# 臺北市立復興高級中學資通安全維護計畫附件

# 目錄

**1.** 資通安全推動小組成員及分工表

# 臺北市立復興高級中學資通安全推動小組成員及分工表

編號：

製表日期：　　年　　月　　日

| 單位職級 | 名稱 | 職掌事項 | 分機 | 備註 |
|---|---|---|---|---|
| 校長 | | 綜理資通安全核定與督導 | 100 | 資通安全長 |
| 秘書 | | 資通安全事務協調 | 101 | 資安策略規劃與管理組 |
| 教務處主任 | | 學生學習歷程系統成績資料安全與維護 | 200 | 資安策略規劃與管理組 |
| 學務處主任 | | 校務行政系統學生出缺勤、獎懲紀錄資料安全與維護 | 300 | 資安通報防護組 |
| 總務處主任 | | 資通安全設備招標採購 | 400 | 資安通報防護組 |
| 輔導室主任 | | 學生學習歷程系統學生進路輔導資料安全與維護 | 500 | 資安策略規劃與管理組 |
| 圖書館主任 | | 資通安全事務協調 | 600 | 資安通報防護組 |
| 系統管理師 | | 擬定資通安全維護計畫 | 641 | 資安策略規劃與管理組 |
| 系統管理師 | | 資通安全事件通報 | 611 | 資安通報防護組 |
| 主任教官 | | 進行資通安全教育宣導 | 550 | 資安策略規劃與管理組 |
| 人事室主任 | | 差勤系統安全與維護，協助資通安全人員獎勵事宜 | 700 | 資安通報防護組 |
| 會計室主任 | | 協助資通安全預算編列與核銷 | 777 | 資安策略規劃與管理組 |
| 一年級級導師 | | 進行一年級學生資通安全宣導 | | 資安策略規劃與管理組 |
| 二年級級導師 | | 進行二年級學生資通安全宣導 | | 資安策略規劃與管理組 |
| 三年級級導師 | | 進行三年級學生資通安全宣導 | | 資安策略規劃與管理組 |

資通安全長[1]： 校長

註：陳核層級請機關依需求調整

[1] 特定非公務機關部分，可能是資通安全管理代表等相關資通安全負責人。

**2.** 資通安全保密同意書

# 臺北市立復興高級中學資通安全保密同意書

編號：

立同意書人＿＿＿＿＿＿於民國＿＿＿＿年＿＿　月＿＿＿　日起於＿＿＿＿＿＿＿＿＿＿任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。

二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。

三、遵守其他本單位資通安全相關之法令及規定。

四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：＿＿＿＿＿＿＿＿（簽章）

身份證字號：＿＿＿＿＿＿＿＿

服務機關：＿＿＿＿＿＿＿＿

機關首長：＿＿＿＿＿＿＿＿

中　　華　　民　　國　　年　　月　　日

**3.** 資通安全需求申請單

# 臺北市立復興高級中學資通安全需求申請單

編號：

| | | | |
|---|---|---|---|
| 申請單位 | （處室） | 申請日期 | 年　　月　　日 |
| 申請項目 | □軟體<br>□硬體<br>□其他 | 項目名稱 | |
| 申請數量 | 1 | 需用日期 | 年　　月　　日 |
| 申請類別 | □新購<br>□升級 | 使用設備 | □主機<br>□使用者電腦<br>□其他 |
| 安裝單位 | | 安裝位置 | |
| 用途說明 | | | |
| 申請人 | | 單位主管 | |
| 資通安全推動小組 | □可採購<br>□不可採購 | 說明： | |
| 資通安全推動小組承辦人員 | | 資通安全長[2] | |

註：陳核層級請機關依需求調整

[2] 特定非公務機關部分，可能是資通安全管理代表等相關資通安全負責人。

**4.** 資訊及資通資產清冊

(事涉敏感資訊僅提供空白表格，清冊同本校財產及軟體管理清冊，人員同附件1)

# 臺北市立復興高級中學資訊及資通資產清冊

| 資產編號 | 資產名稱 | 資產類別 | 擁有單位 | 保管單位 | 使用單位 | 存置地點 | 防護需求 |
|---|---|---|---|---|---|---|---|
| 例:107-IF-01 | 行政業務檔案 | IF | 資訊組 | 資訊組 | 資訊組 | 教務處 | 普 |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

資產類別：IF(資訊) 、SW(軟體)、HW(硬體)、SE(服務)、PE(人員)、PI(個資)

