大 仁 科 技 大 學
Tajen University

管 制 文 件 訂 修 廢 履 歷 表

文件編號	資訊-標準-03	檔案名稱	資訊安全風險評鑑量化表	
使用部門	圖書資訊館		機密等級	普通

版次	頁數	檔修訂摘要	實施日期
A.0	22	初版	99/05/24

訂修廢者	單位主管	圖書資訊館館長

※管制檔不得擅自塗改及做記號並禁止影印。

1.目的

為確保本校圖書資訊館在進行資訊資產風險評鑑作業時,為了能有效計算各項資訊資產的價值度與風險值，進行資訊資產弱點及威脅分析，特制訂本標準書。

2.適用範圍

凡本校圖書資訊館進行各項資訊資產風險評鑑作業時,均適用本標準書。

3.參考文件

無。

4.名詞定義

無。

5.作業內容

5.1 資訊資產評價

5.1.1 評價標準

等級	詳細說明
7	影響程度「極高」
5	影響程度「高」
3	影響程度「中」
1	影響程度「低」

5.1.2 資訊資產評價標準定義

5.1.2.1 文件類資訊資產價值評分標準

文件類資訊資產價值評分標準

風險標準	C (機密性)	I (完整性)	A (可用性)
定義說明	著重於保護資產，確保只有獲得授權的人才能存取該資產	著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊	確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊
(7)極高	■ 資產內資料屬於**密** ■ 資料內容若洩漏會影響**大多數師生權益** ■ 組織**需立即採取補救措施** ■ 資訊、資料存取權限須經由**權責主管或代理人**核准同意者 ■ 可對應至文件分級或資訊資產分級之"**密**"等級	■ 資產內資料若不完整，將導致**全組織作業受創** ■ **影響大多數師生權益**。 ■ 需立即通報**主管機關、權責主管(代理人)或警政單位**，並啟動應變機制	■ 作業**完全仰賴**資訊資產，且一旦資訊遺失或損毀時將**影響全組織**對外提供服務作業

文件類資訊資產價值評分標準

風險標準	C (機密性)	I (完整性)	A (可用性)
(5) 高	■ 資產內資料屬於**密** ■ 資料內容若洩漏會**影響組織聲譽及師生權益** ■ 組織**需採取補救措施** ■ 資訊、資料存取權限須經由**權責主管或代理人**核准同意者 ■ 可對應至文件分級或資訊資產分級之**"密"**等級	■ 資產內資料若不完整，將導致**組織部分作業受影響** ■ 造成**少數師生**權益受損 ■ 需通報**權責主管或代理人**，並採取補救措施	■ 作業**高度仰賴**資訊資產，且一旦資訊遺失或損毀時將**影響組織內跨部門**作業
(3) 中	■ 資產內資料僅供**內部使用** ■ 資料內容若洩漏會對組織造成**有形或無形的損害**，此**損害**為組織**可承受之範圍** ■ 資訊、資料存取權限須經由**單位主管或代理人**核准同意 ■ 可對應至文件分級或資訊資產分級之**"內部使用"**	■ 資產內資料若不完整，將造成**部門作業受影響** ■ 造成**個人**權益受損 ■ 需通報**單位主管或代理人**，損害為組織**可承受之範圍**	■ 作業**仰賴**資訊資產，且一旦資訊遺失或損毀時將**影響部門作業**
(1) 低	■ 資產內為**一般性資料，但須遵守相關發佈流程** ■ 若流傳至組織以外，**不會**對組織**造成**任何有形或無形的**傷害**(註 1) ■ 資訊、資料存取權限只須經由**資產管理人或承辦人**同意者 ■ 可對應至文件分級或資訊資產分級之**"普通"**等級	■ 資產內資料若不完整，將造成**少數或個別承辦人作業受影響** ■ 不對服務對象造成影響，最多是承辦人**重覆作業工作** ■ 不需通報，**資產管理人或承辦人**可自行處理	■ 作業**仰賴**資訊資產，且一旦資訊遺失或損毀時將**影響少數承辦人**作業

