國立彰化高中110年資通安全教育訓練

報告人:國立彰化高中梁仕炘組長

資通安全管理法

- 總統107年6月6日公布資通安全管理法。

➢行政院107年11月21日發布相關子法:

- 資通安全管理法施行細則
- 資通安全責任等級分級辦法
- 資通安全事件通報及應變辦法
- 特定非公務機關資通安全維護計畫實施情形稽核辦法
- 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法

➢行政院107年12月05日函定自108年1月1日施行。

資通安全法令規定

- 資安法第十條

公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

資通安全法令規定

資安法第十二條

公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。

教育體系資安責任等級分級原則

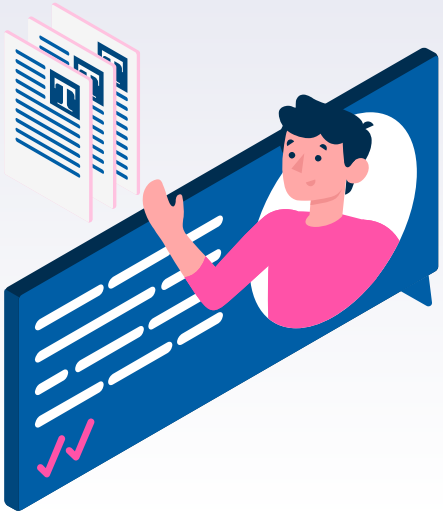
	A	B	C	D
業務個資	❖ 教育部 ❖ 承接敏感業務、研究學校	公立大專校院		
資通系統		❖ 國家教育研究院 ❖ 國家圖書館	❖ 部屬機構(電台、博 物館、圖書館) ❖ 國家運動訓練中心 ❖ 公立高級中等以下 學校(有核心資通系統)	公立高級中等以下學 校(已向上集中無維運 核心資通系統，無機 房或僅設置通訊機房
機關層級	大學附設醫院 (醫學中心)	大學附設醫院 (區域、地區醫院)		

*核心資通系統指依「資通安全管理法施行細則」第 7條第2項:

- ❖ 支持各校「核心業務」持續運作必要之系統。
- ❖ 依分級辦法附表九「資通系統防護需求分級原則」，資通系統判定其防護需求等級為高者。

應辦事項_D級、E級

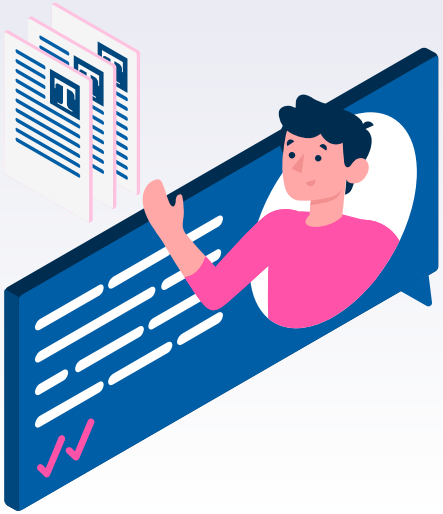
面向 / 作業名稱 / 等級	技術面	認知與訓練
	資通安全防護	資通安全教育訓練
D級	初次受核定或等級變更後之一年內，完成下列資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級 一、防毒軟體 二、網路防火牆 三、具有郵件伺服器者，應備電子郵件過濾機制	一般使用者及主管，每人每年至少接受三小時以上之一般資通安全教育訓練
E級		一般使用者及主管，每人每年至少接受三小時以上之一般資通安全教育訓練



教育部依據「資通安全責任等級分級辦法」第10條第4款，考量中小學資通系統之提供、維運、規模或性質相關之具體事項，調整核定等級。

責任等級		D+級	D級
認定原則	核心資通系統	2021年底前向上集中	已向上集中
	非核心資通系統	自行維運	已向上集中
	資通業務	自行辦理	自行辦理

摘錄自教育部資訊及科技教育司「資通安全管理法教育體系之法尊說明」108年6月11日簡報



教育部依據「資通安全責任等級分級辦法」第10條第4款，考量中小學資通系統之提供、維運、規模或性質相關之具體事項，調整核定等級。

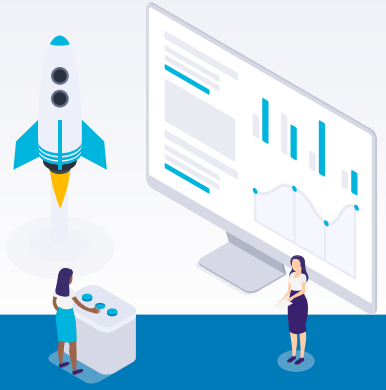
責任等級		D+級	D級
稽核健診	內部稽核	內部檢查	-
	資通安全健診	兩年一次	-
資安人員	配置	專責人員	-
	資安專業訓練	12小時/年	-

