資通安全政策

機密等級：一般

文件編號：ISMS-01-001

版次： 2.1.0

發行日期： 113 年 12 月 18 日

訂修廢紀錄

版次	發行日期	訂 修 廢 內 容 摘 要
1.0	108/01/03	建立第一版本資料
1.1	111/01/16	移除慧廣科技
1.2	111/02/16	修改驗證項目，組織架構
2.0.0	112/12/01	配合 ISO 27001:2022 更版 建立新版
2.1.0	113/12/18	配合 ISO 27701：2019 修改組織及部分文件名稱

1. 目的

本公司為為推動資通安全管理系統，建立企業應用服務及產品發展之持續運作環境安全及可信賴之資訊作業環境，確保資訊的機密性、完整性、可用性與隱私性，使其免於遭受內、外部的蓄意或意外之威脅，爰依「ISO/IEC 27001 資訊科技-安全技術-資訊安全管理系統-要求」及相關法令法規，衡酌本公司之業務需求系統、設備及網路安全，訂定資通安全政策。

2. 適用範圍

2.1. 本公司之員工。

2.2. 資通安全管理之範疇：

2.2.1.組織控制

2.2.2.人員控制

2.2.3.實體控制

2.2.4.技術控制

3. 權責

3.1. 由資安長或其授權人核定、發布本程序。

3.2. 資通安全暨個人資料管理小組審查本程序，並督導本程序之執行。

3.3. 資通安全暨個人資料管理小組研擬、評估及檢討本程序。

4. 名詞定義

4.1. 資通資產

係指為維持本公司相關業務流程運作之文件與紀錄、電腦系統、人員、服務、實體設備。

4.2. 合宜性

管理系統如何適合組織之運作。

4.3. 適切性

管理系統是否符合 ISO 27001 的要求，並進行適當之實施。

4.4. 有效性

管理系統是否達到所預期之結果。

4.5. 資通安全

保護資訊的機密性、完整性、可用性與隱私性。

4.6. 資通安全政策

本公司資通安全管理政策為：保護資通資產之機密性、完整性、可用性及隱私性，進而提供安全、穩定及高效率之整體資訊服務。

4.7. 資安政策聲明

資安做得好，服務沒煩惱。

4.8. 資通安全管理系統(Information Security Management System)

