國立彰化高級中學

風險評鑑與管理

機密等級：一般

文件編號：CHSH-ISMS- D-006

版　　次：3.0

發行日期：115.05.29

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	112.05.30	創立		
3.0	115.05.29	修訂成 115 公告年版本		

目錄

風險評鑑與管理					
文件編號	CHSH-ISMS-D-006	機密等級	一般	版次	3.0

1 目的

建立國立彰化高級中學（以下簡稱本校）風險評鑑與管理，提供本校資通資產之權責單位、保管單位，以及使用單位，共同遵行之風險評鑑標準，有效執行風險控管，預防資通安全事件之威脅。

2 適用範圍

本校承辦相關資訊業務作業流程之風險管理。

3 權責

3.1 資通安全委員會：

負責可接受風險值、風險評鑑結果、風險改善計畫與控制措施之審查及核定。

3.2 資通安全小組：

負責相關資訊資產風險評鑑結果之複核，並針對超過可接受風險值之項目提出建議之控管措施，並產出風險改善計畫。

3.3 權責單位主管：

負責所屬單位業務範圍之風險評鑑結果審核作業。

3.4 資訊資產權責單位：

負責執行資訊資產之威脅與弱點評估、風險值計算等程序項目。

4 名詞定義

4.1 機密性 (Confidentiality)：確保只有經授權的人，才可以存取資訊。

4.2 完整性 (Integrity)：確保資訊與處理方法的正確性與完整性。

4.3 可用性（Availability）：確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 可接受風險值：各類資訊資產之最低風險容忍度。

4.5 殘餘風險（Residual Risk）：在採用相關控制措施之後剩餘的風險。

4.6 威脅（Threat）：可能對系統或組織造成傷害之意外事件。

4.7 弱點（Vulnerability）：因資訊資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

4.8 風險（Risk）：可能對團體或組織的資產發生損失或傷害的潛在威脅，通常利用弱點所產生之影響及發生可能性來衡量。

5 作業說明

5.1 鑑別資產

5.1.1資訊資產之鑑別應依據「資訊資產管理程序書」進行鑑別及分類。

5.2 鑑別風險

5.2.1威脅及弱點評估：參考 ISO 27005 將各類資訊資產可能面臨之威脅與弱點項目，分別建立「威脅及弱點評估表」。

5.2.2可能的威脅、弱點項目：參考國立華南高級商業職業學校及國立中興大學計算機及資訊網路中心之「資訊資產威脅及弱點評估表」列表以下範列。

5.2.2.1　人員（People/PE）可能的威脅、弱點項目。

威脅	弱點	風險改善建議措施
人員可利用性的違反	缺乏人員	加強人員教育訓練及控管
設備或媒體的破壞	不充分的招募程序	加強人員教育訓練及控管
使用上的誤用	不足的安全訓練	加強人員教育訓練及控管
使用上的誤用	不正確的使用硬體和軟體	加強人員教育訓練及控管
使用上的誤用	欠缺安全認知	加強人員教育訓練及控管
非法的處理資料	欠缺監控機制	加強人員教育訓練及控管
媒體或文件的盜竊	外部或清潔人員未經監督的工作	加強人員教育訓練及控管
未經授權的使用設備	欠缺正確使用電信媒體和訊息的政策	加強人員教育訓練及控管

5.2.2.2　文件（Document/DC）可能的威脅、弱點項目。

威脅	弱點
故意的破壞	人員安全訓練不足
	建築物、房間的實體進出控制不足
	缺乏安全警覺
	識別與認證機制的不足
遺失	人員安全訓練不足
	缺乏適當管理機制
失竊	人員安全訓練不足
	外部人員缺乏人員陪同作業
	存取權限授與不當
	資料銷毀時的不注意
操作人員的錯誤	不正確的使用軟體和硬體
	文件化管理之缺乏或不足