**5.** 風險評估表

# 臺北市立復興高級中學風險評估表

編號：

製表日期：　　年　　月　　日

| 風險列表 | 風險評估 | | | | 發生可能性 | 影響後果 | 風險等級 | 管理機制 |
|---|---|---|---|---|---|---|---|---|
| | 機密性 | 完整性 | 可用性 | 法律遵循性 | | | | |
| EX：電力中斷 | | V | V | | 高度：一年發生○次以上；或風險雖未曾發生但發生可能性極高。中度：一年發生○次以上；或風險雖未曾發生但有可能發生。低度：一年發生○次以上；或風險雖未曾發生但發生可能性極低。 | 高：對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。中：對機關之營運、資產或信譽等方面將產生嚴重之影響。普：對機關之營運、資產或信譽等方面將產生有限之影響。 | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

承辦人員：　　單位主管：

**6.** 風險類型暨風險對策參考表

# 臺北市立復興高級中學風險類型暨風險對策參考表

| 作業內容 | 具體風險類型 | 風險處理對策（建議，例示非列舉） |
|---|---|---|
| 網際網路探尋 | 網頁搜尋 | 強化網頁伺服器，避免存放 index.html、default.asp 的檔案資料夾，並禁用相關的目錄索引。使用 robots.txt 指示搜尋引擎不要為其內容編制索引。 |
| | WHOIS 查詢 | 在 WHOIS 資料庫及 TLS 憑證中，使用平常、單一的網路管理人聯絡資訊，以降低社交工程與撥號攻擊的成功率。 |
| | DNS 查詢 | 設定 DNS 伺服器，禁止其對不可信任的主機執行區域轉送，並主動從網際網路掃描 TCP 和 UDP 的端口 53，以便發現是否有偽冒的名稱伺服器。刪減 DNS 區域檔案內容，以防洩漏不必要的訊息，例如非公開的 IP 位址和主機名稱，並且於必要時才使用 PTR 紀錄。 |
| | SMTP 探尋 | 設定 SMTP 伺服器在遇到問題時，例如寄件人不存在時，不要發送 NDN，以防攻擊者藉機列舉內部郵件系統及組態內容。 |
| 區域網路攻擊 | MITM 和偽冒伺服器攻擊 | 強制採用傳輸層安全加秘與透過具有憑證檢驗功能的身份驗證機制 |
| | 802.1X 攻擊 | ●檢測 X.509 憑證是否有效。<br>●指定合法驗證者（RADIUS 伺服器）之一般名稱值。<br>●在安全功能發生問題時，禁止提供詳細資訊給終端使用者，以提高故障安全性。 |
| | 資料連結層攻擊 | ●將交換連接埠設為 access 模式，並關閉動態建立主幹網路的功能。<br>●關閉未用到的乙太網路連接埠，並歸類在隔離的 VLAN 外。 |
| | 網路層與應用層的攻擊 | ●如果沒有明確要求，應關閉 IPv6。<br>●取消對 ICMP 重導向的支援。<br>●停用群播名稱解析及 Windows 的 NetBIOS over TCP/IP 通訊。 |
| 網路服務漏洞 | 網路攻擊表面 | 將不必要的功能關閉。 |
| | 伺服器套件包與程式庫攻擊 | 隨時修補存在攻擊表面的已知攻擊。 |
| | 透過傳輸與遠端維護操作之服務進行攻擊 | ●停用無加密傳輸安全性的 Telnet、FTP、SNMP、VNC 等。<br>●遠端操作維護須透過安全的身份驗證連接。<br>●建構封閉的管理網路。 |
| | SSH 伺服器攻擊 | ●強制使用 2.0 版本的協定，禁止向下相容特性。<br>●停用使用者的密碼驗證機制，強制使用者採取一次性密碼（OTP）、公鑰或多因子驗證，例如可透過 Google Authenticator、Duo Security 或其他平台取得。 |
| | DNS 伺服器攻擊 | ●停止支援來自不受信任來源的遞回查詢。<br>●確保區域檔案不含多餘或敏感資訊。 |

