105 學年度校園資訊安全業務說明

目錄

一、依據

1. 本市校園資訊安全業務依據為「個人資料保護法」、「個人資料保護法施行細則」、「教育機構個人資料保護工作事項」(附件 1)、**「政府機關（構）資通安全責任等級分級作業規定」(附件 2)**、「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」(附件 3)、**「教育體系資通安全暨個人資料管理規範」(附件 4)**、「國中、小學資通安全管理系統實施原則」(附件 5)、「教育機構資安通報應變手冊」(附件 6)、「台灣學術網路管理規範」(附件 7)及教育部之資安要求。
2. 其中**「政府機關（構）資通安全責任等級分級作業規定」**，規定學術機構中各學院、專科學校及高級中等以下學校，資安責任等級屬於 C 級，教育部再於**「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」**中將**「各公私立高級中等學校、各公私立國民中學、各公私立國民小學」**細分為 **C 級第二類學校**。

二、資訊安全責任等級分級作業

1. **C 級第二類學校**資訊安全管理及防護具體作法整理如下表：(詳參附件 3)

C 級第二類學校資訊安全管理及防護具體作法									
資訊系統分類分級	ISMS 推動作業	資安專責人力	稽核方式	業務持續運作演練	防護縱深	監控管理	安全性檢測	資安教育訓練(一般主管、資訊人員/資安人員、一般使用者	專業證照
核心業務如有建置資訊系統，可參考行政院國家資通安全會報頒訂之資訊系統分類分級與鑑別機制參考手冊，視資源能力，建置必要之防護基準。	對核心業務之應用資訊系統進行資訊資產清查，檢視可能之風險，並視資源能力實施適當之管控作為。	應指派一員兼任人員，執行資訊安全管理相關業務	結合機關內部管理機制，每年辦理一次資訊安全自我檢查作業。	對核心業務應用資訊系統依實務需要訂定業務持續運作計畫，並每年至少一次定期檢視計畫適用性。	由各直轄市及縣(市)教育網路中心於網路收容節點，設置防毒及防火牆設備，集中實施資安防護。	結合臺灣學術網路資安監控系統(北區 SOC、南區 SOC、Mini-SOC、TACERT)或本部資安監控系統機制，進行資安預警情資、事件通報及應變處置。	核心業務如有運用資訊系統(或網站)，於系統建置或更新時，或每年至少辦理一次資安弱點檢測作業，並對弱點進行修復作業。	(1)擔任資安業務人員應接受六小時資安專業課程訓練(包括行政院、教育部、各級教學機構、各區網中心及各直轄市及縣(市)教育網路中心等辦理之資安課程、訓練、講習等)，並獲得研習證明，以增進資安專業知識與能力。 (2)一般使用者及主管至少應接受三小時資安宣導課程(包括機關自辦資安宣導講習、上級機關辦理之資安宣導課程)，以提升資安防護認知。	擔任資安業務人員每年至少參加一項資安專業訓練，並取得上課證明。

2. 其中「稽核方式」於本文件「三、學校資通安全管理」說明，「防護縱深」及「安全性檢測」(含網站應用程式弱點掃描、防洩漏個資掃描)由本局統一建置各校配合執行，「監控管理」目前有教育部北區、南區與本局之 SOC 中心協助各校資安事件處理，「資安人員」與「專業證照」教育訓練部份本局將持續辦理，其餘一般主管及一般使用者教育訓練請各校自行辦理。

三、學校資通安全管理

1. 資通安全管理規範分級：
   (1)「高中職」-依據「教育體系資通安全暨個人資料管理規範」(適用範圍第二群)的要求作為資通安全管理規範。
   (2)「國中小」-依據「教育部國中、小學資通安全管理系統實施原則」的要求作為資通安全管理規範。

