# 臺南市市立白河國中(D級)

# 資訊安全線上評量報告書

製作日期：109 年 6 月 16 日

一、依據

教育部[cyear]年度提升校園資訊安全服務計畫之「教育機構個人資料保護工作事項」辦理。

二、目的

因應「個人資料保護法」實施、教育部「各級學校資通安全管理系統實施原則」、「教育部所屬機關及各級公私立學校資通安全工作事項」、本[unit]「各級學校資訊安全工作」及教育部年終視導等相關規定頒布，本局為了解各校資訊安全管理工作執行情形，特安排資訊安全稽核(內稽)及訪視作業，以協助各校建置資訊安全環境，落實資訊安全管理，以避免因疏忽而造成個人敏感性資料外洩，遭到不當利用而觸法，並使學校聲譽受損。

三、稽核項目

包含以下五大項，詳見「[county]政府教育局各學校資安訪視檢查表」。

(一)網路安全

(二)系統安全

(三)實體安全

(四)人員安全

(五)法令認知

四、稽核方式

第一階段：採學校自行內部稽核，相關資料請線上填報

由參與學校先依「[county]政府教育局各學校資安訪視檢查表」自評，於[filldate]期間，登入「全國高中職暨國中小學資訊安全管理平台（https://isas.moe.edu.tw）」填報，並上傳相關佐證資料，供本局作線上審查。

第二階段：線上審查

由本單位相關承辦人員及資安輔導顧問進行線上審查。

第三階段：實地訪視

線上審查完畢後，辦理3天到校資安訪視(日期另行通知)，由教育局及資安顧問組成資安訪視團，自受稽學校中抽出所進行到校訪查，確認線上審查項目落實程度。

五、稽核人員

陳、林、陳、李。

六、評定標準

訪視評定以「符合」、「部分符合」、「不符合」或「不適用」作為評比標準。

以下為評定標準定義：

(一)符合：

1.實際作業依照書面規範進行；紀錄及審核皆按照規定辦理。

2.已建立書面規範，但尚未有實際作業或紀錄。

(二)部分符合：

1.雖按照規範執行作業，但於過程中發生疏失或無相關書面紀錄。

2.作業流程尚有改善空間。

(三)不符合：

1.尚未規劃或執行相關安全管理規定。

2.違反自訂之管理規範。

3.違反教育部或本局之資安相關規範之要求。

(四)不適用：貴校之現行作業無相關作業需求。

## 七、審查結果優點與建議：

無資料

## 八、學校背景資料

| 序 | 項目內容 | 填答 |
|---|---|---|
| 01 | 貴校班級數(班) | 18 |
| 02 | 貴校資訊、資訊安全人力概況(不含委外人力)(人) | 1 |
| 03 | 貴校對外服務主機數量(台),包含實體主機、虛擬主機，不包含託管在教網的主機。 | 0 |
| 04 | 貴校行政電腦數量(台) | 22 |
| 05 | 貴校班級電腦數量(台) | 18 |
| 06 | 貴校電腦教室或專科教室用電腦數量(台) | 62 |
| 07 | 貴校可攜式設備(公發的手機 平板 筆電)數量(台) | 2 |
| 08 | 貴校對外連線頻寬(in/out，Mb) | 300 |
| 09 | 校內個人電腦是否使用網路位址的轉址(NAT，Network Address Translation)? | 否 |
| 10 | 貴校是否建置入侵偵測系統(IDS，Intrusion detection system)? | 是 |
| 11 | 貴校是否建置防火牆? | 是 |
| 12 | 貴校是否建置防毒機制 | 是 |
| 13 | 貴校是否建置郵件過濾機制? | 否 |
| 14 | 貴校重要的系統有哪些，請列出系統名稱 | 無 |
| | | |