為組織整體營運管理系統的一部份，以營運風險為導向，用來建立、執行、操作、監控、審查、維護與改進資通安全。

4.9. 風險分析

系統化的式使用資訊，進而辨識風險的來源，並加以估計。

4.10.風險評估

把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。

4.11.風險評鑑

風險分析與評估的整個過程。

4.12.風險管理

藉由協調各項活動以指導與控管組織之有關風險。

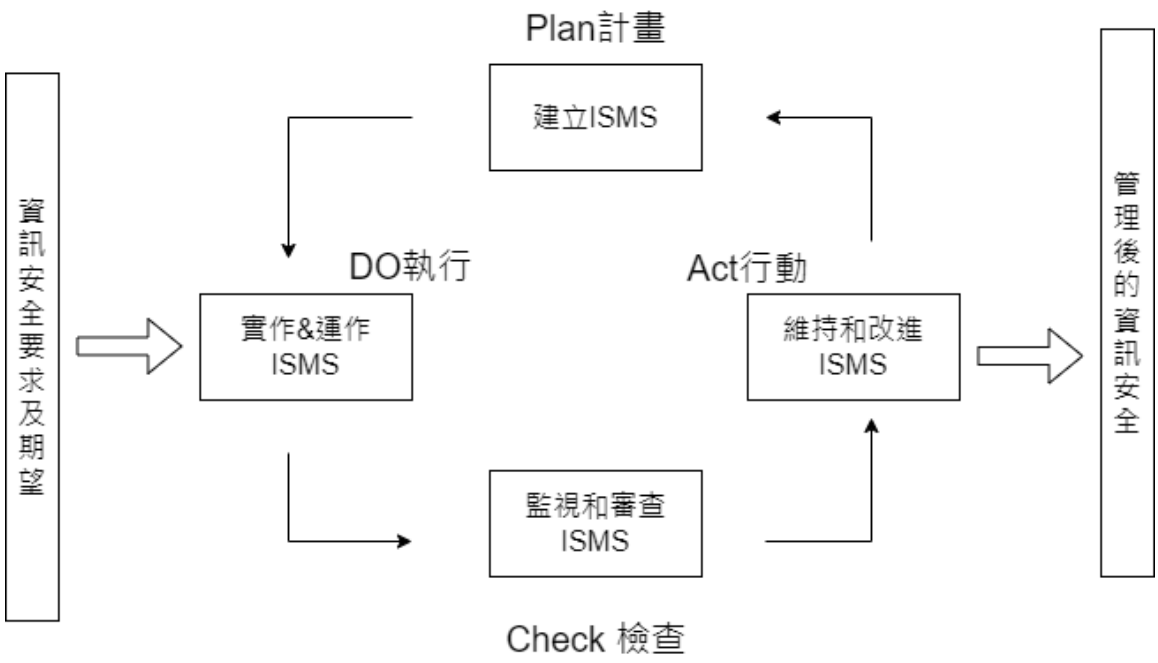
4.13.風險處理

選擇與實作措施的過程藉以矯正風險。

5. 作業內容

5.1. 資通安全管理系統持續改善之 PDCA 模型

依據 ISO 27001 標準要求事項第 4 節至第 10 節要求事項，來進行管理系統之建立、實作、運作、監視、審查、維持與持續改進資通安全管理系統。



5.2. 資通安全暨個人資料管理組織

5.2.1. 為統籌資通安全相關業務之整體規劃、評估、督導、協調、推動及資安事件處理等事項，特設置「資通安全暨個人資料管理委員會」，並於「資通安全暨個人資料管理委員會」下設立「資通安全暨個人資料管理小組」、「資通安全暨個人資料稽核小組」與「資通安全暨個人資料緊急應變小組」。

5.2.2. 依「組織全景與溝通管理程序書」，採用會議型式考慮內、外部議題、關注方期望，進行風險識別與全景評鑑以及資通安全管理系統適用範圍的決定。

5.3. 資通安全管理系統文件管理

5.3.1. 資通安全管理系統文件係為管制資通安全各項管理性及支援性作業而建立之必要程序，詳見「文件暨紀錄管理程序書」。

5.4. 內部稽核

5.4.1. 資通安全管理系統稽核分組應規劃內部稽核作業，將稽核範圍、準則、項目、方法及前次稽核的結果納入考量，每年至少辦理一次內部稽核，以判定資通安全管理系統控制目標、控制措施、過程及程序是否符合下列要求：

5.4.1.1.符合 ISO 27001 條文要求事項。

5.4.1.2.相關外部、內部法規及程序規範。

5.4.1.3.符合已知的資通安全要求。

5.4.1.4.選用之控制措施確實執行與維護。

5.4.1.5.依照預定時程落實執行。

5.4.2. 在稽核時所發現不符合項目，須填寫【矯正與預防作業單】，受稽核單位應進行改善措施並如期完成，資通安全稽核小組應持續追蹤控管改善措施之落實。詳見「矯正預防及持續改善管理程序書」。

5.5. 資通安全管理系統之持續改善

資通安全管理系統之持續改善，應於日常作業中不斷累積，並依據以下各程序所規範之關鍵時點予以檢討，以維持之合宜性、適切性及有效性。

5.5.1. 依「監督與量測控制程序書」，審查監控及量測結果，判定控制措施之有效性。

5.5.2. 依「矯正預防及持續改善管理程序書」針對資通安全管理系統所產生的異常狀況或潛在問題，採取適當處理及研擬改善措施。

5.5.3. 依內部稽核結果，評估資通安全管理系統之管理控制，確保資通安全管理系統政策與目標的適宜性。

5.5.4. 依「營運持續運作管理程序書」確保資訊業務能因應重大資通安全事故，採取適當應變措施。

5.5.5. 依「資通安全暨個人資料管理組織程序書」實施管理審查，以確保資通安全管理系統之政策與目標的適宜性和有效性。

5.5.6. 依【資通安全法令及法規現況總覽表】識別法規之適用性，以避免違反任何法律、行政命令、契約、標準、安全技術等規範。

5.5.7. 實施資通安全管理系統所選用之各項控制措施及其所對應之程序文件詳見 「資通安全適用性聲明書」。

5.6. 委外管理作業

本公司在進行委外活動時，根據「委外管理程序書」，簽署【委外廠商保密切結書】，確保委外廠商及其相關人員均遵循公司資通安全要求，

並通過契約管理、定期審查及安全監控等措施，以降低委外活動可能帶來的風險。

6. 作業說明

6.1. 資通安全管理系統之建立作業說明

6.1.1. 建立資通安全管理系統(Plan 規劃)

6.1.1.1.建立資通安全管理系統之政策、目標、標的、流程及相關程序，以管理風險及改進資通安全，使結果與組織整體政策及組織目標一致。

6.1.1.2.建立資通安全管理系統，含風險評鑑、風險識別、風險分析與評估、風險處理、剩餘風險的核准、管理階層之授權、適用性聲明等。

6.1.2. 實作與運作資通安全管理系統(Do 執行)