   各校依上述規範，推動校園「資訊安全管理制度(ISMS)」相關防護具體作法，落實執行相關的管控措施，以降低學校資訊安全的風險。
2. 規範導入範圍：

   各校實施資通安全管理規範時，全校以最高學部資安規範為實施標準，一校僅實施一種資安規範，無需針對多學部實施不同的資安要求。例如新北市立海山高級中學，雖有附設國中部，但全校仍以高中職資安規範為標準。
3. 稽核方式：
   (1)「高中職」-105 學年度請先進行紙本自評並留存佐證資料。未來將仿造「教育部全國國中、小學資訊安全管理系統」模式，進行線上自評及佐證資料上傳作業，屆時將再發文通知。
   (2)「國中小」-請於收到教育局函文後，登入「教育部全國國中、小學資訊安全管理系統」網站(https://isas.moe.edu.tw/)，將學校資通安全管理規範執行成果，進行線上自評及佐證資料上傳作業，執行年度各項資安作業時請參考「105 教育部全國國民中、小學資安評量項目及準備參考表」(附件 8)，保留相關記錄表單、活動照片，執行自我檢查作業(學校自評)，並配合教育部要求執行年度評核作業。
4. 其他說明請參閱「新北市政府教育局學校資訊安全稽核計畫」(附件 9)。

四、通報安全事件與處理

1. 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。
2. 各校資訊安全事件等級，由輕微至嚴重區分為 0-4 級。
3. 學校任何人於校內發現異常情況或疑似資安事件及應立即向資訊組長(教師)通報，資訊組長（教師）應儘速進行處理並研判事件等級。
4. 資訊組長（教師）當發生研判事件等級 2（含）以上之事件，應立即通報資訊業務主管及校長，並以電話聯絡新北市政府教育局資訊安全管理單位資安承辦人，由校長儘快召集會議研商處理的方式。
5. 當學校發生無法處理之資通安全事件，應通報新北市教育局資訊安全管理單位協助處理。

6. 教育機構資安通報平台（https://info.cert.tanet.edu.tw/），帳號為學校OID：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿，目前已將原OID如下表所示切分為5組，詳參「OID帳號分割作業說明」(附件10)。

OID帳號	OID帳號.1	OID帳號.2	OID帳號.3	OID帳號.4
密碼	密碼	密碼	密碼	密碼
第一聯絡人	第二聯絡人	第三聯絡人	第四聯絡人	第五聯絡人

7. 各校必須指派至少2位同仁擔任第1及第2聯絡人，負責處理該校資安通報業務，資訊組長(教師)預設應擔任第1聯絡人，其他聯絡人建議請資訊業務主管擔任。
8. 針對剩餘未使用之聯絡人帳號，請務必確實關閉。
9. 資安通報依情報來源分為「告知通報」與「自行通報」，若收到「告知通報」事件通知(簡訊及電子郵件)，由資訊組長（教師）登入「教育機構資安通報平台」，完成通報回覆作業及應變回覆作業。
10. 資安事件若為校內人員自行發現，由資訊組長（教師）登入教育機構資安通報平台進行「自行通報」完成通報回覆作業及應變回覆作業。
11. 資安事件須於發生後1小時內進行通報回覆，0、1、2 級事件於事件發生後72 小時內完成應變處理同時上網結案(包括通報與應變)， 3、4 級事件於事件發生後36 小時內完成應變處理同時上網結案(包括通報與應變)。
12. 如有收到教育機構資安通報平台「資安預警情報」事件郵件通知，由資訊組長(教師)登入「教育機構資安通報平台」，進行資安預警事件單處理作業。
13. 相關通報應變流程請依照「教育機構資安通報應變手冊第一版」(附件6)規定辦理。
14. **學校資安聯絡人接獲「告知通報」時，若因「課務」、「校外教學」、「補假」、「研習」、「生病」…等或各種因素無法處理時，請立即通知其他資安聯絡人上網填報回覆，或聯繫本局資訊安全業務承辦人員協助處理。**

五、資安通報演練

1. 教育機構資安演練平台(https://drill.cert.tanet.edu.tw/)-演練期間才開放。
2. 每年約在9-10月進行，105年期程及重點摘錄如下：