威脅	弱點
	缺乏安全警覺
	缺乏資料、程式、文件備份
	缺乏監督監督機制
	專業訓練不足

5.2.2.3　軟體（Software/SW）可能的威脅、弱點項目。

威脅	弱點	風險改善建議措施
濫用權限	無或不充分的軟體測試	建立軟體使用及檢查機制
	軟體上知名的缺點	建立軟體使用及檢查機制
	離開工作站時未確實登出	建立軟體使用及檢查機制
	處置或再使用儲存媒體未適當地消磁	建立軟體使用及檢查機制
	欠缺稽核軌跡	建立軟體使用及檢查機制
	錯誤的存取權限分配	建立軟體使用及檢查機制
資料的訛用	廣泛散佈的軟體	建立軟體使用及檢查機制
	在時間方面將應用系統程式應用至錯誤的資料	建立軟體使用及檢查機制
使用上的誤用	複雜的使用者介面	建立使用者手冊及規定
	欠缺文件	建立使用者手冊及規定
	不正確的參數設定	建立使用者手冊及規定
	不正確的日期	建立使用者手冊及規定
偽造權限	欠缺像使用者授權的識別與授權機制	建立使用者管理機制
	未保護的通行碼	建立使用者管理機制

	不良的通行碼管理	建立使用者管理機制
非法的處理資料	啟動不必要的服務	建立軟體使用及檢查機制
軟體機能失常	不成熟或新的軟體	建立軟體獲取檢查機制
	對開發者不清楚或未完成的規格	建立軟體獲取檢查機制
竄改軟體	欠缺有效的變更控制	建立軟體獲取檢查機制
	未控制的下載與使用軟體	建立軟體獲取檢查機制
	欠缺備份複本	建立軟體獲取檢查機制
媒體或文件的盜竊	欠缺對建築物、門窗的實體保護	建立實體控制機制
未經授權的使用設備	未能產出管理報告	建立實體控制機制

5.2.2.4　通訊（Communication/CM）可能的威脅、弱點項目。

威脅	弱點
線路中斷	連線電纜失效
失效	不正確的使用軟體和硬體
	缺乏適當的維護工作
	缺乏有效變更控制
	缺乏硬體耗損控管
	專業訓練不足
	缺乏監督機制
未經授權使用者的網路存取	外部人員缺乏人員陪同作業
	建築物、房間的實體進出控制的不足

5.2.2.5　硬體（Hardware/HW）可能的威脅、弱點項目。

威脅	弱點	風險改善建議措施
危害資訊系統可維護性	儲存媒體的維護不足或錯誤安裝	建立維護機制
設備或媒體的破壞	缺乏定期更換概要	建立維護機制
灰塵、腐蝕、凍結	對濕度、灰塵、土壤的敏感性	建立環控監測機制
電磁輻射	對電磁輻射的敏感性	建立環控監測機制
使用上的誤用	缺乏有效的組態變更管理	建立變更管理機制
電力供應喪失	對電壓變化的敏感性	建立電力備援機制
氣象現象	對溫度變化的敏感性	建立環控監測機制
媒體或文件的盜竊	未保護的儲存庫	建立實體控制機制
	處置時不小心	建立實體控制機制
	未控制的複製	建立實體控制機制
否認行動	欠缺寄送或接收訊息的證明	建立不可否認性機制
偷聽	未保護的傳輸線	建立電纜線保護監控機制
	未保護的敏感性電信	建立電纜線保護監控機制
電信設備故障	不良的電纜接合	建立電纜線保護監控機制
	單點失誤	建立電纜線保護監控機制
偽造權限	欠缺寄送者或接收者的識別與授權	建立存取制機制
遠端暗中監視	不安全的網路架構	定期檢視網路架構
	以明碼傳送通行碼	建立資料傳送加密機制
資訊系統飽和	不充分的網路管理、路由的彈性	建立網路監控機制
未經授權的使用設備	未保護的公用網路連接	建立網路監控機制