| | | |
|---|---|---|
| 15 | 貴校教職員工人數(人) | 55 |

## 九、線上評量檢查表

受評量單位：白河國中　評量人員：鄭盛南　評量日期：108年10月23日
自評結果：88分　審查結果：86分

| 評量項目 | 自評 | 辦理情形 | 審查結果 | 執行現況或改善建議 |
|---|---|---|---|---|
| **一、核心業務及其重要性** | | | | |
| 01.依據資通安全維護計畫，學校應檢視校內資通業務及重要性盤點。 | 符合 | (無) | 符合 | 已提供維護計畫核心和非核心業務盤點部分截圖。 |
| **二、資通安全政策及目標** | | | | |
| 02.訂定學校資通安全政策及目標，並經校長簽核及公告。 | 符合 | (無) | 符合 | 已提供維護計畫整份文件(上有校長核章) |
| 03.定期召開資通安全管理審查會議，並檢視資安維護計畫實施情形及檢討資通安全政策。 | 符合 | (無) | 符合 | 已提供管審會會議紀錄或照片 |
| **三、設置資通安全推動組織** | | | | |
| 04.學校應設置資通安全管理長及資安推動小組，負責推動及執行資通安全相關業務。 | 符合 | (無) | 符合 | 已提供維護計畫中指派資安長或推動小組名單截圖。 |
| **四、人力及經費之配置** | | | | |
| 05.依據資通安全維護計畫，學校需設置資通安全人員，並鼓勵相關人員取得資安證照或參加相關教育訓練課程；並考量業務之需求分配資安或資訊相關經費。 | 符合 | (無) | 符合 | 已提供相關說明 |
| **五、資訊及資通系統之盤點及核心資通系統、相關資產之標示** | | | | |
| 06.依據資通安全維護計畫，學校應 | 符合 | (無) | 符合 | 已提供相關說明 |

| | | | | |
|---|---|---|---|---|
| 盤點資通訊系統，並完成安全等級分級防護基準評估。 | | | | |
| **六、資通安全風險評估** | | | | |
| 07.依據資通安全維護計畫，學校應完成資訊及資產相關之風險分析評估及處理；並將評估結果擬定因應控制措施。 | 符合 | (無) | 符合 | 已提供風險評鑑空白表 |
| **七、資通安全防護及控制措施** | | | | |
| 08.學校應檢視資通安全防護及控制措施，並完成「資通安全責任等級與分級辦法」要求之安全性檢測、資通安全健診及資通安全防護措施。 | 符合 | (無) | 符合 | 已上傳弱掃報告(集中式xoops) |
| 09.【網路控制措施】<br>(1)與外界連線，應僅限於經由教育局(處)網路管理單位之管控，以符合一致性與單一性之安全要求。<br>(2)宜依業務性質之不同，區分不同內部網路網段(如：教學、行政、宿網等)，以降低未經授權存取之風險。 | 符合 | (無) | 符合 | 已提供網路架構圖 |
| 10.【網路控制措施】<br>應禁止以私人架設網路（如：行動網路、電話線等）連結機房內之主機電腦或網路設備。<br>【無線網路存取】<br>應禁止使用者私自將無線網路存取設備介接至校園網路；若有介接之必要應經權責管理人員同意並設定帳號通行碼或加密金鑰以防未經許可之盜用。 | 符合 | (無) | 符合 | 已提供有關不能私接網路的截圖及公告畫面 |
| 11.【網路控制措施】<br>對於開放提供外部使用者或廠商存取之服務，必須限制使用者之來源IP及網路連線埠(Port)，以確保安全。 | 符合 | (無) | 符合 | 已提供學校開埠申請表 |
| 12.【無線網路存取】<br>校園內應提供無線網路存取服務，並採取適當安全管控措施：<br>(1)專供行政使用之無線網路熱點建議設定加密金鑰防護，避免使用開放 | 符合 | (無) | 符合 | 已提供wifi加密設定畫面或TN-Teacher連線設定畫面或TANetRoaming連 |