資通安全管理系統之政策、控制措施、流程與程序之實施與操作。

6.1.2.1.依「資通資產管理程序書」，識別資通安全管理系統實施範圍內相關資通資產。

6.1.2.2.依「風險評鑑與管理程序書」，釐清資通資產所可能面臨的風險，選取適當的方法進行風險管理，以期將風險降低到可承受之程度。

6.1.2.3.依「人員安全與教育訓練程序書」，使全體工作人員提升資通安全意識及認知，了解本公司資通安全相關規定及違反規定之風險與責任。

6.1.3. 監視和審查資通安全管理系統(Check 檢查)

6.1.3.1.依據資通安全管理系統之政策、目標與實際經驗，以評鑑及測量（適當時）流程績效，並將結果回報給管理階層加以審查。

6.1.3.2.監視與審查資通安全管理系統資安目標量測控制措施的有效性、審查風險評鑑及剩餘風險的等級與已識別的可接受風險、維持與改進資通安全管理系統。

6.1.3.3.資通安全管理系統於執行上之問題，其所對應之各項矯正措施處理，詳見「資通安全稽核作業程序書」。

6.1.4. 維持和改善資通安全管理系統(Act 行動)

6.1.4.1. 依據內部稽核、管理階層審查結果或其他資訊，採取矯正與預防措施，以達成持續改進資通安全管理系統之目的。

6.1.4.2.資通安全管理系統於執行上之問題，其所對應之各項矯正措施處理。詳見「矯正預防及持續改善管理程序書」。

6.1.4.3.確保資安事件與弱點，能夠及時通報與處理，詳見「資通安全事件管理程序書」。

6.1.4.4.為防範核心業務資訊，不遭受未授權的存取、破壞及干擾，人員帳號密碼也不得揭露於辦公室明顯處，電腦也應啟動螢幕保護程式以密碼保護，詳見「實體安全管理程序書」。

6.1.4.5.為確保網路服務及正確與安全地操作資訊處理設施，應建立安全防護措施及管理機制，詳見「網路與通訊安全管理程序書」。

6.1.4.6.資訊系統應訂定定期備份原則，並做復原測試。詳見【備份作業目錄明細】與「備份資料正確性檢測作業」。

6.1.4.7.為避免資訊因為授權之存取而使機密性或限閱性資料遭不當使用，應考量人員職務授予適切權限，詳見「帳號與存取控制管理程序書」。

6.1.4.8.營運持續的需求須做完整規劃，以支援相關資訊系統。詳見「營運持續運作管理程序書」。

6.1.4.9.依「資通安全組織管理程序書」實施管理審查,以確保政策和目標的適宜性和有效性。

7. 使用表單

ISMS-04-014 【矯正與預防作業單】

ISMS-04-028【備份作業目錄明細】

ISMS-04-033 【委外廠商保密切結書】

8. 相關文件

8.1. 國際標準資通安全管理系統(ISO/IEC 27001：2022)。

8.2. 國際標準資通安全管理系統實務指導規範(ISO/IEC 27002：2022)

8.3. ISMS-01-002 資通安全管理適用性聲明書。

8.4. ISMS-02-001 組織全景與溝通管理程序書。

8.5. ISMS-02-002 資通安全暨個人資料管理組織程序書。

8.6. ISMS-02-003 文件暨紀錄管理程序書。

8.7. ISMS-02-004 資通資產管理程序書。

8.8. ISMS-02-005 風險評鑑與管理程序書。

8.9. ISMS-02-006 資通安全稽核作業程序書。

8.10.ISMS-02-007 矯正預防及持續改善管理程序書。

8.11.ISMS-02-008 監督與量測控制程序書。

8.12.ISMS-02-009 人員安全與教育訓練程序書。

8.13.ISMS-02-010 實體安全管理程序書。

8.14.ISMS-02-011 網路與通訊安全管理程序書。

8.15.ISMS-02-012 帳號與存取控制管理程序書。

8.16.ISMS-02-013 資通安全事件管理程序書。

8.17.ISMS-02-014 委外管理程序書。

8.18.ISMS-02-015 營運持續運作管理程序書。

8.19.ISMS-02-016 醫療影像儲傳系統(PACS)作業管理程序書。

8.20.ISMS-02-017 電子病歷系統(EMR)開發與維護程序書。

8.21.ISMS-02-018 資通安全情資管理程序書。

8.22.ISMS-02-019 雲端服務資訊安全管理程序書。

8.23.ISMS-02-020 組態管理程序書。

8.24.ISMS-03-001 資通安全暨個人資料管理內部稽核作業規範。

8.25.ISMS-03-002 人員資訊安全守則。

8.26.ISMS-03-003 主機房管理作業規範。

8.27.ISMS-03-004 備份資料正確性檢測流程。