南臺科技大學

資通安全管理制度指導綱要

機密等級：一般

文件編號：STUST-ISMS-A-01

版　　次：1.0

發行日期：113 年 6 月 28 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 6 月 28 日		呂宜庭	初版

目錄

資通安全管理制度指導綱要					
文件編號	STUST-ISMS-A-01	機密等級	一般	版次	1.0

1 目的

南臺科技大學（以下簡稱本校）為確保所屬教職員工了解本校資通安全管理制度相關程序及規範，並符合相關法規之要求，依據南臺科技大學「資通安全暨個人資料保護管理政策」，特訂定本指導綱要做為參考指引。

2 適用範圍

本校資通安全管理相關作業。

3 權責

本校教職員工應依據組織所賦予之權責，執行本指導綱要之相關資通安全管理規範，委外服務廠商與訪客等皆應遵守本指導綱要。

4 名詞定義

4.1 資訊安全管理系統驗證標準

計有 ISO 27001、CNS 27001、BS 10012 及教育體系資通安全暨個人資料管理規範等，採行標準為 ISO 27001 及 CNS 27001。

5 作業說明

5.1 資通安全管理制度

5.1.1 本校資通安全管理制度依據資訊安全管理系統驗證標準，依過程導向以建立、實施、操作、監督、審查、持續改善的管理循環，以期建立完善的資通安全管理架構，達成資通安全管理之目的。導入步驟如下：

5.1.1.1 定義資通安全管理制度之範圍。

5.1.1.2 制訂資通安全管理制度之政策。

5.1.1.3 成立資通安全管理制度之組織。

5.1.1.4 定義系統化之風險評鑑方法。

依據本校資通安全管理制度施行範圍，討論並制訂出一符合本校資通安全管理、政府法律法規及資訊安全管理

系統驗證標準要求之風險評鑑方法。

5.1.1.5 鑑別及評鑑各項風險

風險評鑑的執行過程，包括資通系統資訊資產的清查，確認資產之擁有者、風險之擁有者，並經由資訊資產之機密性、完整性及可用性來識別資產價值。藉由鑑別資訊資產風險之機率與衝擊，評估風險發生時所造成的影響。