註 1：有形的傷害如：財務上的賠償、主管機關的懲處；
無形的傷害如：形象上的受損、組織內部員工士氣的低落。

5.1.2.2 硬體類、建築與保護類及服務類資訊資產價值評分標準

硬體類、建築與保護類及服務類資訊資產價值評分標準

風險標準	C (機密性)	I (完整性)	A (可用性)
定義說明	著重於保護資產，確保只有獲得授權的人才能存取該資產	著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊	確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊
(7) 極高	■ 不適用	■ 實體與服務若不完整，將導致**全組織作業受創** ■ 需立即通報主管機關、權責主管(代理人)，並啟動應變機制	■ 可忍受服務中斷時間：**4 小時以內** ■ 作業**完全仰賴**資訊資產，且一旦服務中斷時將**影響全組織**對外所提供的服務作業
(5) 高	■ 不適用	■ 實體與服務若不完整，將導致**組織部分作業受影響** ■ 需通報權責主管或代理人，並採取補救措施	■ 可忍受服務中斷時間：**4 小時以上~8 小時** ■ 作業**高度仰賴**資訊資產，且一旦服務中斷時將**影響組織內跨部門**運作
(3) 中	■ 不適用	■ 實體與服務若不完整，將造成**部門作業受影響** ■ 需通報單位主管或代理人，損害為組織可承受之範圍	■ 可忍受服務中斷時間：**8~24 小時** ■ 作業**仰賴**資訊資產，且一旦服務中斷時將**影響部門**運作
(1) 低	■ 實體及服務類之機密性皆屬此一等級	■ 實體與服務若不完整，將造成**少數或個別承辦人作業受影響** ■ 不需通報，資產管理人或承辦人可自行處理	■ 可忍受服務中斷時間：**24 小時以上** ■ 作業**仰賴**資訊資產，且一旦服務中斷時將**影響少數承辦人**作業

5.1.2.3 軟體類資訊資產價值評分標準

軟體類資訊資產價值評分標準

風險標準	C (機密性)	I (完整性)	A (可用性)
定義說明	著重於保護資產，確保只有獲得授權的人才能存取該資產	著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊	確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊
(7) 極高	■ 軟體/程式邏輯若洩漏會**影響組織重大權益** ■ 若遭有心人士所用將**造成組織財務極大損失** ■ 組織**需立即採取補救措施**	■ 軟體若不完整，將導致**全組織作業受創** ■ **影響大多數使用者權益**。 ■ 需立即通報**主管機關、權責主管(代理人)**，並啟動應變機制	■ 可忍受服務中斷時間：4 **小時以內** ■ 作業**完全仰賴**資訊資產，且一旦服務中斷時將**影響全組織**對外所提供的服務作業
(5) 高	■ 軟體/程式邏輯若洩漏會**影響組織財務部分權益** ■ 若遭有心人士所用將**造成財務損失** ■ 組織**需採取補救措施**	■ 軟體若不完整，將導致**組織部分作業受影響** ■ 造成**少數使用者**權益受損 ■ 需通報**權責主管或代理人**，並採取補救措施	■ 可忍受服務中斷時間：4 **小時以上~8 小時** ■ 作業**高度仰賴**資訊資產，且一旦服務中斷時將**影響組織內跨部門**運作
(3) 中	■ 軟體/程式邏輯若洩漏會對組織造成**有形或無形的損害，此損害**為組織**可承受之範圍**	■ 軟體若不完整，將造成**部門作業受影響** ■ 造成**個人**權益受損 ■ 需通報**單位主管或代理人**，損害為組織**可承受之範圍**	■ 可忍受服務中斷時間：**8 ~24 小時** ■ 作業**仰賴**資訊資產，且一旦服務中斷時將**影響部門**運作
(1) 低	■ 軟體/程式邏輯若流傳至組織以外，**不會**對組織**造成**任何有形或無形的**傷害**(註 1)	■ 軟體若不完整，將造成**少數或個別承辦人作業受影響** ■ 不對服務對象造成影響，最多是承辦人**重覆作業工作** ■ 不需通報，**資產管理人或承辦人**可自行處理	■ 可忍受服務中斷時間：**24 小時以上** ■ 作業**仰賴**資訊資產，且一旦服務中斷時將**影響少數承辦人**作業