| | | |
|---|---|---|
| | Kerberos 伺服器攻擊 | 停止支援較弱的 HMAC 演算法。<br>●在微軟環境中，可考慮強制使用最高的網域功能等級。 |
| VPN 服務 | VPN 攻擊 | ●確認 VPN 伺服器的維護作業，並修補到最新版本。<br>●強制使用 AH 和 ESP 功能身份驗證及機密性服務。<br>●使用數位憑證取代預置共享金鑰，並要求對設備進行身份驗證。<br>●過濾內連的 VPN 流量，以便在發生入侵事件時限制網路存取。<br>●定期稽核已授權的 VPN 使用者，以防有偽冒的帳號。 |
| 網頁應用程式框架 | Web 應用伺服器攻擊 | ●確保應用程式框架組件都已修補至最新版本，包括相依與間接使用的組件。<br>●禁止將管理介面或特權功能公開在不受信任的網路上。<br>●在可行的情況下，將開放網頁應用程式和管理功能隔離。 |
| 資料儲存機制 | 資料庫攻擊 | ●限制資料服務只與經授權的對象往來，特別是雲端環境中。<br>●避免使用不支援身份驗證的儲存系統和協定。<br>●禁止在可公開讀取的儲存裝置，例如 NFS、iSCSI、SMB 和 AFP 等，以未加密狀態儲存機敏資料，包括系統和資料庫的備份檔案通常存有機敏資料，例如密碼、身份憑證。<br>●確保密碼強度。<br>●限制只有受信任的網路才能存取管理服務。<br>●稽查和監控身份驗證事件，識別濫用身份憑據和暴力拆解密碼的情形。 |
| 參考來源：資安風險評估指南，第三版，Chris McNab，江湖海譯。 | | |

**7.** 管制區域人員進出登記表

# 臺北市立復興高級中學管制區域人員進出登記表

編號：

製表日期：　　年　　月　　日

| 編號 | 姓名 | 單位 | 陪同人員 | 日期 | 進入時間 | 離開時間 | 事由 | 權限 | 進出設備 | 攜帶物品 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

承辦人員：　　單位主管：

註：陳核層級請機關依需求調整

**8.** 委外廠商執行人員保密切結書、保密同意書

# 臺北市立復興高級中學委外廠商執行人員保密切結書

立切結書人----------（簽署人姓名）等，受----------（廠商名稱）委派至----------（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。

二、 未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、 經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、 廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。

五、 機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、 本保密切結書不因立切結書人離職而失效。

七、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

| 姓名及簽章 | 身分證字號 | 聯絡電話及戶籍地址 |
| --- | --- | --- |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

立切結書人所屬廠商：

| 廠商名稱及蓋章 | 廠商負責人姓名及簽章 | 廠商聯絡電話及地址 |
| --- | --- | --- |
| | | |

填表說明：

一、廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。

二、廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中　華　民　國　　年　　月　　日

# 臺北市立復興高級中學委外廠商執行人員保密同意書

茲緣於簽署人 ----------（簽署人姓名，以下稱簽署人）參與----------（廠商名稱，以下稱廠商）得標----------（機關名稱）（以下稱機關）資通業務委外案----------（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條 簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。

第二條 簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第三條 簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第四條 簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第五條 簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第六條 本同意書一式叁份，機關、簽署人及----------（廠商）各執存一份。

簽署人姓名及簽章：
身分證字號：
聯絡電話：
戶籍地址：
所屬廠商名稱及蓋章：
所屬廠商負責人姓名及簽章：
所屬廠商地址：
中　華　民　國　　年　　月　　日

**9.** 委外廠商查核項目表

# 臺北市立復興高級中學委外廠商查核項目表

編號：

填表日期：　　年　　月　　日

查核人員：

| 查核項目 | 查核內容 | 查核結果 | | | 說明 |
|---|---|---|---|---|---|
| | | 符合 | 不符合 | 不適用 | |
| 1. 資通安全政策之推動及目標訂定 | 1.1 是否定義符合組織需要之資通安全政策及目標？ | □ | □ | □ | 已訂定資通安全政策及目標。 |
| | 1.2 組織是否訂定資通安全政策及目標？ | □ | □ | □ | 政策及目標符合機關之需求。 |
| | 1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？ | □ | □ | □ | 依規定按時進行教育訓練之宣達。 |
| | 1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？ | □ | □ | □ | 定期進行政策及目標之檢視、調整。 |
| | 1.5 是否隨時公告資通安全相關訊息？ | □ | □ | □ | 將資安訊息公告於布告欄。 |
| 2. 設置資通安全推動組織 | 2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？ | □ | □ | □ | 指派首長擔任資安長。 |
| | 2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？ | □ | □ | □ | 有設置內部資通安全推動小組，並制訂相關之權責分工。 |
| | 2.3 是否訂定組織之資通安全責任分工？ | □ | □ | □ | 機關內部訂有資安責任分工組織。 |
| 3. 配置適當之資通安全專業人員及適當之資源 | 3.1 是否訂定人員之安全評估措施？ | □ | □ | □ | 有訂定人員錄用之安全評估措施 |
| | 3.2 是否符合組織之需求配置專業資安人力？ | □ | □ | □ | 機關依規定配置資通安全兼辦人員1人。 |