5.1.1.6 訂定可接受風險值

透過本委員會討論，訂定可接受風險值，作為風險管理之依據。

5.1.1.7 擬訂風險改善計畫

經執行風險評鑑作業後，為確保風險降低至可接受風險值，將高於可接受風險值之資產，由各單位制訂「風險改善計畫表」，作為風險控管之依據。

5.1.1.8 溝通或傳達

與資通安全管理相關之內部及外部議題，必須進行溝通或有傳達的需要時，其溝通或傳達至少包括下列事項：

(1) 溝通或傳達事項。

(2) 溝通或傳達時間。

(3) 溝通或傳達對象。

(4) 溝通或傳達人員。

(5) 進行有效溝通或傳達所採用過程。

5.1.1.9 訂定適用性聲明

應參考 ISO 27001 及 CNS 27001，選擇適當之控制措施，由本委員會相關工作小組制訂「適用性聲明書」條列本

校所採用之控制及驗證範圍。

5.1.1.10 執行資通安全內部稽核

本委員會相關工作小組規劃資通安全稽核作業的執行方式，以評估資通安全管理制度是否有效落實，以使資通安全管理制度能達到持續改善之目的。

5.1.1.11 管理審查作業

本委員會應定期審查資通安全管理制度實施成效，並針對範圍、政策、組織、風險評鑑方法等適用性進行審查；以及資通安全內部稽核的結果、資通安全管理的維護改善等進行審查。

5.1.1.12 持續改善

本委員會應經由資通安全政策、安全目標、稽核結果、事件監控之分析、矯正措施以及管理階層審查之使用，持續改進資通安全管理制度之有效性。

5.2 資通安全文件暨紀錄管理

5.2.1 資通安全管理文件架構

5.2.1.1 一階文件（政策、指導綱要）：本校資通安全最高指導文件。

5.2.1.2 二階文件（程序書）：各項作業之管理原則與程序。

5.2.1.3 三階文件（作業說明書）：各項作業之標準作業程序。

5.2.1.4 四階文件（表單、紀錄）：資通安全管理制度執行紀錄。

5.2.2 ISO 27001 及 CNS 27001 控制項目與參考文件之對照，請參閱「適用性聲明書」。

5.2.3 資通安全文件與紀錄相關管理規定，請參閱「文件管理程序書」。

5.3 安全政策

為加強電腦使用安全、維護資料機密及作業管制，以達到資訊之機密性、完整性與可用性，確保資料安全與正確性，進而提升作業效率，本校應制訂資通安全政策。

5.4 資通安全的組織

5.4.1 本委員會相關人員之工作執掌、運作方式，應明確劃分。

5.4.2 資通安全相關工作人員之任用資格，以及本校所屬教職員工資通安全相關教育訓練規劃應符合主管機關要求，由本委員會相關工作小組督促進行或另訂規範。

5.5 資產管理

訂定相關處理規範或包含項目如下。

5.5.1 本校資通系統資訊資產應由本委員會相關工作小組建立資通系統資訊資產清單並識別其擁有者、使用者及保管者，並予以適當分類及標示。

5.5.2 各類資訊資產名詞定義、分級與處理、資訊資產清單之維護等。

5.5.3 資訊設備之新增、異動、報廢、汰換、攜出入機房、故障叫修及定期保養等管理程序。

5.6 人力資源安全

訂定相關處理規範或包含項目如下。

5.6.1 人員於聘任前、任職期間，為確保工作人員、承包商及第三方使用者了解其職責、且有能力在日常工作中支持組織安全政策，於職務異動或離職時，各單位應有變更之程序。

5.6.2 人員於報到進用、調動或離職時，有關之權責與安全事項說明，保密切結、違規查處及懲戒等，各單位應加以明確律訂。

5.6.3 教職員工須參與資通安全教育訓練，每年訓練時數應符合資通安全責任等級 C 級之特定非公務機關應辦事項之規定。

5.6.4 各單位對資通作業委外合約、委外服務人員管理等應訂有安全需求及規定。

5.7 實體與環境安全

訂定相關處理規範或包含項目如下。

5.7.1 電腦機房人員、設備進出管制，辦公區域環境安全管理等。

5.7.2 機房設備安全維護，資產移轉、送修管理等。

5.8 通訊與作業管理

訂定相關處理規範或包含項目如下。

5.8.1 網路設備之架構設計、管理與維護等。

5.8.2 電腦病毒碼更新機制、電腦病毒掃描機制、中毒通報與處理等。

5.8.3 帳號申請作業、網段區隔與安全管理、網路流量異常管理等。

5.8.4 防火牆系統之一般規範及作業規範等相關控制措施。

5.8.5 電子郵件系統帳號申請、維護作業、使用規範等。

5.8.6 設備資源規劃與評估、設備新增之安裝及設定、上線前測試、驗收作業、帳號與權限申請、操作與變更管理、維護作業、資源管理、監控程序、技術安全稽核等。

5.8.7 資料備份架構規劃、資料備份政策及時程規劃、備份管理作業等。

5.8.8 設備、系統的變更管理等。

5.9 存取控制

訂定相關處理規範或包含項目如下。

5.9.1 資訊之存取型態、職務權責區分、工作所需最小權限、帳號存取權限註冊與註銷、使用者權限管制、密碼管理原則、網路存取之安全控制、電腦系統之存取控制、應用系統之存取控制、存取事件紀錄、存取控管作業查核、外部存取等。

5.9.2 設備新增之安裝及設定、帳號與權限申請、操作與變更管理等。

5.9.3 外部單位與本校資料交換。

5.9.4 資料庫管理共通性規範等。

5.10 資通系統獲取、開發與維護

訂定相關處理規範或包含項目如下。

5.10.1 新資通系統之設計應視需要將必要之安全需求納入考量，並符合資料輸入／輸出之確認、系統內部處理及系統與系統間資料驗證機制，以及確保系統訊息完整性之相關控制措施。

5.10.2 資通系統開發生命週期（SDLC）管理、確保系統之正確處理、存取控制、檔案及資料之保護、系統執行與維護管理等。

5.10.3 程式庫設置與存取處理流程、程式版本管理等。

5.10.4 資通系統上線及變更管理等作業。

5.11 資通安全事故管理

訂定相關處理規範或包含項目如資通安全事件日常監控，制訂災害復原作業程序，事件之通報、辨識、抑制、排除、復原、檢討及學習、檢查測試演練等。

5.12 營運持續管理

訂定相關處理規範或包含項目如災害之預先防制、業務永續運作計畫之啟動、過程及結束之規範，定期演練及維護業務永續運作計畫等。

5.13 遵循性

訂定相關處理規範或包含項目如資通安全稽核頻率、稽核類別、擔任資通安全內部稽核人員資格，以及資通安全矯正與預防措施等。

6 相關文件

6.1 文件管理程序書。

6.2 風險改善計畫表。

6.3 適用性聲明書。