| | | | | |
|---|---|---|---|---|
| 之無線網路存取重要資訊系統及處理敏感性資料。<br>(2)教學區域、會議室等場所佈建之無線網路熱點應具有使用者身分認證機制，並經由校園無線路漫遊服務系統提供外校來賓使用。 | | | | 線登入畫面 |
| 13.(3)專供師生教學活動使用之無線網路熱點，若採用其他管理方式確有不便時，應採取限定開放時間及限制開放區域等管理措施，減少遭受不當利用之機會。 | 符合 | (無) | 符合 | 已提供無線網路管理辦法 |
| 14.(4)開放校外人士出入之公共空間可視需要提供民眾無線上網服務，其網段應與校園網路隔離，或委由網路服務業者提供。 | 符合 | (無) | 符合 | 已提供TANetRoaming連線登入畫面，及無線網路架構圖 |
| 15.【資訊存取限制】<br>共用的個人電腦（如：電腦教室電腦、教師休息室電腦等）應以特定功能為目的，並設定特定安全管控機制（如：限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。 | 符合 | (無) | 符合 | 已提供電腦上的使用者有一般使用者與最高權限使用者的畫面 |
| 16.【存取權限之移除或調整】<br>人員報到或離退職應會辦電腦系統帳號管理人員，執行電腦系統的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取，該作業應包括以下內容：<br>(1)使用唯一的使用者帳號。<br>(2)檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。<br>(3)保存一份包含所有帳號註冊的記錄 。<br>(4)使用者調職或離職後，應移除其帳號的存取權限。<br>(5)每學期應檢查使用者帳號，以確保帳號的有效性。 | 符合 | (無) | 符合 | 已提供帳號清查表 |
| 17.【特權管理】<br>電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄。 | 符合 | (無) | 符合 | 已提供特權帳號清單 |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 18.【設備區隔】<br>伺服器主機可依個別應用系統之需要，設置專屬主機，以避免未經授權之存取，(如:網路服務主機、電子郵件、網站主機等)、教學系統主機(如:隨選視訊主機等)。 | 符合 | (無) | 符合 | 已提供設備或機櫃標示照片 |
| 19.【對抗惡意軟體、隱密通道及特洛依木馬程式】<br>個人電腦應：<br>(1)裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理。<br>(2)作業系統及軟體應定期更新，以防範系統漏洞。 | 符合 | (無) | 符合 | 已提供更新截圖 |
| 20.【對抗惡意軟體、隱密通道及特洛依木馬程式】<br>個人電腦所使用的軟體應有授權。 | 符合 | (無) | 符合 | 已提供軟體授權證明 |
| 21.【對抗惡意軟體、隱密通道及特洛依木馬程式】<br>新伺服器系統啟用前，應執行相關程序(如：確認適合該作業系統之掃毒工具、預設通行碼更新、系統更新等)，並記錄於啟用與報廢紀錄單，以防範可能隱藏的病毒或後門程式。 | 符合 | (無) | 符合 | 已提供啟用與報廢紀錄 |
| 22.【資料備份】<br>系統管理人員需針對學校重要電腦系統及資料（如:系統檔案、網站、資料庫等）應定期(建議每週至少進行一次)備份工作；建議使用設備執行異地備份或使用外接式硬碟、隨身碟、光碟等執行或異地存放，並定期檢查備份資料之可用性與完整性。 | 符合 | (無) | 符合 | 已提供系統向上集中證明，由中心備份 |
| 23.【資訊工作日誌】<br>系統管理人員需針對重要電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之查核。 | 符合 | (無) | 符合 | 已提供資訊工作日誌 |
| 24.【資訊工作日誌】<br>系統管理人員應至少每季執行一次校時。 | 符合 | (無) | 符合 | 已提供系統校時設定畫面，同步時間至少在108/05以後(含) |

| | | | | |
|---|---|---|---|---|
| 25.【桌面淨空與螢幕淨空政策】<br>(1)個人辦公桌面應避免存放機敏性文件，結束工作時應妥善存放具有機密或敏感特性的資料（如:公文、學籍資料等）。<br>(2)個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及終端機安全，個人電腦應設定螢幕保護機制。 | 符合 | （無） | 符合 | 建議提供螢幕鎖定畫面 |
| 26.【通行碼之使用】<br>(1)管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。<br>(2)資訊系統與服務應避免使用共用帳號及通行碼。 | 符合 | （無） | 符合 | 已提供密碼設定畫面 |
| 27.【通行碼之使用】<br>由學校發佈通行碼制定與使用規則給使用者，內容應包含以下各項：<br>(1)使用者應該對其個人所持有通行碼盡保密責任。<br>(2)要求使用者的通行碼設定，應該包含英文字及數字，長度為8碼（含）以上。 | 符合 | （無） | 符合 | 已提供維護計畫中密碼規定截圖 |
| 28.【設備安置及保護】<br>主機機房及電腦教室宜設置偵煙、偵熱或滅火設備（氣體式滅火器），並禁止擺放易燃物或飲食。 | 符合 | （無） | 符合 | 已提供資訊機房偵煙、偵熱與滅火設備照片，及電腦教室標語或使用規定 |
| 29.【設備安置及保護】<br>主機機房及電腦教室的電源線插頭應有接地的連結（如:接地線、避雷針等）裝置，避免雷擊事件所造成設備損害情況。 | 符合 | （無） | 符合 | 已提供電源箱接地線、避雷針或凸波電源保護裝置照片 |
| 30.【設備安置及保護】<br>主機機房及電腦教室應實施門禁管制。 | 符合 | （無） | 符合 | 已提供主機機房及電腦教室區域門禁照片 |
| 31.【溫濕度控制】<br>重要的資訊設備（如：主機機房等）宜有溫濕度控制措施(溫度建議控制在20℃~25℃，濕度建議控制在相對濕度50%R.H.~70%R.H.)，以防止資 | 符合 | （無） | 符合 | 已提供機房內溫濕度顯示裝置照片 |

