國立中科實驗高級中學

風險評鑑與管理

機密等級：限閱

文件編號：NEHS-ISMS-B-004

版　　次：1.0

發行日期：

風險評鑑與管理					
文件編號	NEHS-ISMS-B-004	機密等級	限閱	版次	1.0

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				初版

風險評鑑與管理					
文件編號	NEHS-ISMS-B-004	機密等級	限閱	版次	1.0

目錄

風險評鑑與管理					
文件編號	NEHS-ISMS-B-004	機密等級	限閱	版次	1.0

1 目的

建立 國立中科實驗高級中學（以下簡稱「本校」）資訊安全管理制度（以下簡稱 ISMS)風險評鑑與管理規範,提供本校資訊資產之權責單位、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，預防資訊安全事件之威脅。

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 資訊安全委員會：

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。

3.2 資訊安全小組：

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 資訊資產保管單位：

對於指定資訊資產，具有落實資訊資產權責單位所委託之保護管理責任。

3.5 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 事件發生機率與影響程度評估

5.2.2.1 依威脅的等級對應表（表 1）評估各事件之威脅等級：

表 1 威脅的等級對應表

評估標準	數值
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

5.2.2.2 依弱點的等級對應表（表 2）評估各事件之弱點等級：

表 2 弱點的等級對應表

評估標準	數值
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

5.2.3 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）

5.3 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，需經資訊安全委員會開會決議，並記載於會議紀錄中。

5.3.1.2 資訊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 資訊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，並產出「風險改善計畫表」，說明風險控管措施之執行辦法。

5.3.2.2「風險改善計畫表」應陳報資訊安全委員會開會審核，並列入追蹤管理程序。

5.3.2.3 資訊安全小組依據風險控管措施產出「適用性聲明書」。

5.3.3 風險改善狀況的後續追蹤

5.3.3.1 資訊安全小組應針對「風險改善計畫表」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，資訊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 1 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 資訊資產管理程序書

6.2 風險評鑑彙整表

6.3 風險改善計畫表

6.4 適用性聲明書

6.5 威脅及弱點評估表

7 附件

7.1 事件風險權值對照表

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