.1. 宣達資訊安全政策、目標及績效標準。

5.15.2. 定期確認資訊安全績效指標達成狀況與檢討。

5.16. 資訊安全稽核與矯正措施：

5.16.1. 驗證資訊安全管理系統是否有效實施，以適時發掘問題，並採取矯正措施，以維護各項資訊安全管理相關作業之有效運作。

5.16.2. 資訊安全稽核方式，應兼具內部稽核與外部稽核兩種方式執行。

5.16.3. 內部或外部稽核結果所發現之缺失，應開立不符合通知單及矯正措施處理單，持續處理與追蹤，直至缺失已確實矯正。

5.16.4. 所有稽核缺失與矯正處理記錄應彙整至「資訊安全稽核報告書」，呈主管審查並於管理

審查會議中提出報告和說明。

5.17. 資訊安全事故管理：

1.1.1. 驗證資訊安全管理系統是否有效實施，以適時發掘問題。

1.1.2. 根據稽核結果所發現之缺失，彙整稽核報告，並上呈主管單位查核。

1.1.3. 採取矯正與預防措施並持續追蹤，以維護各項資訊安全管理相關作業之有效運作。

1.1.4. 健全資訊安全事故通報體系。

5.18. 監控與防毒：

5.18.1. 防範各類惡意程式碼入侵資訊系統，避免造成系統軟體之破壞。

5.18.2. 完整監控所有資訊系統行為，並檢測未經授權之活動，以便於事故發生時提供證據，確保資訊安全。

5.18.3. 核心資訊資產之基本組態與安全組態設定、及技術脆弱性控制。

5.18.4. 內部及外部系統使用之監控管理，包括事件紀錄、鐘訊同步、帳號清查、登入登出、容量管理。

5.18.5. 委外廠商之監控及防毒作業要求及督導。

5.18.6. 處理與回應由關注方提供之資訊系統弱點掃描報告。

5.18.7. 防火牆、弱點掃描與威脅情資之監控。

5.19. 加密政策與金鑰管理：

5.19.1. 依照法規、客戶要求、個人資料及資訊資產風險鑑別來設置加密機制。

5.19.2. 管制金鑰產生、分派啟用、儲存、更新、廢止到封存和銷毀等作業。

5.19.3. 各項技術控制措施之實際應用(如: 選擇加密演算法、管理加密金鑰、郵件與檔案加密、傳輸加密、欄位加密、系統安全機制)，皆應予以記錄至「資安技術控制措施」文件內，以利持續追蹤與管理。

5.19.4. 文件與記錄之安全機制：結合資料存取分級，遵循最小權限原則，保護文件與記錄之存取安全。

5.19.5. 人員對加密相關的資訊系統操作，如金鑰的使用、加密/解密活動等皆應有留有存取日誌，以便後續的查詢與稽核。

5.19.6. 加強人員培訓，提升資安意識、蒐集資安威脅情資，且落實持續監控與稽核。

5.20. 安全系統開發生命週期管理：

5.20.1. 將安全性考量整合到軟體開發的每個階段，從需求分析、設計、開發實作、測試，到部署與維護的流程。

5.20.2. 適當性納入「加密政策與金鑰管理程序」之「技術控制」，將加密技術與金鑰控管機制整

合到軟體開發的每個階段。

5.20.3. 從源頭預防安全漏洞，提升軟體可靠性並降低後期修補成本。

5.21. 雲端服務安全管理：

5.21.1. 為確保公司本地端各類資訊資產，在發生設備損毀、惡意軟體入侵攻擊、軟體錯誤、人為操作不慎刪除資料或自然災害時，公司關鍵營運資料能不受波及，且可運用其備存資料來迅速回復本地端資安管理系統運作，遵循 3-2-1 備份原則，將具備彈性與安全性的雲端服務，建置異地備份機制，用以降低資料遺失所導致營運中斷風險，並符合 ISO27001 備援與資訊保護相關要求。

5.21.2. 具體擬定相關執行策略，包括從雲端服務選擇準則、服務協議(SLA)、雲端服務使用權限、雲端服務組態與容量管理、傳輸管理、退場管理、服務終止計畫、實地演練計畫、執行與監控。

2. 適用性聲明書

依據「ISO 27001 資訊安全管理系統」要求產出「適用性聲明書」，以書面方式列舉資訊資產是否適用其標準所列之控制措施，及其不適用之原因。當組織架構、人員、設備、實體環境等變動時，資訊安全管理委員應重新定義控制措施之適用性。

3. 實施

本政策經總經理核定後實施，修訂時亦同。

4. 使用表單

4.1. 文件關係矩陣圖（ISMS-4-046）。

4.2. 資訊安全政策公告（ISMS-4-047）。