| 查核項目 | 查核內容 | 查核結果 | | | 說明 |
|---|---|---|---|---|---|
| | | 符合 | 不符合 | 不適用 | |
| | 3.3 是否具備相關專業資安證照或認證？ | □ | □ | □ | 專業人員具備ISO27001之證照。D級單位不適用。 |
| | 3.4 是否配置適當之資源？ | □ | □ | □ | 機關並未投入足夠資安資源。 |
| 4. 資訊及資通系統之盤點及風險評估 | 4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？ | □ | □ | □ | 依規定建置資產目錄，並定時盤點。 |
| | 4.2 各項資產是否有明確之管理單位及使用單位？ | □ | □ | □ | 資產依規定指定管理單位及使用單位。 |
| | 4.3 是否定有資訊、資通系統分級與處理之相關規範？ | □ | □ | □ | 資訊訂有分級處理之作業規範。 |
| | 4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？ | □ | □ | □ | 已進行風險評估及擬定相應之控制措施。 |
| 5. 資通安全管理措施之實施情況 | 5.1 人員進入重要實體區域是否訂有安全控制措施？ | □ | □ | □ | 機房訂有門禁管制措施。 |
| | 5.2 重要實體區域的進出權利是否定期審查並更新？ | □ | □ | □ | 離職人員之權限未刪除。 |
| | 5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？ | □ | □ | □ | 對於進出人員並未監督其活動。 |
| | 5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？ | □ | □ | □ | 按時檢測機房物理面之情況。 |
| | 5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？ | □ | □ | □ | 依規定定期檢查並按時提供同仁安全設備之使用運練。 |
| | 5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？ | □ | □ | □ | 並未陪同或監視第三方支援人員。 |
| | 5.7 重要資訊處理設施是否有特別保護機制？ | □ | □ | □ | 對於核心系統主機並未設置特別保護機制。 |
| | 5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？ | □ | □ | □ | 定期檢查物理面之風險。 |

| 查核項目 | 查核內容 | 查核結果 | | | 說明 |
|---|---|---|---|---|---|
| | | 符合 | 不符合 | 不適用 | |
| | 5.9 電源之供應及備援電源是否作安全上考量？ | □ | □ | □ | 有設置備用電源。 |
| | 5.10 通訊線路及電纜線是否作安全保護措施？ | □ | □ | □ | 電纜線老舊，並未設有安全保護措施。 |
| | 5.11 設備是否定期維護，以確保其可用性及完整性？ | □ | □ | □ | 設備按期維護。 |
| | 5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？ | □ | □ | □ | 訂有相關之保護措施。 |
| | 5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)? | □ | □ | □ | 攜帶式設備訂有保護措施。 |
| | 5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？ | □ | □ | □ | 設備報廢前均有進行資料清除程序。 |
| | 5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？ | □ | □ | □ | 人員下班後並未將機敏性公文妥善存放。 |
| | 5.16 系統開發測試及正式作業是否區隔在不同之作業環境？ | □ | □ | □ | 系統開發測試與正式作業區隔。 |
| | 5.17 是否全面使用防毒軟體並即時更新病毒碼？ | □ | □ | □ | 按時更新病毒碼。 |
| | 5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？ | □ | □ | □ | 定期進行相關系統之病毒掃瞄。 |
| | 5.19 是否定期執行各項系統漏洞修補程式？ | □ | □ | □ | 定期進行漏洞修補。 |
| | 5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)? | □ | □ | □ | 系統設有檢查之機制。 |
| | 5.21 重要的資料及軟體是否定期作備份處理？ | □ | □ | □ | 有定期做備份處理。 |
| | 5.22 備份資料是否定期回復測試，以確保備份資料之有效性？ | □ | □ | □ | 備份資料均有測試。 |
| | 5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？ | □ | □ | □ | 均有設加密之保護措施。 |
| | 5.24 是否訂定可攜式媒體(光碟片、隨身碟、隨身硬碟及報表等)管理程序？ | □ | □ | □ | 訂有可攜式媒體之管理程序。 |
| | 5.25 是否訂定使用者存取權限註冊及註銷之作業程序？ | □ | □ | □ | 訂有使用者存取權限註冊及註銷之作業程序。 |