註 1：有形的傷害如：財務上的賠償、主管機關的懲處；
無形的傷害如：形象上的受損、組織內部員工士氣的低落。

5.1.2.4 人員類資訊資產價值評分標準

人員類資訊資產價值評分標準

風險標準	C（機密性）	I（完整性）	A（可用性）
定義說明	著重於保護資產，確保只有獲得授權的人才能存取該資產	著重於確保資料的正確性及資產(作業)處理的完整性，以避免因運用錯誤的資料或因資產處理的不完全，而造成對組織的衝擊	確保資產提供使用者所需的服務，以達成預期之功能，主要為避免因災害而致使組織無法持續運作或提供服務之衝擊
(7)極高	■ 人員所接觸之資料內容屬於**密** ■ 資料內容若洩漏會**影響大多數師生權益**	■ 人員因人為的疏忽、失誤、操作錯誤造成資料不完整，將**影響全組織**對外所提供的服務作業	■ 作業**完全仰賴**該員，且一旦該員無法作業時，將**影響全組織**對外所提供的服務作業
(5)高	■ 人員所接觸之資料內容屬於**密** ■ 資料內容若洩漏會嚴重**影響組織聲譽及師生權益**	■ 人員因人為的疏忽、失誤、操作錯誤造成資料不完整，將**影響組織內跨部門**運作	■ 作業**高度仰賴**該員，且一旦該員無法作業時，將**影響組織內跨部門**運作
(3)中	■ 人員所接觸之資料內容僅供**內部使用** ■ 資料內容若洩漏會對組織造成**有形或無形的損害**，此損害為組織**可承受之範圍**	■ 人員因人為的疏忽、失誤、操作錯誤造成資料不完整，將**影響部門**運作	■ 作業**仰賴**該員，且一旦該員無法作業時，將**影響部門**運作
(1)低	■ 人員所接觸之資料為**一般性資料，但須遵守相關發佈流程** ■ 若流傳至組織以外，**不會**對組織**造成**任何有形或無形的**傷害**(註 1)	■ 人員因人為的疏忽、失誤、操作錯誤造成資料不完整，僅**影響少數承辦人**作業	■ 作業**仰賴**該員，且一旦該員無法作業時，將**影響少數承辦人**作業，其工作可暫時委由他人替代。

註 1：有形的傷害如：財務上的賠償、主管機關的懲處；
無形的傷害如：形象上的受損、組織內部員工士氣的低落。

5.2 資訊資產之弱點、威脅與衝擊對應表

5.2.1 文件類資訊資產

大類	小類	弱點	威脅	C	I	A
文件類	全類	缺乏文件及紀錄之管控	遺失、毀損、未授權存取	1	1	1
		缺乏實體保護	遺失、遭竊	1	1	1
			未授權存取	1	1	1
		缺乏備援拷貝	資料損毀	0	0	1
		缺乏加密機制	資料外洩	1	1	1
			非授權的存取	1	1	1
		攜帶方便、易被拷貝	資料外洩	1	0	1

5.2.2 人員類資訊資產

大類	小類	弱點	威脅	C	I	A
人員類	全類	人員短缺	人員短缺	0	0	1
		不足的安全訓練及認知	操作人員的錯誤	1	1	1
		不當使用軟體及(或)硬體	操作人員的錯誤	1	1	1
			非法輸出/入軟、硬體	1	1	1
		不當的招募程序	罷工、怠工	1	1	1
			偷竊	1	1	1
			惡意損毀	1	1	1
		無簽署保密協議	機密資料外洩	1	1	1
		缺乏專業領域技能	作業延遲或中斷	1	1	1

