管理系統文件

文 件 類 別	第 二 階 文 件	
文 件 編 號	IMS-P-004	
文 件 名 稱	資通安全風險管理程序書	
發 行 單 位	國立虎尾科技大學	
發 行 日 期	110 年 11 月 01 日	
版　　次	1.4	
適用單位/範圍	全校	
訂修廢單位	審　　查	核　　准

（原版簽名頁保存於 IMS 推動小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
1.0	106/01/11	初版發行
1.1	108/08/21	因應資通安全管理法施行及配合法規用詞，將「資訊」一詞修改為「資通」。
1.2	109/06/12	修改保存地點為「各單位」
1.3	110/03/29	3. 參考文件 刪除「附錄 A 資通安全管理規範」， 增 訂 「 國 際 標 準 資 訊 安 全 管 理 系 統 (ISO27001：2013)」。
1.4	110/11/01	修改 5.9.3(1). 5.9.3 中「教版:資通安全規範(附錄 A)」修改為「國際標準資訊安全管理系統(ISO27001 2013) 」

1. 目的

為促使本校資通資產風險評鑑與處理作業有一明確規範，以鑑別資通資產之弱點及威脅而導致之風險，並依據評鑑結果採取對策或控制措施，降低資通資產遭受損害的風險。

2. 適用範圍

本校資通安全風險評鑑與處理各項作業之管理。

3. 參考文件

3.1 國際標準資訊安全管理系統(ISO27001：2013)。

3.2 教育體系資通安全暨個人資料管理規範。

3.3 IMS-P-003 資通資產管理程序書。

3.4 IMS-W-002 資通安全風險評鑑量化標準書。

4. 名詞定義

4.1 風險（Risk）

威脅會利用單一或一群資產的弱點，造成資產的損失或損壞的潛在可能性。

4.2 威脅（Threat）

資通資產因面臨未預期的意外事件，可能會對系統或組織造成傷害，威脅必須利用資產的弱點才能對資產造成傷害。

4.3 弱點（Vulnerability）

指單一或一系列會讓威脅有機可趁而造成資產損害的狀況，資產的脆弱點本身並不會造成傷害。

4.4 風險管理（Risk management）

以可接受的成本，對可能影響資通資產的安全風險進行鑑別、控制及降低或排除的過程，包含風險評鑑與風險處理。

4.5 風險評鑑（Risk assessment）

對資通資產及各項資訊設施的威脅、衝擊及弱點及其發生可能性的評鑑。

4.6 風險處理（Risk treatment）

選擇與實施各項控制措施，以修正風險的過程。

4.7　資產價值（資產鑑價 C、I、A）

4.7.1　機密性（Confidentiality，簡稱 C）：確保只有經過授權的人才能存取資訊。

4.7.2　完整性（Integrity，簡稱 I）：保護資訊及其處理方法的準確性和完整性。

4.7.3　可用性（Availability，簡稱 A）：確保經過授權的用戶在需要時可以存取資訊並使用相關資訊資產。

5. 作業內容

5.1 資通安全風險管理流程圖

作業流程	權責單位	相關表單
產生風險評鑑需求	IMS 推動小組	
建立風險評鑑方法	IMS 推動小組	
資通資產鑑別與評價	各單位 彙整給 IMS 推動小組	資通資產清冊
弱點及威脅分析	各單位	風險評鑑工作表
計算風險值	各單位 彙整給 IMS 推動小組	風險評鑑工作表
撰寫風險評鑑報告	IMS 推動小組	風險評鑑報告
決定可接受風險等級（No）	資通安全暨個人資料保護推動委員會	風險評鑑報告
擬定及執行風險處理計畫	各單位 彙整給 IMS 推動小組	風險處理計畫表
評估風險處理執行成效	資通安全暨個人資料保護推動委員會	殘餘風險評鑑工作表
Yes		
紀錄保存	各單位	

5.2　產生風險評鑑需求

為提升及維持本校資通安全管理制度之運作，每年定期（每年至少執行一次）由 IMS 推動小組進行資通安全風險評鑑作業。除每年定期執行外，亦應於下列情形發生時，針對變動範圍內的作業程序與資通資產進行風險評鑑：

5.2.1　營運組織變更。

5.2.2　相關法令法規變更而影響到本校。

5.2.3　作業流程或服務範圍改變。

5.2.4　資通資產新增或變更。

5.2.5　相關利害團體反映時。

5.2.6　發生重大資通安全事件。

5.3　建立風險評鑑方法

5.3.1　風險評鑑因素

風險評鑑為計算資通資產風險值之程序，用以決定風險處理之優先順序。資通資產風險值是以其機密性、完整性、可用性等三項因子所構成之資通資產價值，以及資通資產所面臨之弱點脆弱度、威脅發生機率及衝擊影響程度決定。

5.3.2　風險值計算流程

依據資產管理作業程序判定資通資產價值（P），依據風險評鑑作業程序識別弱點之脆弱度（V）、威脅之發生機率（T）以及衝擊影響程度（IM），將此四項評分進行相乘，即求出該資通資產之風險值。

5.3.3　風險值公式

風險值因子	代號
資產價值	P
弱點脆弱度	V
威脅發生機率	T
衝擊嚴重程度	IM

資通資產總風險值 = SUM（P × V × T × IM）

5.4　資通資產鑑別與評價

5.4.1　資通資產鑑別

IMS 推動小組依據「IMS-P-003 資通資產管理程序書」之作業說明，請各單位執行資通資產鑑別作業，並建立「IMS-P-003-01 資通資產清冊」，建立「IMS-P-003-01 資通資產清冊」之作業方式詳見「IMS-P-003 資通資產管理程序書」。