| 查核項目 | 查核內容 | 查核結果 | | | 說明 |
|---|---|---|---|---|---|
| | | 符合 | 不符合 | 不適用 | |
| | 5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？ | □ | □ | □ | 未定期檢視使用者存取權限。 |
| | 5.27 通行碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？ | □ | □ | □ | 通行碼符合規定。 |
| | 5.28 通行碼是否規定需有大小寫字母、數字及符號組成？ | □ | □ | □ | 通行碼符合規定。 |
| | 5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？ | □ | □ | □ | 依規定訂定適當之存取權限。 |
| | 5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？ | □ | □ | □ | 對於特定網路有訂定相關之控制措施。 |
| | 5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？ | □ | □ | □ | 有針對行動式電腦訂定管理政策。 |
| | 5.32 重要系統是否使用憑證作為身份認證？ | □ | □ | □ | 針對重要系統設有身份認證。 |
| | 5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？ | □ | □ | □ | 系統更新後相關措施仍有效。 |
| | 5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？ | □ | □ | □ | 可即時取得系統弱點並採取應變措施。 |
| 6. 訂定資通安全事件通報及應變之程序及機制 | 5.1 是否建立資通安全事件發生之通報應變程序？ | □ | □ | □ | 有訂定通報應變程序。 |
| | 5.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？ | □ | □ | □ | 同仁及委外廠商均知悉通報應變程序，並定期宣導。 |
| | 5.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？ | □ | □ | □ | 有留存相關紀錄。 |
| 7. 定期辦理資通安全認知宣導及教育訓練 | 7.1 是否定期辦理資通安全認知宣導？ | □ | □ | □ | 有定期辦理宣導。 |
| | 7.2 是否對同仁進行資安評量？ | □ | □ | □ | 按期進行資安評量。 |
| | 7.3 同仁是否依層級定期舉辦資通安全教育訓練？ | □ | □ | □ | 有定期辦理教育訓練。 |
| | 7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？ | □ | □ | □ | 同仁均瞭解單位之資通安全政策及目標。 |
| 8. 資通安全維護 | 8.1 是否設有稽核機制？ | □ | □ | □ | 訂有稽核機制。 |

| 查核項目 | 查核內容 | 查核結果 | | | 說明 |
|---|---|---|---|---|---|
| | | 符合 | 不符合 | 不適用 | |
| 計畫實施情形之精進改善機制 | 8.2 是否定有年度稽核計畫？ | □ | □ | □ | 有訂定年度稽核計畫。 |
| | 8.3 是否定期執行稽核？ | □ | □ | □ | 有按期執行稽核。 |
| | 8.4 是否改正稽核之缺失？ | □ | □ | □ | 訂有稽核後之缺失改正措施。 |
| 9. 資通安全維護計畫及實施情形之績效管考機制 | 10.1 是否訂定安全維護計畫持續改善機制？ | □ | □ | □ | 有訂定持續改善措施。 |
| | 10.2 是否追蹤過去缺失之改善情形？ | □ | □ | □ | 有追蹤缺失改善之情形。 |
| | 10.3 是否定期召開持續改善之管理審查會議？ | □ | □ | □ | 定期召開管理審查會議。 |

單位主管：　　資通安全長[3]：

註：陳核層級請機關依需求調整

[3] 特定非公務機關部分，可能是其資安代表，或單位之資安負責人員。

**10.** 年度資通安全教育訓練計畫

**臺北市立復興高級中學**　　年度資通安全教育訓練計畫

壹、依據

臺北市立復興高級中學之資通安全維護計畫辦理。

貳、目的

為精進所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行本校之資通安全維護計畫，以強化本校之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

參、實施範圍

本校所屬人員：

| 人員類別 | 人數 |
|---|---|
| 資通安全專責人員 | |
| 一般行政人員<br>(含約聘僱) | |
| 主管人員 | |
| 教師 | |
| 共計 | |

肆、訓練項目

| 人員類別 | 訓練課程[4] | 時數 |
|---|---|---|
| 例：<br>資通安全專責人員 | | |
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | | |

[4] 可參考行政院國家資通安全會報技術服務中心之資安職能課程項目，網址：https://www.nccst.nat.gov.tw/Capacity?lang=zh

伍、訓練期程

由本校自行排定教育訓練期程。

陸、訓練方式

由本校自行依課程內容，採取合宜教育訓練方式(實體課程、線上課程…)。

**11.** 資通安全認知宣導及教育訓練簽到表

# 臺北市立復興高級中學資通安全認知宣導及教育訓練簽到表

編號：

課程名稱：_____

時　　間：

地　　點：_____

| 單　位 | 職　稱 | 姓　名 | 簽　名 |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**12.** 資通安全維護計畫實施情形