5.2.3 服務類資訊資產

大類	小類	弱點	威脅	C	I	A
服務類	全類	不足的安全訓練	操作者錯誤	1	1	1
		不當使用軟體及(或)硬體	操作者錯誤	1	1	1
		不當的招募程序	偷竊	1	0	0
			惡意損毀	0	1	1
		不當的服務維護回應	硬體故障	0	1	1
			電力供應故障	0	1	1
		缺乏安全的認知(awareness)	使用者錯誤	1	1	1

5.2.4 建築與保護類資訊資產

大類	小類	弱點	威脅	C	I	A
建築與保護類	一般辦公區域	不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1
		缺乏門禁管制	偷竊	1	1	1
	特殊辦公區域	位處易有水患之地	水災土石流	0	1	1
		不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1
		缺乏門禁管制	偷竊	1	1	1
	資訊機房區域	位處易有水患之地	水災土石流	0	1	1
		不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬　體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1

		缺乏門禁管制	偷竊	1	1	1
		缺乏備援拷貝	水災土石流	0	1	1
			資料遺失或毀損	0	1	1
			惡意損毀	0	1	1
		對溫度變化敏感	空調故障	0	0	1
			溫度與濕度超過限值	0	0	1
	倉庫(庫房)	不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		位處易有水患之地	水災土石流	0	1	1
		建築或房間不當或疏於使用實體進出管制	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的不正確使用	1	1	1
	建築保護設施(環境控制系統如:火偵測、熱偵測、水偵測系統、自動消防滅火系統、溫濕度偵測等)	位處易有水患之地	水災土石流	0	1	1
		不足的維護或安裝的錯誤	地震	0	0	1
			維護錯誤	0	1	1
			儲存媒體變質	0	1	1
		不當的服務維護回應	水供應故障	0	0	1
			空調故障	0	0	1
			硬體故障	0	1	1
			電力供應故障	0	0	1
		未監督外來人員或清潔人員之工作	偷竊	1	1	1
		不當控管及使用或疏於管制實體進出	偷竊	1	1	1
			惡意損毀	1	1	1
			資源的損壞	1	1	1
		缺乏監控(monitoring)機制	以非授權的方式使用軟體	1	0	1
			以非授權的方式使用網路設施	1	0	1
			非法使用軟體	1	1	1
			非法輸出/入軟體	1	0	1

			溫度與濕度超過限值	0	1	1
		對溫度變化敏感	空調故障	0	0	1
			溫度與濕度超過限值	0	0	1
		對電壓變化敏感	電壓不隱定	0	0	1

5.2.5 軟體類資訊資產

大類	小類	弱點	威脅	CI	II	AI
軟體類	軟體開發工具	缺乏備援拷貝	惡意軟體	1	1	1
		缺乏有效變更控制	操作人員的錯誤	0	1	1
			使用者的錯誤	0	0	1
		繁複的使用者介面	操作人員的錯誤	0	1	1
			使用者的錯誤	0	1	1
		缺乏稽核軌跡	未經授權的使用	1	0	0
		缺乏識別及鑑別機制(如使用者鑑別)	假冒使用者身分	1	0	0
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用	1	0	0
			偷竊	1	0	0
		離開工作站沒有登出(Logout)	未經授權的使用	1	0	0
		沒有或不足的軟體測試	軟體故障	0	1	1
		不良的通行碼(password)管理	假冒使用者身分	1	0	0
		通行碼以明碼傳送	未經授權的使用	1	0	0
		軟體的已知缺陷	非法輸出/入軟體	1	1	0
			惡意的軟體	0	1	1
			軟體故障	0	1	1
	資訊安全系統	缺乏備援拷貝	惡意軟體	1	1	1
		缺乏有效變更控制	操作人員的錯誤	0	1	1
			使用者的錯誤	0	0	1
		繁複的使用者介面	操作人員的錯誤	0	1	1
			使用者的錯誤	0	1	1
		不當的服務維護回應	空調故障	0	0	1
			電力供應故障/停水	0	0	1
			硬體故障	0	0	1