| | | | | |
|---|---|---|---|---|
| 訊設備意外損壞。機房內應有溫濕度顯示裝置，以觀察實際之溫濕度情況。 | | | | |
| 32.【電源供應保護】<br>重要的資訊設備（如:主機機房等）應有適當電力保護設施，如設置UPS、電源保護措施(如:穩壓器、接地線等)，以免斷電或過負載而造成損失，並設置緊急照明設備以作為停電照明之用。 | 符合 | (無) | 符合 | 已提供電力保護設施、緊急照明設備照片 |
| 33.【纜線安全】<br>主機機房及電腦教室內線路應考量設置保護設施(如：高架地板、線槽、套管等)。 | 符合 | (無) | 符合 | 已提供線路保護設施照片 |
| 34.【設備與儲存媒體之安全報廢或再使用】<br>所有包括儲存媒體的設備項目，在報廢前應填寫「啟用與報廢紀錄單」，確認已將任何敏感資料和授權軟體刪除或覆寫。 | 符合 | (無) | 符合 | 已提供啟用與報廢紀錄單 |
| 35.【財產攜出】<br>(1)禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。<br>(2)當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。 | 符合 | (無) | 符合 | 已提供設備進出紀錄表及登記歸還記錄 |
| 36.【設備安全管理】<br>公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應設定保護機制，如設定通行碼、圖形辨識、臉孔辨識或指紋辨識等；應執行安全相關程序(如：掃毒、預設通行碼更新、系統更新等)，以防範可能隱藏的病毒或後門程式。 | 符合 | (無) | 符合 | 已提供可攜式電腦設備(如:平板、筆電、手機等)螢幕鎖定，及防毒更新畫面 |
| 37.【設備安全管理】<br>公務用可攜式儲存媒體(如：隨身碟、光碟、磁帶等)應依儲存資料的機敏性實施安全控管措施，如檔案加密儲存或將該儲存媒體存放於上鎖儲櫃或安全處所。 | 符合 | (無) | 符合 | 已提供可攜式儲存媒體(如:隨身碟、光碟、外接式硬碟等)安全控管措施照片(如:上鎖儲櫃照 |

| | | | | |
|---|---|---|---|---|
| | | | | 片、檔案解密畫面等） |
| 38.【人員安全責任管理】<br>非正式人員、臨時人員，因業務需要，而接觸公務機密、個人權益及學校機敏資料者須填寫保密切結書。 | 符合 | （無） | 符合 | 已提供保密切結書 |
| **八、資通安全事件通報、應變及演練相關機制** | | | | |
| 39.依據資通安全維護計畫應建置資通安全事件通報、應變及演練等相關機制。學校已建立資訊安全事件（包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等）通報程序，通報程序包括學校內部通報，以及學校向教育機構通報平台通報。 | 符合 | （無） | 不符合 | 建議提供資安事件通報程序書(108資安法實施後的) |
| **九、資通安全情資之評估及因應機制** | | | | |
| 40.學校應檢視資通安全情資之評估及因應機制。 | 符合 | （無） | 符合 | 已提供學校的歷史通報畫面 |
| **十、資通系統或服務委外辦理之管理** | | | | |
| 41.1.資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密規定，應要求委外廠商簽訂安全保密切結書 。<br>2.委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結書。<br>3.委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限<br>4.依據資通安全維護計畫，學校如有資通系統或服務委外辦理之管理，應檢視委外廠商資通安全維護情形。 | 符合 | （無） | 符合 | 已提供廠商人員切結書等相關資料 |
| **十一、資通安全教育訓練** | | | | |
| 42.依據資通安全維護計畫，學校應辦理資訊安全教育訓練或宣導活動，提昇校園資訊安全認知能力。 | 符合 | （無） | 符合 | 已提供學校宣導照片，或講義及簽到表 |
| **十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制** | | | | |
| 43.依據資通安全維護計畫，相關人 | 符合 | （無） | 符合 | 已提供學校平時 |