# 臺北市立復興高級中學資通安全維護計畫實施情形

編號：

本校之業務因涉及全國性民眾個人資料檔案之持有及處理，經主管機關核定後本單位之資通安全責任等級為 D 級 ，依資通安全管理法第 12 條之規定，向 鈞局 提出本（107）年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

| 實施項目 | 實施內容 | 實施情形說明 |
|---|---|---|
| 1. 核心業務及其重要性 | 1.1 核心業務及重要性盤點 | 本校無須維護。 |
| 2. 資通安全政策及目標之訂定 | 2.1 資通安全政策訂定及核定 | 本校已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定(詳公文附件)。 |
| | 2.2 資通安全目標之訂定 | 本校已訂定資通安全目標，詳參資通安全維護計畫。 |
| | 2.3 資通安全政策及目標宣導 | 本校為推動資通安全政策，已定期向同仁及利害關係人進行宣達。 |
| | 2.4 資通安全政策及目標定期檢視 | 本校已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性（詳會議記錄）。 |
| 3. 設置資通安全推動組織 | 3.1 設定資通安全長 | 本校已指定校長為資通安全長，其職掌詳參資通安全維護計畫。 |
| | 3.2 設置資通安全推動小組 | 本校已設置資通安全推動小組，其組織、分工及職常詳參資通安全維護計畫。 |
| 4. 專責人力及經費之配置 | 4.1 專職(責)人員配置 | 本校依規定配置資通安全兼任人員1人。另因其業務內容將涉及機密性資料，故已進行相關安全評估。 |

| | | |
|---|---|---|
| | 4.2 經費之配置 | 本校今年視需求已合理分資安經費，資安經費佔資訊經費之　　%。 |
| 5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示 | 5.1 資訊及資通系統之盤點 | 本校已於今年　　月盤點本校之資訊、資通系統，建立資產目錄。 |
| | 5.2 機關資通安全責任等級分級 | 本校依資通安全責任等級分級辦法，為資通安全責任等級 D 級機關。 |
| 6. 資通安全風險評估 | 6.1 資通安全風險評估 | 本校已於今年　　月完成本校之資訊、資通系統及相關資產之風險分析評估及處理。 |
| | 6.2 資通安全風險之因應 | 本校已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。 |
| 7. 資通安全防護及控制措施 | 7.1 資訊及通系統之保管 | 本校已依安全維護計畫辦理，詳附件資料。(以下為未導入 CNS27001 機關之範例) |
| | 7.2 存取控制與加密機制管理 | 本校已依安全維護計畫辦理。 |
| | 7.3 作業及通訊安全管理 | 本校已依安全維護計畫辦理。 |
| | 7.4 系統獲取、開發及維護 | 本校已依安全維護計畫辦理。 |
| | 7.5 執行資通安全健診 | 本校已依安全維護計畫辦理。 |
| 8. 資通安全事件通報、應變及演練相關機制 | 8.1 訂定資通安全事件通報、應變及演練相關機制 | 本校已依規定訂定資通安全事件通報應變程序。(詳附件) |
| | 8.2 資通安全事件通報、應變及演練 | 本校已依規定進行資通安全事件通報。<br>本校已依規定於今年◯月辦理社交工程演練，並於◯月辦理通報應變演練。 |
| 9. 資通安全情資之評估及因應機制 | 9.1 資通安全情資之分類評估 | 本校接受情資後，已進行分類評估。 |
| | 9.2 資通安全情資之因應措施 | 本校已接受情資之分類，採取對應之因應措施。 |

| | | |
|---|---|---|
| 10. 資通系統或服務委外辦理之管理 | 10.1 選任受託者應注意事項 | 本校資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。 |
| | 10.2 監督受託者資通安全維護情形應注意事項 | 本校已依規定監督受託者資通安全維護情形，客製化資通系統開發者，已要求其出具安全性檢測證明。 |
| 11. 資通安全教育訓練 | 11.1 資通安全教育訓練要求 | 本校人員已規定進行資通安全教育訓練。 |
| | 11.2 辦理資通安全教育訓練 | 本校已於今年○月辦理資通安全教育訓練。 |
| 12. 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 | 12.1 訂定考核機制並進行考核 | 本校已建立考核機制，並已依規定進行平時及年終考核。 |
| 13. 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 | 13.1 資通安全維護計畫之實施 | 本校已依規定訂定各階文件、流程、程序或控制措施，據以實施並保存相關之執行成果記錄。 |
| | 13.2 資通安全維護計畫實施情形之稽核機制 | 本校已依規定辦理內部稽核。 |
| | 13.3 資通安全維護計畫之持續精進及績效管理 | 本校已依規定辦理內部召開管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。 |
| 其他說明 | | |

單位主管：　　資通安全長：

註：陳核層級請機關依需求調整

**13.** 資通安全稽核計畫

# 臺北市立復興高級中學　年度資通安全稽核計畫

壹、依據

一、本校之資通安全維護計畫辦理。

二、資通安全管理法第十三條規定辦理。

貳、目的

為瞭解本校資通安全維護計畫執行之有效性，爰擬定本稽核計畫，執行稽核作業。

參、稽核期程

（各機關自行定義）

由各機關自行排定稽核期程。

肆、稽核團隊成員

（各機關自行定義）

由各機關自行考量稽核之需求，邀請具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識之公務機關代表或專家學者，稽核團隊人數原則為 3 至 7 人。