			軟體故障	0	1	1
		缺乏稽核軌跡	未經授權的使用	1	0	0
		缺乏有效的建構變更控制	使用者的錯誤	0	1	1
			操作人員的錯誤	0	1	1
			軟體故障	0	1	1
		缺乏識別及鑑別機制(如使用者鑑別)	假冒使用者身分	1	0	0
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用	1	0	0
			偷竊	1	0	0
		離開工作站沒有登出(Logout)	未經授權的使用	1	0	0
		沒有或不足的軟體測試	軟體故障	0	1	1
		不良的通行碼(password)管理	假冒使用者身分	1	0	0
		通行碼以明碼傳送	未經授權的使用	1	0	0
		不明確或不完整的開發規格	軟體故障	0	1	1
		軟體的已知缺陷	非法輸出/入軟體	1	1	0
			惡意的軟體	0	1	1
			軟體故障	0	1	1
	作業系統	缺乏稽核軌跡	未經授權的使用	1	0	0
		缺乏備援拷貝	惡意軟體	0	0	1
		缺乏有效的建構變更控制	操作人員的錯誤	1	1	1
			使用者的錯誤	0	1	1
			軟體故障	0	1	1
		缺乏識別及鑑別機制(如使用者鑑別)	假冒使用者身分	1	0	0
		離開工作站沒有登出(Logout)	未經授權的使用	1	0	0
		沒有或不足的軟體測試	軟體故障	0	1	1
		不良的通行碼(password)管理	未經授權的使用	1	0	0
			假冒使用者身分	1	0	0
		通行碼以明碼傳送	未經授權的使用	1	0	0
		軟體的已知缺陷	非法輸出/入軟體	1	1	0
			惡意軟體	1	1	0

			軟體故障	0	1	1
	應用系統	缺乏備援拷貝	惡意軟體	1	1	1
		缺乏有效變更控制	操作人員的錯誤	0	1	1
			使用者的錯誤	0	0	1
		繁複的使用者介面	操作人員的錯誤	0	1	1
			使用者的錯誤	0	1	1
		不當的服務維護回應	空調故障	0	0	1
			電力供應故障/停水	0	0	1
			硬體故障	0	0	1
			軟體故障	0	1	1
		缺乏稽核軌跡	未經授權的使用	1	0	0
		缺乏有效的建構變更控制	使用者的錯誤	0	1	1
			操作人員的錯誤	0	1	1
			軟體故障	0	1	1
		缺乏識別及鑑別機制(如使用者鑑別)	假冒使用者身分	1	0	0
		缺乏發送端與接收端識別及鑑別機制	未經授權的使用	1	0	0
			偷竊	1	0	0
		離開工作站沒有登出(Logout)	未經授權的使用	1	0	0
		沒有或不足的軟體測試	軟體故障	0	1	1
		不良的通行碼(password)管理	假冒使用者身分	1	0	0
		通行碼以明碼傳送	未經授權的使用	1	0	0
		不明確或不完整的開發規格	軟體故障	0	1	1
		軟體的已知缺陷	非法輸出/入軟體	1	1	0
			惡意的軟體	0	1	1
			軟體故障	0	1	1

