農業部
農業藥物試驗所
資通安全管理政策

文件等級：■一般 □內部 □限閱

編　　號：ACRI-ISMS-1-01

版　　本：V1.1

發行日期：112 年 09 月 01 日

文件制/修訂紀錄表

文件版本	發行日期	修訂內容	修訂單位	修訂人
V1.0	109/10/12	初版	技術服務組	游適彰
V1.1	112/09/01	組改名稱修正	技術服務組	游適彰

目　錄

1. 目的

農業部農業藥物試驗所(以下簡稱本所)為貫徹資通安全管理法執行資訊安全管理系統(Information Security Management System，ISMS)並確保其運作有效性及持續監督管理，以維護資通系統之機密性、完整性、可用性與法律遵循性，特訂定資通安全管理政策，作為資通安全工作之指導方針，藉以降低營運風險。

2. 適用範圍

本所各組室及往來委外廠商均應遵守資通安全管理政策。

3. 名詞定義

3.1. 機密性

使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

3.2. 完整性

保護資產之準確度和完全性的性質。

3.3. 可用性

在獲授權個體要求時，可取得及使用之性質。

3.4. 法律遵循性

符合法律、法規之要求。

4. 作業內容

4.1. 資通安全政策

為使本所業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，特制訂本政策如下，以供全體同仁共同遵循：

4.1.1. 建立本所資通安全保護及管理機制，確保核心資通系統服務營運持續可用性。

4.2.1. 針對資安事件之處理、通報與復原能快速完成。

4.3.1. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本所同仁之資通安全意識，本所同仁亦應確實參與訓練。

4.2. 作業流程執行與要求

4.2.1. 組織設置

設置資通安全推動小組，負責本所資通安全與個人資料保護管理之建立及推動。

4.2.2. 安全教育

定期實施資通安全教育訓練，宣導資通安全管理政策及實施規定。

4.2.3. 規劃資源

建立資訊資產管理機制，統籌分配並有效應用資源，解決安全問題。

4.2.4. 事先防範

新資通系統或服務建置或推出前，應納入資通安全因素，以防範危害安全情況之發生。

4.2.5. 安全監控

建立資通安全監控與防護措施，並定期進行檢視。

4.2.6. 授權管理

明確規範資通系統、網路服務、敏感資訊之使用權限，防止未經授權存取之行為。

4.2.7. 檢討改善

訂定及執行內外部稽核活動，以落實資通安全管理制度，並針對未盡事項執行改善。

4.2.8. 業務持續

訂定資通安全之營運持續計畫並實際演練，確保突發事故發生時得以應變。

4.2.9. 資安文化

所有人員皆負有資通安全之責任，且應了解及遵守相關之資通安全規定，並於工作職責中落實。

4.2.10. 領導承諾

本所管理階層應積極參與資通安全管理活動，並提供推展資通安全管理系統所需之支持及承諾。

4.3. 資通安全責任

4.3.1. 本所管理階層負責建立及審查資通安全管理政策。

4.3.2. 資通安全管理者應透過適當的標準和程序推動資通安全管理政策。

4.3.3. 所有人員皆應遵守相關安全管理程序以維護資通安全管理政策。

4.3.4. 所有人員均有責任通報資通安全事件和任何已鑑別出的弱點。

4.3.5. 任何蓄意違反資通安全的行為將受到相關規範或法律行動。

4.4. 溝通或傳達

為使本所之政策、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。

4.5. 政策修訂

4.5.1. 本政策每年應配合資通安全推行小組會議至少評估檢討一次，以反映本所資通安全需求、政府法令法規、外在網路環境變化及資通安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。

4.5.2. 本政策如遇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。

5. 參考文件

5.1. ISO/IEC 27001：2013(Information technology — Security techniques — Information security management systems — Requirements)

5.2. ISO/IEC 27002：2013(Information technology — Security techniques — Code of practice for information security management)。

5.3. 資通安全管理法及相關子法

6. 輸出文件/紀錄

無