國立臺南藝術大學

資訊安全組織全景管理規範

機密等級：一般

文件編號：IS-A-001

版　　次　：3.2

發行日期：111.08.02

資訊安全組織全景管理規範					
文件編號	IS-A-001	機密等級	一般	版本	3.2

修訂紀錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
3.0	109/9/25	新增	詹怡珊	依「教育體系資通安全暨個人資料管理規範」、ISO 27001：2013版制定
3.1	110/11/19	修訂	詹怡珊	依「資通安全責任等級分級辦法」本校C級公務機關，所有核心資通系統完成ISMS導入
3.2	111/08/02	目錄、5、6	詹怡珊	修訂資訊系統名稱

目　錄

壹、目的

國立臺南藝術大學（以下稱本校）為推動資訊安全管理系統，藉由全面性了解組織全景及與本校往來之關注方對資訊安全期望與要求，訂定評估方法，以界定本校資訊安全管理的方針與實施範圍，爰訂定「資訊安全組織全景管理」（以下簡稱本規範）。

貳、參考依據

一、 教育體系資通安全暨個人資料管理規範：2019 年版

二、 ISO/IEC 27001：2013

三、 資通安全責任等級分級辦法

參、適用範圍

本校涉及資安議題之營運與服務業務範圍，均適用之。

肆、名詞定義

一、 管理階層：指本校具決策職權之主管。

二、 關注方(interested parties)：與本校資訊安全管理有利害關係之團體或個人，包含：

(一)內部關注方：指本校教職員生。

(二)外部關注方：上級機關、廠商、往來之機關團體、資安相關法令法規、合約。

三、 核心資通系統：支持本校核心業務持續運作必要之系統。

伍、權責

一、 管理階層

(一)審核「資訊安全組織全景管理規範」及「組織全景表」。

(二)擔任組織與聲譽之風險擁有者。

(三)核定組織與聲譽之風險接受程度及因應對策。

二、 資安處理組

(一)鑑別本校之營運作業與目標。

(二)鑑別內、外部關注方之期望與要求及資訊安全管理系統驗證範圍。

(三)鑑別組織與聲譽風險發生時，潛在的衝擊影響及因應對策。

(四)定期檢視修訂本校組織全景。

三、 各單位

(一)鑑別單位內涉及資訊安全議題之營運作業與服務。

(二)鑑別內、外部關注方之期望與要求。

(三)執行單位資通系統分級。

(四)鑑別單位之組織與聲譽風險。

(五)單位風險因應對策之討論，並執行風險改善作業。

(六)提供上述資料予資安處理組彙整。

陸、作業說明

一、 鑑別組織之營運作業、內部與外部議題及關注方之期望與要求

(一)資安處理組在鑑別組織全景時，首先應取得管理階層對本校主要營運作業與服務（核心營運業務與服務）資訊安全的願景與承諾。

(二)各單位依「組織全景表」鑑別單位內涉及資訊安全議題之營運作業與服務、資訊安全相關法令規，及內、外部關注方之期望與要求，提供資安處理組彙整評估，由資安處理組建立「組織全景表」，陳資通安全長核定。

(三)與資訊安全相關之內部與外部議題來源：

1. 外部議題

(1) 上級機關發布之資訊安全相關命令或規定。

(2) 與資訊安全相關之法律或合約、協議要求。

2. 內部議題

(1) 校務會議、行政會議、資訊安全執行小組會議、其他業務會報等高階主管會議。

(2) 資訊安全管理審查會議。

以上內、外部議題，經決議之相關資訊安全事項，由各單位規劃執

行；並於召開資訊安全管理審查會議時由資安處理組彙整提出檢討，並適時調整「組織全景表」。

二、 鑑別 ISMS 實施範圍

(一)資通系統分級作業

三、 各單位應依行政院「資通安全責任等級分級辦法」規定，填寫「安全等級評估表」送交資安處理組彙整製作「資通系統清冊」，經簽核程序由資通安全長核定安全等級後，由資安處理組依系統分級結果，評定核心資通系統填入「組織全景表」。

(一)ISMS 實施範圍評估

1. 資安處理組依「組織全景表」之核心資通系統並參考內、外部關注方之期望與要求，建議 ISMS 施作/驗證範圍。

2. 評估原則：於發生資安事件時將會嚴重影響本校主要營運作業與服務項目之關資通系統(以安全等級列優先順序) ，在本校經費及人力許可範圍內，或上級、法律、合約要求必須納入之相關核心資通系統及其相關支援性設施及場域(如網路設施、機房、人員)均應 納入 ISMS 施作/驗證範圍。

四、 依「資通安全責任等級分級辦法」本校屬 C 級公務機關，所有核心資通系統完成 ISMS 導入。

(一)資訊安全政策與資訊安全目標制訂

1. 資安處理組依「組織全景表」及 ISMS 實施範圍制修訂本校資訊安全管理政策與資訊安全目標。

2. 資訊安全目標制定要求

(1) 由資安處理組依「組織全景表」及「資訊安全管理政策」要求，制定本校「ISMS 有效性量測表」，內容應包含：量測項目、目標水準、量測週期、負責人、量測方法、資源需求、量測結果等項目。

(2) 量測方法應以可量化為原則。

(3) 應考量風險評鑑與風險處理結果，尤其高風險項目應納入追蹤量測項目。

(4) 每年納入管理審查會議檢討，包含達成成效及內容之適切性。

(5) 每年制修訂後，應向相關人員說明或佈達。

(二)組織全景之風險評估及風險改善

資安處理組針對「組織全景表」所鑑別出的資訊安全期望與要求，應評估考量納入組織與聲譽資產實施風險評鑑，評鑑方法請參照「風險評鑑管理程序」評估相關脆弱點與威脅及可能對組織與聲譽造成的衝擊程度影響，鑑別出風險等級，如超出可接受風險值，由資安處理組擬訂因應對策(風險改善計畫)，並於完成風險改善後重新評估風險值，再陳資通安全長核定是否對殘餘風險接受。

柒、維護與審查

「組織全景表」每年應至少審查 1 次，並於營運流程改變、組織結構變更、內部與外部議題或關注方期望變更時，應修訂之，並同步檢討「適用性聲明書」、「資訊安全管理政策」及「ISMS 目標有效性量測表」。

捌、實施

一、 本規範經資通安全長核定後實施，修訂時亦同。

玖、輸出表單／紀錄

一、 IS-D-001 組織全景表

二、 IS-D-002 安全等級評估表

三、 IS-D-003 資通系統清冊

四、 IS-D-004ISMS 有效性量測表