5.4.2　資通資產評價

資通資產管理者須針對各項資通資產之機密性、完整性、可用性等三項資通資產價值因子進行資通資產評價。各因子評價標準應依據「IMS-P-003 資通資產管理程序書」對資通資產進行評價。

5.5　弱點及威脅分析

5.5.1　資通資產管理者須針對各項資通資產之使用及管理現狀，識別資通資產所面臨之內部弱點及外在威脅，並分析其脆弱度與發生機率。

5.5.2　資通資產弱點之識別應依據「IMS-W-002 資通安全風險評鑑量化標準書」中「資通資產之弱點與威脅對應表」內之對應關係，列出各項資通資產可能之弱點。

5.5.3　資通資產威脅之識別應依據「IMS-W-002 資通安全風險評鑑量化標準書」中「資通資產之弱點與威脅對應表」內之對應關係，列出各項資通資產弱點所存在之可能威脅。

5.5.4　依據「IMS-W-002 資通安全風險評鑑量化標準書」中「資產衝擊影響評估標準」，鑑別各項威脅對資通資產所造成之機密性、完整性、可用性之衝擊。

5.5.5　根據 5.5.2、5.5.3、5.5.4 作業，建立「IMS-P-004-01 風險評鑑工作表」。

5.5.6　資通資產管理者依「IMS-P-004-01 風險評鑑工作表」，針對資通資產弱點之脆弱度（「脆弱點評估」欄）及威脅之發生機率（「威脅評估」欄）進行評分。評分標準分別詳見「IMS-W-002 資通安全風險評鑑量化標準書」中「資產脆弱點評鑑標準」及「資產威脅評鑑標準」章節。

5.6　計算風險值

根據「IMS-P-004-01 風險評鑑工作表」所評鑑之資產價值（「資產價值評估」欄）、弱點（「脆弱點評估」欄）及威脅（「威脅評估」欄）分析，依本程序書 5.3.3 之計算公式進行風險值之計算，以獲得資通資產個別弱點與威脅之風險值（「風險值小計」欄）及資通資產所有弱點與威脅之風險總值（「總風險值」欄）。

5.7　撰寫風險評鑑報告

IMS 推動小組依據彙整各單位的 IMS-P-004-01 風險評鑑工作表結果撰寫「IMS-P-004-02 風險評鑑報告」，並分析資通資產安全需求，提出可接受之風險等級建議，提報「資通安全暨個人資料保護推動委員會」審查及決定可接受之風險等級。

5.8　決定可接受之風險等級

5.8.1　「資通安全暨個人資料保護推動委員會」應審查「IMS-P-004-02 風險評鑑報告」，並針對所提出之風險等級建議，決定可接受之風險等級。

5.8.2　可接受風險等級之決定因素：

5.8.2.1　風險嚴重（衝擊）程度。

5.8.2.2　風險處理急迫性。

5.8.2.3　可分配之資源。

5.9　擬訂風險處理計畫

5.9.1　依風險評鑑結果及可接受風險等級之決議，由 IMS 推動小組針對需降低風險等級之資通資產擬訂風險處理計畫，以期將風險降至可接受之程度。

5.9.2　風險處理計畫應依據「IMS-P-004-03 風險處理計畫表」之格式撰寫。

5.9.3　風險處理計畫之風險處理措施，應根據國際標準資訊安全管理系統(ISO27001：2013)。對各項資通安全之要求目標，擬訂適當之處理措施及相關執行資源之資訊。

5.9.4 風險處理計畫應提報「資通安全暨個人資料保護推動委員會」審查後執行。

5.10 執行風險處理計畫

應依據風險處理計畫之風險處理項目、所需資源、預訂完成日期等規劃，執行各項風險控制措施，並將執行進度紀錄於「IMS-P-004-03 風險處理計畫表」之「風險處理進度」欄。

5.11 評估風險處理計畫執行成效

5.11.1 風險處理計畫於處理完成或有預期成效後，須由 IMS 推動小組針對進行風險處理之資通資產，依本程序書之風險評鑑程序實施風險重新評鑑，並紀錄於「IMS-P-004-04 殘餘風險評鑑工作表」，以確認風險處理計畫之執行達到風險減緩預期效益之目標，並將風險重新評鑑之結果提報「資通安全暨個人資料保護推動委員會」審查。

5.11.2 若經風險重新評鑑後，資通資產之風險值未達預期效益，亦即仍處於不可接受之風險等級，IMS 推動小組則需依本程序書之風險處理程序進行風險再處理作業或接受該項風險。

5.12 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	風險評鑑工作表	各單位	至少 3 年
2	風險評鑑報告	各單位	至少 3 年
3	風險處理計畫表	各單位	至少 3 年
4	殘餘風險評鑑工作表	各單位	至少 3 年

6. 附件

6.1 IMS-P-003-01 資通資產清冊。

6.2 IMS-P-004-01 風險評鑑工作表。

6.3 IMS-P-004-02 風險評鑑報告。

6.4 IMS-P-004-03 風險處理計畫表。

6.5　IMS-P-004-04 殘餘風險評鑑工作表。