伍、稽核範圍

（各機關自行定義）

全機關

陸、稽核項目及內容

（各機關自行定義）

依據各機關安全維護之內容，並參考國際資訊安全管理標準 ISO 27001:2013、國際資訊技術服務管理標準 ISO 20000、「個人資料保護法」、「個人資料保護法施行細則」、「政府機關(構)資通安全責任等級分級作業規定」或「資訊系統分級與資安防護基準作業規定」等，以及其他相關規定，由各機關自行定義當年度之稽核項目、內容及執行方式。

一、核心業務及其重要性：(內容由各機關自行定義)

二、資通安全政策及目標：(內容由各機關自行定義)

[5] 各機關可依執行稽核之類別填列適當之依據。

三、資通安全推動組織：(內容由各機關自行定義)

四、專責人力及經費之配置：(內容由各機關自行定義)

五、公務機關資通安全長之配置：(內容由各機關自行定義)

六、資訊及資通系統之盤點，並標示核心資通系統及相關資產：(內容由各機關自行定義)

七、資通安全風險評估：(內容由各機關自行定義)

八、資通安全防護及控制措施：(內容由各機關自行定義)

九、資通安全事件通報、應變及演練相關機制：(內容由各機關自行定義)

十、資通安全情資之評估及因應機制：(內容由各機關自行定義)

十一、資通系統或服務委外辦理之管理措施：(內容由各機關自行定義)

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：(內容由各機關自行定義)

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：(內容由各機關自行定義)

柒、改善作業

(各機關自行定義)

由各機關自行評估對於稽核結果表現優良者是否給予行政獎勵，並針對缺失或待改善項目者研擬後續追蹤方式及頻率(如將前次稽核結果納入本次稽核範圍中追蹤辦理情形及進度)。

**14.** 稽核項目表

# 臺北市立復興高級中學稽核項目表

編號：

製表日期：○○○年○○月○○日

預計稽核日期：○○○年○○月○○日

稽核標準：本校資通安全維護計畫

| 受稽核單位 | 稽核項目 | 稽核項目 | 稽核時程 | 稽核方式 |
|---|---|---|---|---|
| EX：<br>圖書館 | 依據：本校資通安全維護計畫<br>稽核範圍：資訊資產 | 資訊及資通系統資產 | 每年 | 資料查閱 |
| EX：<br>總務處 | 依據：本校資通安全維護計畫<br>稽核範圍：機房 | 實體環境安全 | 每半年 | 資料查閱 |
| EX：<br>人事室 | 依據：本校資通安全維護計畫<br>稽核範圍：業務系統 | 權限存取 | 每月 | 抽樣檢查 |

**15.** 稽核結果紀錄表

# 臺北市立復興高級中學稽核結果紀錄表

編號：

稽核日期：○○○年○○月○○日

稽核範圍：全機關

| 受稽核單位 | 稽核項目 | 稽核結果 | 備註 |
|---|---|---|---|
| EX：總務處 | 資產盤點 | □符合<br>□不符合<br>□不適用 | 經驗證其資產項目表，按規定進行資產盤點，各項資產均依規定建檔並指派責任人。 |
| EX：人事室 | 權限控管 | □符合<br>□不符合<br>□不適用 | 可使用高權限登入 A 網站，提供一般同仁進行課程報到作業外，亦可查詢所有同仁之個人資料。 |
| | | □符合<br>□不符合<br>□不適用 | |
| | | □符合<br>□不符合<br>□不適用 | |
| | | □符合<br>□不符合<br>□不適用 | |
| | | □符合<br>□不符合<br>□不適用 | |
| 附註 | | | |
| 受稽核人員： | | | 受稽核單位主管： |

註：陳核層級請機關依需求調整

**16.** 稽核委員聘任同意暨保密切結書

# 臺北市立復興高級中學○○○(計畫名稱)
# 稽核委員聘任同意暨保密切結書

本人_____（以下簡稱甲方）為協助臺北市立復興高級中學（以下簡稱乙方）執行「○○○」（以下簡稱本計畫），接受乙方之邀請，擔任 108 年資安稽核團隊之稽核委員，特立書同意事項如下：