5.2.2.6　資料（Data/DA）可能的威脅、弱點項目。

威脅	弱點
故意的破壞	人員安全訓練不足
	建築物、房間的實體進出控制不足
	缺乏安全警覺
	識別與認證機制的不足
遺失	人員安全訓練不足
	缺乏適當管理機制
失竊	人員安全訓練不足
	外部人員缺乏人員陪同作業
	存取權限授與不當
	資料銷毀時的不注意
操作人員的錯誤	不正確的使用軟體和硬體
	文件化管理之缺乏或不足
	缺乏安全警覺
	缺乏資料、程式、文件備份
	缺乏監督監督機制
	專業訓練不足
未適當控管儲存媒介之存取	人員安全訓練不足
	未經控管之資料複製
	存取權限授與不當
	識別與認證機制的不足
	未落實桌面淨空或螢幕鎖定
	缺乏安全警覺
	缺乏監督機制
	資料銷毀時的不注意
	機密資料的外洩
	儲存媒介內之資料沒有適當刪除就丟棄或重覆使用
	外部人員缺乏人員陪同作業

5.2.2.7　環境（Environment/EV）可能的威脅、弱點項目。

威脅	弱點	風險改善建議措施
設備或媒體的破壞	對建築物與房間不充分或草率的實體存取控制	建立實體控制機制
颱風	缺乏建築物、門、窗等物質的保護	建立實體控制機制
地震	缺乏建築物、門、窗等物質的保護	建立實體控制機制
淹水、水災	位於容易淹水、水災的區域	建立環控監測機制
漏水	沒有做好維護的工作	建立環控監測機制
	環境控制系統失效	建立環控監測機制
火災	人員安全訓練不足	建立環控監測機制
	缺乏消防器材的保護	建立環控監測機制
	儲存易燃物	建立環控監測機制
	環境控制系統失效	建立環控監測機制
停電、電力供應喪失	不穩定的供電	建立環控監測機制
	不斷電系統失效	建立環控監測機制
	發電機失效	建立環控監測機制
灰塵	容易潮濕、有灰塵、穢物	建立環控監測機制
空調失效	沒有做好維護的工作	建立環控監測機制
	維護服務回應時間過長	建立環控監測機制
	缺乏緊急應變機制	建立環控監測機制
設備的盜竊	欠缺建築物、門窗的實體保護	建立實體控制機制
濫用權限	欠缺軟體使用者註冊與撤銷註冊的正式程序	建立帳密存取控制機制
	欠缺存取權限審查監督程序	建立帳密存取控制機制
	欠缺或未充分提供安全聯絡通道	建立帳密存取控制機制
	欠缺監控資訊處理設施的正式程序	建立帳密存取控制機制
	欠缺一般的稽核、監控	建立帳密存取控制機制
	欠缺風險識別與評鑑的程序	建立帳密存取控制機制
	欠缺記錄於管理員與操作員日誌的錯誤報告	建立帳密存取控制機制
危害資訊系統可維護性	不充分的服務維護回覆	建立適當的維護機制
	欠缺或不充分的服務等級協議	建立適當的維護機制
	欠缺變更控制程序	建立適當的維護機制
資料的訛用	欠缺文件控制程序	建立文件控制及監督之程序

威脅	弱點	風險改善建議措施
	欠缺記錄監督程序	建立文件控制及監督之程序
來自不可信賴來源的資料	欠缺公開資訊授權程序	建立公開資訊審核機制
否認行動	欠缺資訊安全職責的適當配置	建立不可否認性機制
設備故障	欠缺持續計畫	建立設備故障復原之機制
使用上的誤用	欠缺電子郵件使用政策	建立電子郵件使用機制
	欠缺引進軟體至業務系統的程序	建立軟體使用及控管機制
	欠缺管理員與操作員日誌的記錄	建立日誌紀錄機制
	欠缺機密資訊處理的程序	建立機密資訊處理之程序
	欠缺在工作說明的資訊安全職責	加強人員教育訓練
非法的處理資料	欠缺或未充分提供安全處理	建立安全提供資料及聯絡機制
設備的盜竊	欠缺已定義的資訊安全事故懲戒程序	建立資安事故相關獎懲程序
	欠缺行動電腦使用的正式政策	建立行動電腦使用之管理機制
	欠缺場所外資產的控制	建立資訊資產進出管理之機制
媒體或文件的盜竊	欠缺或不充分桌面淨空和螢幕淨空	建立桌面淨空之機制
	欠缺資訊處理設施的授權	建立實體控制機制
	欠缺已建立的安全危害監控機制	建立實體控制機制
未經授權的使用設備	欠缺一般的管理階層審查	建立管理階層審查機制
	欠缺通報安全弱點的程序	建立完整資通安全通報機制
使用偽造或複製的軟體	欠缺遵循智慧財產權規定的程序	建立軟體使用及控管機制