5.2.6 硬體類資訊資產

大類	小類	弱點	威脅	C	I	A
硬體類	個人電腦	不當使用軟體及(或)硬體	資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		未保護的儲存空間	偷竊	1	0	1
			惡意損毀	1	0	1
			溫度與濕度超過限值	0	1	1
			儲存媒體變質	0	1	1
		存取控制的錯誤配置	未授權即使用媒體	1	0	1
			資源的不正確使用	1	0	1
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏監控(monitoring)機制	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			溫度與濕度超過限值	0	1	1
			資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		缺乏稽核軌跡	未授權即使用媒體	1	0	1
			資源的不正確使用	1	0	1
		對電磁輻射敏感	硬體故障	0	0	1
			電磁輻射	0	0	1
			靜電	0	0	1
			儲存媒體變質	0	1	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不隱定	0	0	1
			儲存媒體變質	0	1	1
		對濕度灰塵及塵土敏感	灰塵	0	0	1
			空調故障	0	0	1
			硬體故障	0	0	1
			儲存媒體變質	0	1	1
	可攜式電腦	不足的維護或儲存媒體錯誤的安裝	硬體故障	1	0	1
			維護錯誤	0	0	1

		不當使用軟體及(或)硬體	硬體故障	0	0	1
			資源的不正確使用	1	0	1
		不當的服務維護回應	硬體故障	0	0	1
		未控制通訊線路	由非授權人員存取網路	1	0	1
			流量分析	1	0	1
			訊息轉接(rerouting)	1	0	1
			資源的不正確使用	1	0	1
		存取控制的錯誤配置	偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏監控(monitoring)機制	偷竊	1	0	1
			惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不隱定	0	0	1
		廢棄物處理疏於照管	偷竊	1	0	1
			資源的不正確使用	1	0	1
		撥接線路	由非授權人員存取網路	1	0	1
			資源的不正確使用	1	0	1
		儲存媒體未加以適當清除即丟棄或再利用	偷竊	1	0	1
			資源的不正確使用	1	0	1
	伺服器	不足的維護或儲存媒體錯誤的安裝	硬體故障	0	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	硬體故障	0	0	1
			資源的不正確使用	1	0	1
		不當的服務維護回應	硬體故障	0	0	1
		存取控制的錯誤配置	偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1

		缺乏有效的建構變更控制	硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏監控(monitoring)機制	偷竊	1	0	1
			惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		單點失效(Single point of failure)	通訊服務故障	0	0	1
			通訊纜線損壞	0	0	1
			硬體故障	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不隱定	0	0	1
		廢棄物處理疏於照管	偷竊	1	0	1
			資源的不正確使用	1	0	1
		儲存媒體未加以適當清除即丟棄或再利用	偷竊	1	0	1
			資源的不正確使用	1	0	1
	其他硬體	不足的維護或儲存媒體錯誤的安裝	硬體故障	0	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	硬體故障	0	0	1
			資源的不正確使用	1	0	1
		不當的服務維護回應	硬體故障	0	0	1
		存取控制的錯誤配置	未授權即使用媒體	1	0	1
			非法輸出/入軟體	1	0	0
			偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏監控(monitoring)機制	偷竊	1	0	1
			惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1

			操作人員的錯誤	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不隱定	0	0	1
		廢棄物處理疏於照管	偷竊	1	0	1
			資源的不正確使用	1	0	1
	網路設備	不良的佈線	通訊服務故障	0	0	1
			通訊纜線損壞	0	0	1
			傳輸錯誤	0	0	1
			滲透通訊	1	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		不良的通行碼(password)管理	由非授權的人員使用軟體	1	0	1
			假冒使用者身分	1	0	1
		不足的維護或儲存媒體錯誤的安裝	通訊服務故障	0	0	1
			硬體故障	0	0	1
			網路組件故障	0	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	通訊服務故障	0	0	1
			硬體故障	0	0	1
			資源的不正確使用	1	0	1
			網路組件故障	0	0	1
		不當的服務維護回應	通訊服務故障	0	0	1
			硬體故障	0	0	1
			網路組件故障	0	0	1
		不當的網路管理	流量超載	0	0	1
			通訊服務故障	0	0	1
		未保護公眾網路連線	由非授權人員存取網路	1	0	1
			資源的不正確使用	1	0	1
		未保護敏感性資訊流	流量分析	1	0	1
			訊息被重組或轉送	1	1	1
		未保護通行碼資料表	由非授權的人員使用軟體	1	0	1
			假冒使用者身分	1	0	1
		未控制通訊線路	流量分析	1	0	1
			訊息轉接(rerouting)	1	0	1