(1) 資料整備期：自學校收到公文起 至 9月 14日止。

(2) 資料整備期作業：

A. 請至教育機構資安通報平臺(https://info.cert.tanet.edu.tw)確認或修改第1及第2連絡人資料。

B. 變更第1及第2聯絡人密碼。

C. 第 3 至第 5 連絡人如未使用，請確實關閉帳號。

(3) 資安通報演練作業：本市學校為 105 年 9 月 19 日 至 9 月 23 日止。

(4) 演練採「告知通報」方式進行，以電子郵件及簡訊傳送「資安事件通知單」，並加註「告知通報演練」字樣，演練期間請注意手機簡訊及 E-mail 通知。

(5) 資料整備常見錯誤：

- 郵件地址：格式不符（如 abcde123@gmail.com.tw 、abcde123@YAHOO.COM.TW）。
- 手機號碼：未填、格式不符、資料不對。

3. 本市學校收到演練通報後，請儘速於 1 小時內至「教育機構通報演練平臺(https://drill.cert.tanet.edu.tw/)」完成通報及應變處理。
4. 其他事項請參考「105 年度教育部學術與部屬機關(構)分組資通安全通報演練計畫」(附件 11)。

六、弱點掃描

弱點掃描目前分為「網站主機系統弱點掃描」與「網站應用程式弱點掃描」，說明如下：

1. **「網站主機系統弱點掃描」**-目前統一由本局資安作業委外得標廠商執行，作業期程分為初掃及複掃兩階段，掃描方式主要是利用掃描工具程式，於中心架設掃描主機對各校掃描，以 port scan 的方式，對各校的校網主機作業系統進行網路 port 掃描，作業時以學校網址反查 IP 進行掃描，初掃結果通知學校進行修補作業，完成後再進行複掃。
2. **「網站應用程式弱點掃描」**-由本局建置弱掃系統各校配合執行掃描，主要針對 OWASP Top 10 中的 6 項(XSS、SQLInjection、備份檔案、目錄索引、惡意檔案執行、不適當配置管理)進行網站應用程式弱點掃描，掃描結果提供網站「**管理單位**」修補建議。網站應用程式弱點的攻擊，不同於網路主機系統弱點攻擊，是一種不當的網路行為，多利用 port80 進行，無法以傳統防火牆來阻擋。因此教育部委託成大資安團隊研發，於各縣市教育網路中心架設營運網站，採會員申請制，供轄下各級連線學校使用，各校可於該網站申請一組學校專用帳號，填寫目前管理者資料，以利將來交接及資料更新，**新北市教網營運點網址為 http://ewavs.ntpc.edu.tw/**。

七、防洩漏個資掃描

1. 因應「個人資料保護法」實施，教育部委託成大資安團隊研發「防洩漏個資掃瞄平台」，

於各縣市教育網路中心架設營運網站，供轄下各級連線學校使用，採會員申請制，目前由各校配合執行掃描。

2. 教育單位防洩漏個資掃瞄平台主要提供 TANet 連線單位申請網站個資掃瞄服務，協助各教育單位避免其網站之開放區域有洩漏個人資料的情事，以自動化方式掃瞄申請單位轄下之網站，分析其個資洩漏的狀態與風險，提升 TANet 個資防護水準。
3. 教育機構防洩漏個資掃瞄平台-新北市教網營運點網址 http://epdp.ntpc.edu.tw/。

八、SOC 作業

1. SOC 為一種集中式的安全監控機制，其目的在於整合並管理組織各種不同環境下的資安訊息，並且對安全事件做出對應的機制。
2. 成立 SOC 主要目的在於即時收集可能危害組織網路安全的的事件，加以整合及分析，並提出解決的方法，以確保組織單位網路安全。
3. 本市 SOC 系統登入、案件處理、監控儀表板使用等請參閱「學校 soc 使用操作教育訓練」(附件 12)。