| | | | | |
|---|---|---|---|---|
| 員辦理業務涉及資通安全應建立或列入考核機制。 | | | | 考核規定 |
| **十三、資通安全維護計畫及實施情形之持續精進及績效管理機制** | | | | |
| 44.依據資通安全維護計畫，提出資通安全維護計畫實施情形，對於不符合事項進行改善。 | 符合 | （無） | 符合 | 已提供資安維計畫實施情形（空白） |

本校受審查(稽核)後的發現事項，提出改善措施，並進行審核：

| |
|---|
| 第39.依據資通安全維護計畫應建置資通安全事件通報、應變及演練等相關機制。學校已建立資訊安全事件(包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等)通報程序，通報程序包括學校內部通報，以及學校向教育機構通報平台通報。 |

修正內容：

# 臺南市立白河國民中學

# 學校資通安全事件通報及應變管理程序

## 目錄

## 目的

臺南市立白河國民中學(以下簡稱本校)為遵照資通安全管理法第 14 條及本校資通安全維護計畫之規定，建立資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

## 適用範圍

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

## 責任

一、本校於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

二、本校應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本部進行通報，於完成事件之通報及應變程序後，依本校指示提供相關之紀錄或資料。

三、本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依教育部指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

## 事件通報窗口及緊急處理小組

一、臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構資安通報應變小組(簡稱通報應變小組)負責，聯繫資訊如下：

（一） 聯絡電話：(07)525-0211

（二） 網路電話：98400000

（三） 電子郵件：service@cert.tanet.edu.tw

二、本校應至少指派二位以上資安聯絡人員，並於「教育機構資安通報應變平台」(https://info.cert.tanet.edu.tw)登錄相關聯絡資料，如有異動亦應立即上網更新。

三、本校之資通安全事件通報窗口及聯繫專線為：

| 聯絡人姓名 | 職稱 | 電話 | E-mail |
|---|---|---|---|
| 黃郁珉 | 教務主任 | 06-6852067#101 | cuteamin@tn.edu.tw |
| 陳躍升 | 資訊組長 | 06-6852067#101 | musasa@tn.edu.tw |

四、本校應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

五、本校所屬人員知悉資通安全事件後，應立即至教育機構資安通報平台(https://info.cert.tanet.edu.tw)通報登錄資安事件細節、影響等級及支援申請等資訊。

六、本校應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

七、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

八、事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本校所屬分校或受託廠商所通報之資通安全事件時，亦同。

九、緊急處理小組成員由資通安全長指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

十、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

## 通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

本校之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。

2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。

3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。

4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。

5. 事件其他足以影響資通安全事件等級之因素。

(二)本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於確認資安事件條件成立後 1 小時內，與所隸屬區縣市網路中心及通報應變小組聯繫，先行提供該次資安事件應通報之內容及無法通報依規定方式通報之事由，並於事由解除後，依原方式補行通報。

(三)資通安全事件等級如有變更，本校權責人員或通報應變小組應告知通報單位，使其續行通報作業。

(四)本校於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向委託單位所屬之權責人員通知，以指定之方式進行通報。

(五)本校於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或通報應變小組應於知悉資通安全事件後一小時內，將該事件依教育部或行政院所指訂或認可之方式，通知該機關。

(六)本校執行通報應變作業時，得視情形向所隸屬區縣市網路中心人員提出技術支援或其他協助之需求。

## 應變程序

一、事件發生前之防護措施規劃

本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、損害控制機制

(一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1. 資安事件之衝擊及損害控制作業。
2. 資安事件所造成損害之復原作業。
3. 重大(第「三」級、第「四」級)資安事件相關鑑識及其他調查作業。
4. 重大(第「三」級、第「四」級)資安事件之調查與處理及改善報告之方式。
5. 重大(第「三」級、第「四」級)資安事件後續發展及與其他事件關聯性之監控。
6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。
7. 其他資通安全事件應變之相關事項。