5.2.3事件發生機率與影響程度評估如下：

5.2.3.1 威脅的等級對應評估標準

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

5.2.3.2 弱點的等級對應評估標準

評估標準	評估值
該弱點不容易被威脅利用	1
該弱點容易被威脅利用	2
該弱點非常容易被威脅利用	3

5.2.4風險值的計算

評估威脅發生之可能性及弱點受到威脅利用之容易度，計算出風險值。

風險值=（資訊資產價值 × 威脅等級 × 弱點等級）

5.2.5事件風險權值對照

威脅等級（發生之可能性）		低(1)			中(2)			高(3)		
弱點等級（受到威脅利用之容易度）		低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	低(1)	中(2)	高(3)
資產價值	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36

5.3 風險管理

5.3.1可接受風險值的決定

5.3.1.1 資訊資產之可接受風險值，需經資通安全委員會開會決議，並記載於會議紀錄中。

5.3.1.2 資通安全委員會每年召開會議檢討可接受風險值。可接受風險必須考量組織環境及作業之安全需求,並進行適當地調整。

5.3.1.3 資通安全小組應針對高於可接受風險值項目，產出「風險評鑑彙整暨改善計劃表」作為風險管理之依據。

5.3.2選擇控制措施

5.3.2.1 超出可接受風險值之項目，應選擇適當之控管措施，並填寫「風險評鑑彙整暨改善計畫表」,說明風險控管措施之執行辦法。

5.3.2.2 「風險評鑑彙整暨改善計劃表」應陳報資通安全委員會開會審核，並列入追蹤管理程序。

5.3.3風險改善狀況的後續追蹤

5.3.3.1 資通安全小組應針對「風險評鑑彙整暨改善計劃表」彙整控管，持續追蹤至完成改善為止。

5.3.3.2 應於各項風險改善措施完成後，應進行風險再評鑑，以確保相關改善措施的有效性。

5.4 覆核

5.4.1監控

控制措施的實施必須建立相對應的指標或紀錄，以反應出控制措施實施的狀況及成效,便於管理階層及相關人員做定期或不定期審視。

5.4.2持續改善

為保持本風險評鑑方法之有效性與適用性，資通安全小組得定期檢

討可接受風險值與「威脅及弱點評估表」之項目。以期確保資訊資產均處於最佳保護之下，提供持續不中斷的營運。

5.4.3風險重新評鑑

5.4.3.1 每年應至少執行一次風險評鑑。

5.4.3.2 當有新增系統、系統有重大異動或作業環境改變時則應執行不定期之風險評鑑。

6 相關文件

6.1 資訊資產管理

6.2 威脅及弱點評估表

6.3 風險評鑑彙整暨改善計劃表

6.4 國立中興大學計算機及資訊網路中心之「資訊資產威脅及弱點評估表」：共同開發者為教育機構資安驗證中心、中興大學計算機及資訊網路中心、中興大學前瞻無所不在商務實驗室、屏東大學數位應用資訊安全實驗室、品科技（網址：https://sites.google.com/email.nchu.edu.tw/ssdlc/ra2）。

風險評鑑與管理					
文件編號	CHSH-ISMS-D-006	機密等級	一般	版次	3.0

威脅及弱點評估表

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級	弱點等級	風險值

風險評鑑與管理					
文件編號	CHSH-ISMS-D-006	機密等級	一般	版次	3.0

風險評鑑彙整暨改善計劃表

項次	資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值	風險改善建議措施	預計改善時間與處理方式	負責人員	風險再評估			
							威脅	弱點					資產價值	威脅等級	弱點等級	風險值