九、防毒

1. **集中式防毒架構**

   本市防毒機制採集中式防毒架構，防毒軟體統一由教育局採購，供連線學校使用，希望經由集中式防毒整合服務中自動化管理更新機制，將最新的病毒碼、最新的掃毒引擎以最速簡的方式提供給市轄之公私立各級學校的電腦使用，做為校園電腦的基本安全防護，持續提供各級學校乾淨低病毒風險的資訊環境與可靠的病毒防禦機制。
2. **防毒軟體廠牌名稱**

   Trend Micro OfficeScan 產品全校授權。
3. **授權期限**

   4 年授權，自 104 年 10 月 25 日至 108 年 12 月 31 日止。
4. **學校端技術支援及服務**

   (1) 每所學校四年共 20 次 remote control service 遠端協助問題排除。
   (2) 提供原廠專屬客製化 Virus Clean Tool(VCT)解毒工具。
   (3) 得標廠商每年提供九大區，每區各二場，每場六小時之教育訓練，訓練場地由教育局安排，日期則由雙方另訂之。
   (4) 得標廠商提供專線電話支援。
   (5) 得標廠商提供專屬電子郵件技術服務。
   (6) 提供各校專屬諮詢網頁及管理系統。
   (7) 防毒管理 SOP，包含提供安裝步驟 SOP、解毒步驟 SOP。
5. **佈署方式**

校內電腦透過使用本局提供之「離線安裝檔」，安裝 Client 端防毒軟體完成佈署。離線安裝檔放置於全市資訊組長專用的 FTP(ftp://ftp.ntpc.edu.tw)內>伺服器軟體>Trend Micro Enterprise Solutions>各分區資料夾中。

病毒事件發生時，本局將主動通知學校，請資訊組長(教師)協助後續病毒清除作業。

6. **安裝使用注意事項**
   (1) 學校請在安裝防毒軟體之前先變更電腦名稱,於原電腦名稱前加上學校的 Domain Name，以供本局辨識與通知學校時使用。例如大觀國小內一部電腦原名稱為「教務處」則變更名稱為「tgps 教務處」，如有發現無法辨識之電腦，本局將由伺服器端逕行移除。
   (2) Client 端防毒軟體安裝後請立即重新啟動電腦，確認病毒碼及掃毒引擎已更新至最新版本，完成後立即開啟 Officescan 主控台執行完整掃描，此後防毒軟體系統將自動更新病毒碼、掃毒引擎、每週定期自動完整掃毒。
7. **本市防毒軟體安裝(用戶端)、專屬網頁管理系統使用操作等請參閱「學校防毒教育訓練」(附件 13)。**

十、咨詢電話

1. 教育研究發展科業務承辦人陳先生 電話：8072-3456 分機 506
2. 教育機構資安通報平台服務電話：(07)525-0211　網路電話：98400000
3. SOC 駐點工程師，電話 8072-3456 分機 534 王先生
4. 防毒聯絡人：張宏銘先生 公司電話：25984299 分機 512 行動電話：0953606229
5. 趨勢科技防毒客服電話：2377-2323#1(請表明為新北市 OO 學校即可尋求協助)

十一、資訊安全業務相關網站

1. **教育部全國國中小學資訊安全管理系統(https://isas.moe.edu.tw/)**
2. **教育機構資安通報平台(https://info.cert.tanet.edu.tw/)**
3. **教育機構資安演練平台(https://drill.cert.tanet.edu.tw/)**
4. **教育機構網站應用程式弱點監測平台-新北市教網營運點(http://ewavs.ntpc.edu.tw/)**
5. **教育機構防洩漏個資掃瞄平台-新北市教網營運點(http://epdp.ntpc.edu.tw/)**
6. **教育部校園資訊安全服務網(http://cissnet.edu.tw/)**
7. **TACERT 臺灣學術網路危機處理中心(http://cert.tanet.edu.tw/)**
8. **國家資通安全會報技術服務中心 (http://www.icst.org.tw/)**
9. **新北市教育研究發展科_資訊教育股(http://enctc.ntpc.edu.tw/)資訊安全網頁**