摘錄自教育部資訊及科技教育司「資通安全管理法教育體系之法尊說明」108年6月11日簡報

「國立彰化高中資通安全防護計畫」學校應配合辦理事項及作業時程

資訊及資產盤點作業

109年 4月 20日
～109年 5月 7日



核心資通系統向上集中

109年 8月 20日～
110年7月 31日

資安防護作業事項

109年 4月 20日～ 110年7月31日

校務行政系統 (或有師生個人資料的系統)

2021年底前需向上集中至台灣科技大學雲端

網域名稱系統(DNS)

DNS Server 已向上集中至國立成功大學

學校官方網站

WWW Serve r向上集中至成功大學(已更新網頁。預訂110年3月30日前)

電子郵件系統

本校使用Gmail 電子郵件帳號

若作公務信箱使用(建議機密資料加密)

學習歷程檔案系統

高中職使用國教署平台(本校已向上集中)

有明確區隔
(不得直接存取)

教育部資訊及科技教育司「資通安全管理法教育體系之法遵說明」108年6月11日簡報

非核心

- 校園廣播系統
- 影音相簿系統
- 電子看板系統
- 圖書管理系統
- 場地管理系統
- 監視系統
- 門禁系統
- 排課系統
- 差勤系統
- 教學檔案系統
- 薪資系統
- NAS系統
- AD系統
- 防毒系統
- DHCP系統

定期	校務系統資料庫定期備份置於不同儲存地點，敏感或機密性資訊備份應加密保護，至少保留3代。
定期	本校資訊中心負責完整備份config及data置於不同儲存地點，至少保留3代。
自動	國教署學習歷程平台的備份為國教署責任
自動	教育部雲端電子郵件系統的備份為教育部責任
定期	學校官方網站定期進行完整備份，至少保留3代。

1.5 是否定期執行重要資料之備份作業，且備份資料異地存放？存放處所環境是否符合實體安全防護？

定期

校務系統資料庫定期備份置於不同儲存地點，敏感或機密性資訊備份應加密保護，至少保留3代。

定期

本校資訊中心負責完整備份config及data置於不同儲存地點，至少保留3代。

備份頻率應滿足復原點目標 (RPO)之要求

每季於測試環境執行確認資料備份有效性

定期

學校官方網站定期進行完整備份，至少保留3代。

1.6 是否訂定備份資料之復原程序，且定期執行回復測試，以確保備份資料之有效性？復原程序是否定期檢討及修正？

校務行政系統 (或有師生個人資料的系統)
2021年底前需向上集中至台灣科技大學雲端

網域名稱系統(DNS)
DNS Server 已向上集中至國立成功大學

學校官方網站
WWW Serve r向上集中至成功大學(已更新網頁。預訂110年3月30日前)

電子郵件系統
本校使用Gmail 電子郵件帳號
若作公務信箱使用(建議機密資料加密)

學習歷程檔案系統
高中職使用國教署平台(本校已向上集中)