(二)對於第一級、第二級資通安全事件，本校應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

(三)本校完成資安事件處理後，須至教育機構資安通報平台填報資安事件處理辦法及完成時間。

(四)本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

## 重大(第「三」級、第「四」級)資安事件後之復原、鑑識、調查及改善機制

一、本校若發生重大(第「三」級、第「四」級)資通安全事件時，於完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、重大(第「三」級、第「四」級)資通安全事件調查、處理及改善報告應包括以下項目：

(一)事件發生、完成損害控制或復原作業之時間。

(二)事件影響之範圍及損害評估。

(三)損害控制及復原作業之歷程。

(四)事件調查及處理作業之歷程。

(五)為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

(六)前款措施之預定完成時程及成效追蹤機制。

三、本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

## 紀錄留存及管理程序之調整

一、本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「教育機構資安通報平台」上填報完整之紀錄，該平台事件通報應變紀錄由通報應變小組於年度彙整後，提交至本部資訊及科技教育司覆核備查。

二、本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

## 演練作業

一、本校應配合教育部依資通安全事件通報應變辦法之規定所辦理之社交工程演練、資通安全事件通報及應變演練。

二、本校應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

(一)社交工程。

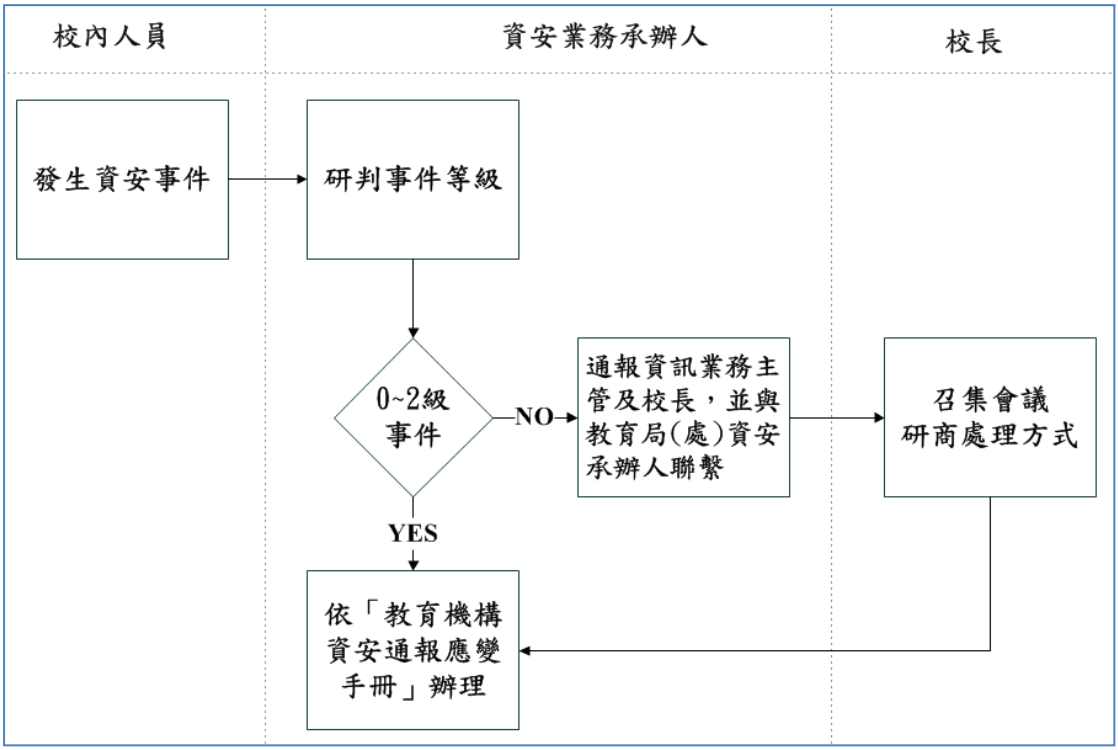
(二)資安事件通報及應變

(三)網路攻防

(四)情境演練

(五)其他資安演練

# 資安事件通報程序




| 人員 | 姓名 | 聯絡電話 |
|---|---|---|
| 資安業務承辦人 | **陳躍升** | **0932772958** |
| 資安業務主管 | **黃郁珉** | **0912737969** |
| 校長 | **于淑英** | **0937614211** |
| 教育局(處)資安承辦人 | **鄭盛男** | **(921)64095** |
| 臺灣學術網路危機處理中心(TACERT) | **略** | **07-5250211** |