			通訊纜線損壞	0	0	1
		存取控制的錯誤配置	惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			網路組件故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏發送端與接收端識別及鑑別機制	由非授權人員存取網路	1	0	1
			訊息被重組或轉送	1	1	1
			訊息轉接(rerouting)	1	0	1
		缺乏監控(monitoring)機制	惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		缺乏稽核軌跡	以非授權的方式使用網路設施	1	0	1
			由非授權人員存取網路	1	0	1
			惡意損毀	1	0	1
		缺乏識別及鑑別機制(如使用者鑑別	由非授權的人員使用軟體	1	0	1
			假冒使用者身分	1	0	1
		軟體的已知缺陷	由非授權的人員使用軟體	1	0	1
			軟體故障	0	0	1
			惡意軟體	1	0	1
		通行碼以明碼傳送	由非授權的人員使用軟體	1	0	1
			假冒使用者身分	1	0	1
		單點失效(Single point of failure)	通訊服務故障	0	0	1
			硬體故障	0	0	1
			網路組件故障	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不隱定	0	0	1
		繁複的使用者介面	操作人員的錯誤	0	0	1
	通訊設備	不良的佈線	通訊服務故障	0	0	1
			通訊纜線損壞	0	0	1
			傳輸錯誤	0	0	1

			滲透通訊	1	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
			竊聽	1	0	0
		不良的通行碼(password)管理	假冒使用者身分	1	0	1
			資源的不正確使用	1	0	1
		不足的維護或儲存媒體錯誤的安裝	通訊服務故障	0	0	1
			硬體故障	0	0	1
			維護錯誤	0	0	1
		不當使用軟體及(或)硬體	通訊服務故障	0	0	1
			硬體故障	0	0	1
			資源的不正確使用	1	0	1
		不當的服務維護回應	通訊服務故障	0	0	1
			硬體故障	0	0	1
		未保護公眾網路連線	資源的不正確使用	1	0	1
			竊聽	1	0	0
		未保護敏感性資訊流	竊聽	1	0	0
		未控制通訊線路	通訊纜線損壞	0	0	1
			竊聽	1	0	0
		存取控制的錯誤配置	惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的建構變更控制	通訊服務故障	0	0	1
			硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏發送及接收訊息的證據	否認服務交易或收送訊息	1	1	1
		缺乏發送端與接收端識別及鑑別機制	否認服務交易或收送訊息	1	1	1
			資源的不正確使用	1	0	1
		缺乏監控(monitoring)機制	惡意損毀	1	0	1
			硬體故障	0	0	1
			資源的不正確使用	1	0	1
		缺乏稽核軌跡	惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏識別及鑑別機制(如使	否認服務交易或收送訊息	1	1	1

		用者鑑別	假冒使用者身分	1	0	1
		單點失效(Single point of failure)	通訊服務故障	0	0	1
			硬體故障	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不隱定	0	0	1
		撥接線路	資源的不正確使用	1	0	1
		繁複的使用者介面	使用者錯誤	0	0	1
	可攜式儲存媒體	不良的通行碼(password)管理	未授權即使用媒體	1	0	1
		不足的維護或儲存媒體錯誤的安裝	硬體故障	0	0	1
			儲存媒體變質	0	1	1
		不當使用軟體及(或)硬體	非法使用軟體	1	0	1
			非法輸出/入軟體	1	0	0
			資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		未保護的儲存空間	偷竊	1	0	1
			惡意損毀	1	0	1
			溫度與濕度超過限值	0	0	1
			儲存媒體變質	0	1	1
		未控制複製	偷竊	1	0	1
			資源的不正確使用	1	0	1
		存取控制的錯誤配置	未授權即使用媒體	1	0	1
			非法使用軟體	1	0	1
			非法輸出/入軟體	1	0	0
			資源的不正確使用	1	0	1
		缺乏正確使用通訊媒體與傳訊的政策	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			惡意損毀	1	0	1
			資源的不正確使用	1	0	1
		缺乏有效的變更控制	使用者錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏定期替換計畫(schemes)	硬體故障	0	0	1
			儲存媒體變質	0	1	1
		缺乏備援拷貝	水災土石流	0	0	1
			火災	0	0	1