1.1 是否界定機關之核心業務，完成資通系統盤點分級，每年至少檢視1次分級妥適性？

資通系統防護作為

1 系統開發維護&委外

2 資訊/系統管理&健診

3 網路安全控管

4 資通安全防護設備

5 系統特權帳號管理

6 遠距工作安全措施

7 電腦機房門禁管理

8 電腦機房環境控制

資安防護組

全校同仁

1 系統通行碼管理

2 加密管理

3 防範惡意軟體措施

4 電子郵件安全管理

5 辦公室實體安全

6 媒體防護措施

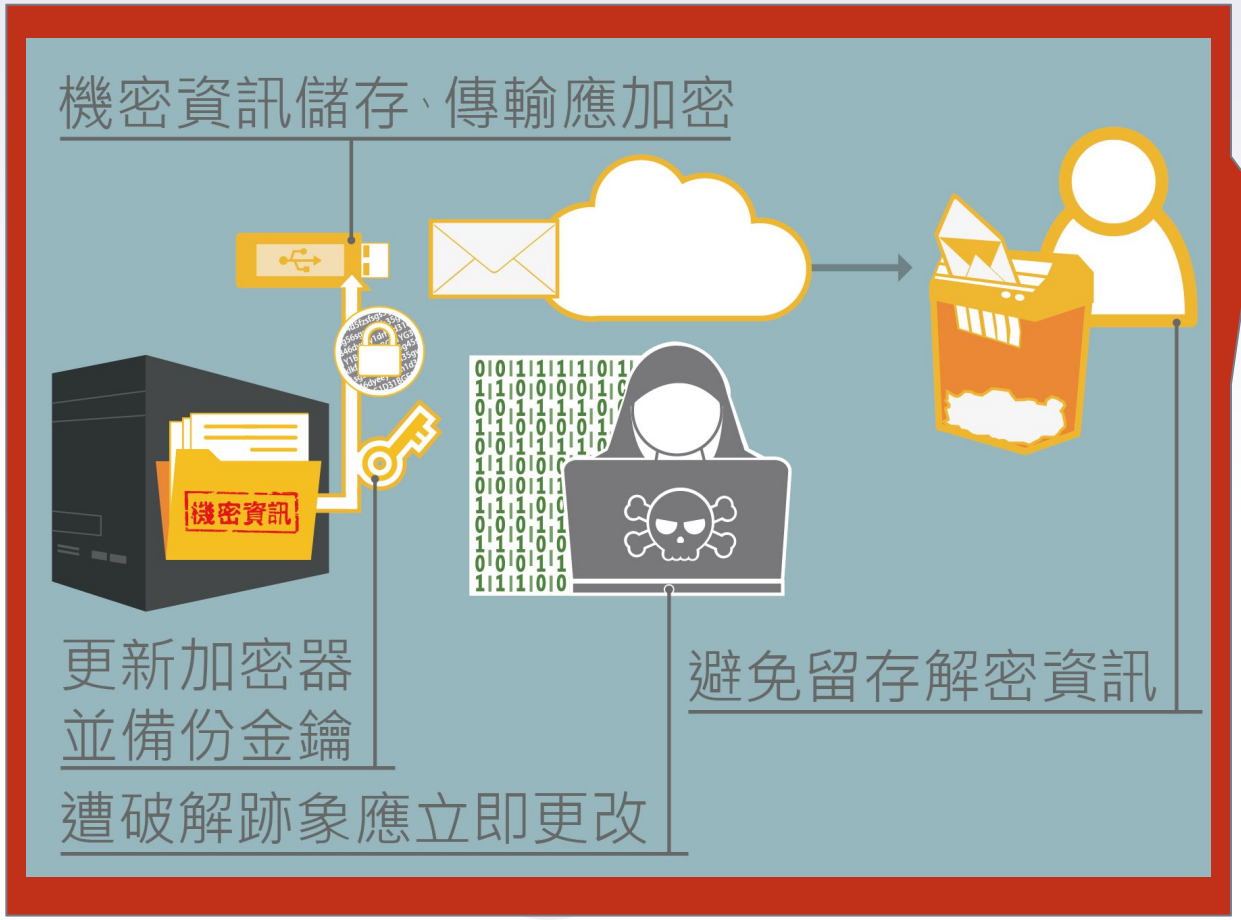
7 電腦使用安全管理

8 行動設備安全管理

1. 資通系統應設置通行碼管理，通行碼要求需滿足：
   (1)通行碼長度 8碼以上。
   (2)通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。
   (3)使用者每90 天應更換一次通行碼。

1 系統通行碼管理
2 加密管理
3 防範惡意軟體措施
4 電子郵件安全管理
5 辦公室實體安全
6 媒體防護措施
7 電腦使用安全管理
8 行動設備安全管理

1. 系統通行碼管理
2. 加密管理
3. 防範惡意軟體措施
4. 電子郵件安全管理
5. 辦公室實體安全
6. 媒體防護措施
7. 電腦使用安全管理
8. 行動設備安全管理



1. 系統通行碼管理
2. 加密管理
3. 防範惡意軟體措施
4. 電子郵件安全管理
5. 辦公室實體安全
6. 媒體防護措施
7. 電腦使用安全管理
8. 行動設備安全管理