一、 甲方應遵守國家機密保護法、個人資料保護法、行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、著作權法及其他相關法令之規定，並對因執行本計畫或因執行本計畫之機會所知悉之機密資訊負有保密義務；且上開各義務不因甲方與乙方或與技服中心間，就本年度擔任稽核委員相關事宜之法律關係解除、終止或完成而失其效力。

二、 甲方就因執行本計畫或因執行本計畫之機會，所知悉或接觸之乙方、受稽機關或其他第三人之機密資訊，除因執行本計畫所必須，且事先經乙方書面同意者，或法律另有明文規定外，不得有下列行為：

（一）全部或一部重製或留存上開機密資訊；

（二）以任何方式向任何第三人揭露上開機密資訊之全部或一部；

（三）以任何方式使任何第三人知悉、持有或使用上開機密資訊之全部或一部；

（四）以任何方式使自己或任何第三人就上開機密資訊之全部或一部取得任何權利；

（五）揭露、公開或使用上開機密資訊之全部或一部。

三、 甲方因執行本計畫所製作之報告、文件或其他產出，其智慧財產權及其他權利均歸屬乙方所有。

四、 甲方與受稽機關有下列情形之一者，就與該受稽機關之稽核相關事宜，應主動迴避，或事先以書面告知乙方，以確認是否得免予迴避：

（一）甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人，與受稽機關間，有財產上或非財產上利益之利害關係者。

（二）甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬，與受稽機關或其負責人間現有或於過去兩年間曾有僱傭、承攬、委任、代理或其他類似之關係者。

（三）甲方或其現任職或於過去兩年內曾任職之機關，於民國 105 年至本次稽核期間，曾為受稽機關進行與受稽事項相關之顧問輔導者。

五、 前條所稱財產上利益，係指動產、不動產、現金、有價證券、債權、其他財產上權

利、具有經濟價值或得以金錢交易取得之利益；所稱非財產上利益，係指有利於甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人於受稽機關或其關聯機關之任用、陞遷、調動及其他人事措施。

六、 有其他情形足認甲方有不能公正執行職務之虞，經受稽機關敘明理由，並由乙方作成迴避決定者，甲方應迴避之。

七、 甲方有第四條各款情形之一，而未自行迴避，亦未事先以書面告知乙方相關情事，並經乙方書面同意免予迴避者，乙方得終止本契約，甲方應返還已收取之報酬，如乙方， 因此認有必要對受稽核機關重為全部或一部稽核，或受有其他不利益時，甲方並應賠償乙方因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

八、 甲方如違反第二條或就相關事宜涉及其他不法情事，將移送司法機關處理；如致乙方、受稽機關，遭受任何不利益，或受第三人法律上請求或訴追者，甲方應賠償乙方、受稽機關，因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

九、 甲方應公正執行職務，並應避免使人誤認推薦特定廠商、產品或服務；且處理稽核相關事務或出席會議，應親自為之。

此　致

臺北市立復興高級中學

立 同 意 書 人

姓　　名：　　（簽章）

身 份 證 字 號：

中 華 民 國　　年　　月　　日

**17.** 稽核結果及改善報告

# 臺北市立復興高級中學稽核結果及改善報告

| 稽核範圍 | | | | |
|---|---|---|---|---|
| 稽核日期 | | | | |
| 審查日期 | | | | |
| 改善措施 | | | | |
| 編號 | 稽核缺失或待改善稽核項目 | 改善措施 | 改善期程規劃 | 相關證明資料 |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |

單位主管：　　資通安全長：

註：陳核層級請機關依需求調整

**18.** 改善績效追蹤報告

# 臺北市立復興高級中學改善績效追蹤報告

編號：

製表日期：

| 稽核發現 | | | |
|---|---|---|---|
| 稽核日期 | | 受稽核單位 | |
| 稽核區域 | | | |
| 缺失或待改善項目與內容 | | | |
| 影響範圍評估 | | | |
| 發生原因分析 | | | |
| 改善措施成效追蹤 | | | |
| 改善措施 | | 預計成效 | 執行情況 |
| 管理面 | | | |
| 技術面 | | | |

| | | | |
|---|---|---|---|
| | | | |
| 人力面 | | | |
| 資源面 | | | |
| 作業程序 | | | |
| 其他 | | | |
| 績效管考 | | | |
| 改善措施確認 | | | |
| 經費需求或編列執行金額 | | 經費執行情形 | |
| 預定完成日期 | | 實際完成日期 | |
| 完成進度或情形說明 | | | |
| 改善成效考核 | | | |
| 後續成效追蹤 | | | |
| 資通安全推動小組 | | 資通安全長[6] | |

註：陳核層級請機關依需求調整

[6] 特定非公務機關部分，可能是資通安全管理代表等相關資通安全負責人。