			偷竊	1	0	1
			惡意損毀	1	0	1
			儲存媒體變質	0	1	1
		缺乏發送及接收訊息的證據	否認服務交易或收送訊息	1	1	1
			儲存媒體變質	0	1	1
		缺乏監控(monitoring)機制	未授權即使用媒體	1	0	1
			非法使用軟體	1	0	1
			非法輸出/入軟體	1	0	0
			偷竊	1	0	1
			溫度與濕度超過限值	0	0	1
			資源的不正確使用	1	0	1
			儲存媒體變質	0	1	1
		缺乏稽核軌跡	未授權即使用媒體	1	0	1
			資源的不正確使用	1	0	1
		對電磁輻射敏感	硬體故障	0	0	1
			電磁輻射	0	0	1
			靜電	0	0	1
			儲存媒體變質	0	1	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不隱定	0	0	1
			儲存媒體變質	0	1	1
		對濕度灰塵及塵土敏感	灰塵	0	1	1
			空調故障	0	0	1
			硬體故障	0	0	1
			儲存媒體變質	0	1	1
		廢棄物處理疏於照管	偷竊	1	0	1
			資源的不正確使用	1	0	1
		儲存媒體未加以適當清除即丟棄或再利用	未授權即使用媒體	1	0	1
			偷竊	1	0	1
			資源的不正確使用	1	0	1
	電腦保護設施	不足的維護或儲存媒體錯誤的安裝	硬體故障	0	0	1
			維護錯誤	0	0	1
		不當的服務維護回應	硬體故障	0	0	1
		存取控制的錯誤配置	惡意損毀	1	0	1

			資源的不正確使用	1	0	1
		位處易有水患之地	水災土石流	0	0	1
		缺乏有效的建構變更控制	硬體故障	0	0	1
			維護錯誤	0	0	1
			操作人員的錯誤	0	0	1
		缺乏定期替換計畫(schemes)	硬體故障	0	0	1
			儲存媒體變質	0	1	1
		缺乏監控(monitoring)機制	惡意損毀	1	0	1
			硬體故障	0	0	1
			溫度與濕度超過限值	0	0	1
			操作人員的錯誤	0	0	1
		單點失效(Single point of failure)	硬體故障	0	0	1
			電力供應故障	0	0	1
			電壓不隱定	0	0	1
		對電壓變化敏感	硬體故障	0	0	1
			電壓不隱定	0	0	1

5.3 資訊資產弱點脆弱度評分

評分標準：必須評估脆弱點的嚴重程度，亦即容易被威脅所利用。

等級	影響程度	詳細說明
7	極高	弱點無受到適當控制且無初步計畫與認知。
5	高	弱點無受到適當控制且無初步計畫但具有認知。
3	中	弱點無受到適當控制但已有初步計畫。
1	低	弱點已受到適當控制（控制措施正在執行）。

5.4 資訊資產威脅發生機率評分

判斷該威脅對資訊資產造成營運衝擊的可能性。

等級	發生可能性	詳細說明
7	極高	每季發生一次以上 (MIN：4 次/年)。
5	高	每半年發生一次以上 (MIN：2 次/年)。
3	中	每年發生一次以上 (MIN：1 次/年)。
1	低或無	每 2 年發生一次以上 (MIN：1 次/2 年)。