1. 系統通行碼管理
2. 加密管理
3. 防範惡意軟體措施
4. 電子郵件安全管理
5. 辦公室實體安全
6. 媒體防護措施
7. 電腦使用安全管理
8. 行動設備安全管理

1. 系統通行碼管理
2. 加密管理
3. 防範惡意軟體措施
4. 電子郵件安全管理
5. 辦公室實體安全
6. 媒體防護措施
7. 電腦使用安全管理
8. 行動設備安全管理

1. 系統通行碼管理
2. 加密管理
3. 防範惡意軟體措施
4. 電子郵件安全管理
5. 辦公室實體安全
6. 媒體防護措施
7. 電腦使用安全管理
8. 行動設備安全管理

機敏資料與一般資料
分開儲存並妥善保管

實體媒體傳送應留意
包裝、人員、簽收

媒體劣化前重製保存

1 系統通行碼管理
2 加密管理
3 防範惡意軟體措施
4 電子郵件安全管理
5 辦公室實體安全
6 媒體防護措施
7 電腦使用安全管理
8 行動設備安全管理

1. 系統通行碼管理
2. 加密管理
3. 防範惡意軟體措施
4. 電子郵件安全管理
5. 辦公室實體安全
6. 媒體防護措施
7. 電腦使用安全管理
8. 行動設備安全管理

1. 系統通行碼管理
2. 加密管理
3. 防範惡意軟體措施
4. 電子郵件安全管理
5. 辦公室實體安全
6. 媒體防護措施
7. 電腦使用安全管理
8. 行動設備安全管理

- 系統開發維護&委外 1
- 資訊/系統管理&健診 2
- 網路安全控管 3
- 資通安全防護設備 4
- 系統特權帳號管理 5
- 遠距工作安全措施 6
- 電腦機房門禁管理 7
- 電腦機房環境控制 8

- 系統開發維護&委外 1
- 資訊/系統管理&健診 2
- 網路安全控管 3
- 資通安全防護設備 4
- 系統特權帳號管理 5
- 遠距工作安全措施 6
- 電腦機房門禁管理 7
- 電腦機房環境控制 8

資通安全健診	D+級
網路架構檢視	每二年辦理一次(預計於109年12月31日前依左列項目內容或採取經教育部認可之措施完成6項檢視及缺失改善)
網路惡意活動檢視	
使用者端電腦惡意活動檢視	
伺服器主機惡意活動檢視	
目錄伺服器設定檢視	
防火牆連線設定檢視	

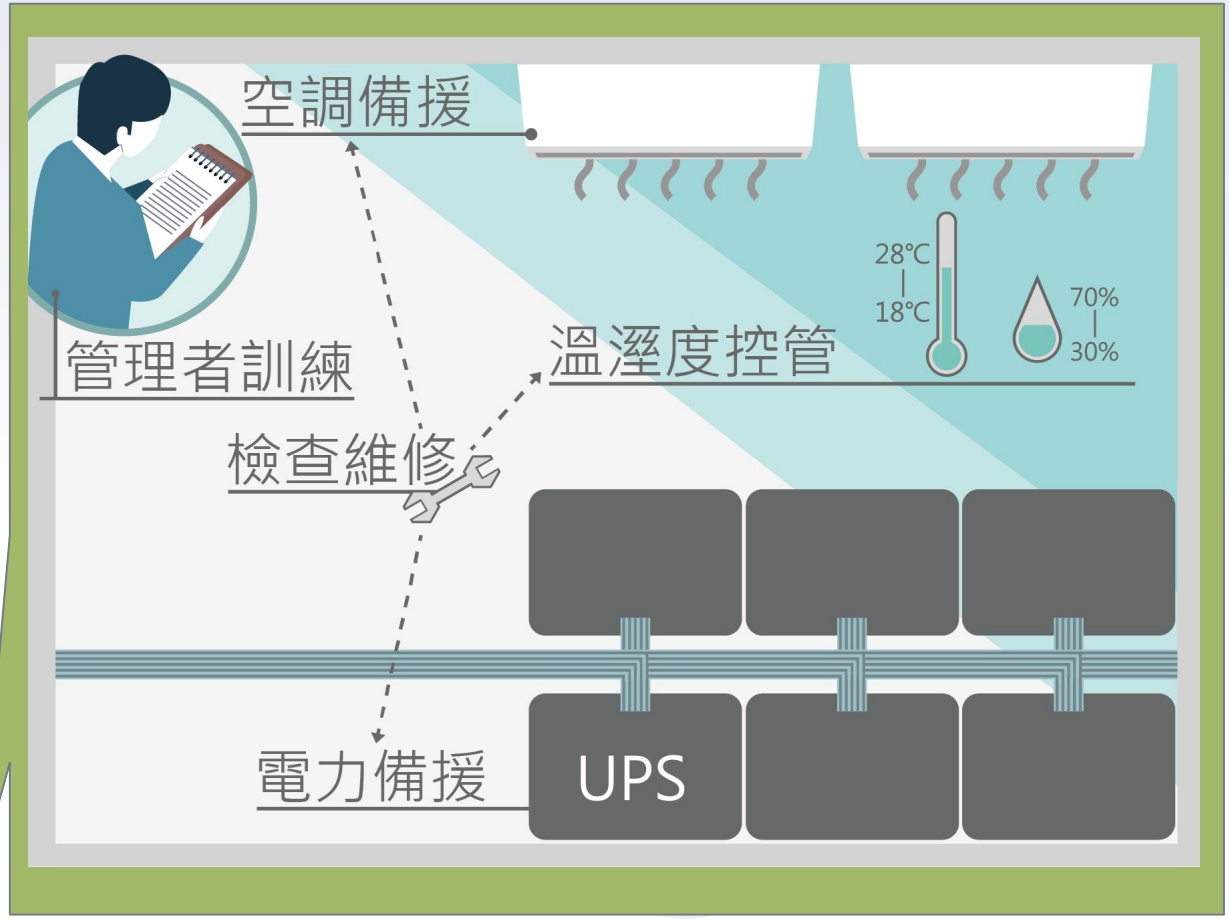
摘錄自「臺中市政府教育局所屬學校資通安全防護計畫」附表2

- 系統開發維護&委外 1
- 資訊/系統管理&健診 2
- 網路安全控管 3
- 資通安全防護設備 4
- 系統特權帳號管理 5
- 遠距工作安全措施 6
- 電腦機房門禁管理 7
- 電腦機房環境控制 8

1. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。
2. 對於通過防火牆之來源端 IP位址、目的端IP位址、來源通訊埠號、目的地通訊埠號、通訊協定、登入登出時間、存取時間及採取行動，均應確實記錄。
3. 內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。
4. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。
5. 遵循資通安全法暨臺灣學術網路管理規範。
6. 無線網路防護 (1)機密資料原則不得透過無線網路及設備存取、處理或傳送。(2)行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。(3)用以儲存傳輸資料且具無線傳輸功能之個人設備與工作站應安裝防毒軟體並定期更新病毒碼。

- 系統開發維護&委外 1
- 資訊/系統管理&健診 2
- 網路安全控管 3
- 資通安全防護設備 4
- 系統特權帳號管理 5
- 遠距工作安全措施 6
- 電腦機房門禁管理 7
- 電腦機房環境控制 8

1. 系統開發維護&委外
2. 資訊/系統管理&健診
3. 網路安全控管
4. 資通安全防護設備
5. 系統特權帳號管理
6. 遠距工作安全措施
7. 電腦機房門禁管理
8. 電腦機房環境控制



訂定

於「資訊安全維護計畫」明訂「資訊安全政策」

審核

每年召開「資通安全管理審查會議」審核

傳達

資安政策目標公開於網站上，傳達給全體人員包含正式、臨時、派遣人員，且在管審會後向利害關係人進行宣導。

2.1 是否訂定資通安全政策及目標，由管理階層核定，並定期檢視且有效傳達其重要性？

資通安全維護計畫及實施情形之持續精進及績效管理

資通安全維護計畫

訂定各階文件、流程、程序或控制措施，落實計畫之推動。

實施情形稽核機制

資通安全推動小組擬定資通安全稽核計畫並安排稽核成員，稽核人員應受適當培訓並具備稽核能力。

資通安全管理審會議

召開資通安全管理審查會議，確認資通安全維護計畫之實施情形。

持續改善機制

改善績效追蹤報告，相關記錄保存做為審查執行之證據。

2.2 是否訂定資通安全之績效評估方式(如績效指標等)，且定期監控、量測、分析及檢視？