

臺北市立第一女子高級中學

資通安全維護計畫

第 2.0 版

生效日期：114 年 3 月 20 日

文件制／修訂紀錄表

文件版本	生效日期	制／修定摘要說明	承辦單位	承辦人
V1.0	108年1月19日	初次建立，108年1月18日本校資通安全推動小組會議通過	資訊組	黃芳蘭
V1.1	109年5月11日	修訂資通安全長姓名；新增附件十五、臺北市立第一女子高級中學稽核結果及改善報告；新增附件十六、臺北市立第一女子高級中學改善績效追蹤報告。	資訊組	張清俊
V1.2	111年10月27日	刪除校內非核心業務主機兩台(www、國語文學科中心虛擬主機已經向上集中至臺北市政府教育局機房)	資訊組	楊喻文
V1.3	112年10月11日	修訂第十三條第一項資通安全教育訓練要求；修訂附件一、臺北市立第一女子高級中學資訊安全推動小組成員及分工表。	資訊組	楊喻文
V2.0	114年3月20日	依北市教資字第1133102825號函，參酌臺北市政府教育局訂定所屬各級學校資通安全維護計畫範本，修訂本校資通安全維護計畫。	資訊組	楊喻文

資通安全長：陳智源校長

壹、實施計畫

一、依據及目的：本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。本計畫依據下列法規訂定：

- (一) 資通安全管理法第 10 條及其施行細則第 6 條。
- (二) 臺北市政府資通安全管理規定。

二、適用範圍：本計畫適用範圍涵蓋本校各單位。

三、核心業務及重要性

(一) 核心業務及重要性：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
教務：負責課程教學、學籍管理、實驗研究、教學設備與特教等業務	無	■ 為本機關依組織法職掌，足認為重要者	學校教學業務無法運作	8 小時
學務：負責學生活動、生活輔導、生活教育、衛生保健及體育活動等業務	無	■ 為本機關依組織法職掌，足認為重要者	學校學生事務業務無法運作	8 小時
總務：負責校內公物維修管理、校舍及財產管理、環境綠美化、校園安全計畫、公文及檔案管理、出納管理等業務	無	■ 為本機關依組織法職掌，足認為重要者	學校總務業務無法運作	8 小時
輔導：負責增進學生心理健康、生涯適性發展等業務	無	■ 為本機關依組織法職掌，足認為重要者	學校輔導業務無法運作	8 小時
圖書館：負責服務推廣、資訊業務推展活動等業務	無	■ 為本機關依組織法職掌，足認為重要者	學校圖書館業務無法運作	8 小時

(二) 非核心業務及說明：對本校之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
人事：辦理人事管理業務	人事業務無法運作	24 小時

會計：辦理歲計、會計等業務	會計業務無法運作	24 小時
---------------	----------	-------

四、資通安全政策及目標

(一) 依「臺北市政府資通安全管理規定」壹、總則各規定辦理。

(二) 資通安全政策

為使本學業務順利運作，防止資訊或資通業務受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性 (Confidentiality)、完整性 (Integrity) 及可用性 (Availability)，特制訂本政策如下，以供全體同仁共同遵循：

1. 定期因應內外資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 針對各資料的機密性與完整性應妥善保護，避免資料遭竄改。
3. 建立資通安全防護 (如:防火牆、防毒軟體)。
4. 辦理資通安全教育訓練 (一般使用者與主管，每人每年 3 小時以上之一般資通安全教育訓練)，提升同仁資通安全意識。
5. 禁止多人共用同一帳號。
6. 落實資通安全通報機制。

(三) 本校量化型目標

1. 資安事件發生，於規定的時間完成通報、應變及復原作業。
2. 資通安全研習完成率達 50%。

(四) 資通安全政策及目標核定程序：資通安全政策由資通安全推動小組會議通過簽請校長核定後實施，修正時亦同。

(五) 資通安全政策及目標之宣導：本校之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向學校內所有人員進行宣導。

(六) 資通安全政策及目標定期檢討程序：資通安全政策及目標應定期於資通安全推動小組會議 (得與資訊教育推動小組會議合併召開) 中檢討其適切性。

五、資通安全推動組織

(一) 資通安全長

依本法第 11 條之規定，本校訂定校長為資通安全長，負責督導學校資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。
2. 資通安全責任之分配及協調。
3. 資通安全資源分配。

- 4.資通安全防護措施之監督。
- 5.資通安全事件之檢討及監督。
- 6.資通安全相關規章與程序、制度文件核定。
- 7.資通安全管理年度工作計畫之核定。
- 8.資通安全相關工作事項督導及績效管理。
- 9.其他資通安全事項之核定。

(二) 資通安全推動小組：

1.組織

為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各處室主任以上之人員代表成立資通安全推動小組，其任務包括：

- (1) 跨處室資通安全事項權責分工之協調。
- (2) 應採用之資通安全技術、方法及程序之協調研議。
- (3) 整體資通安全措施之協調研議。
- (4) 資通安全計畫之協調研議。
- (5) 其他重要資通安全事項之協調研議。

2.分工及職掌

本校之資通安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本校資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

(1) 策略規劃組

- (a) 資通安全政策及目標之研議。
- (b) 訂定學校資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。
- (c) 依據資通安全目標擬定學校年度工作計畫。
- (d) 傳達學校資通安全政策與目標。
- (e) 其他資通安全事項之規劃。

(2) 資安防護組

- (a) 資通安全技術之研究、建置及評估相關事項。
- (b) 資通安全相關規章與程序、制度之執行。
- (c) 資訊及資通系統之盤點及風險評估。
- (d) 資料及資通系統之安全防護事項之執行。

(e) 資通安全事件之通報及應變機制之執行。

(f) 其他資通安全事項之辦理與推動。

六、專責人力及經費配置

(一) 專責人力及資源配置

- 1.本校依資通安全責任等級分級辦法之規定，屬資通安全責任等級D級，無需設置資通安全專職人員，惟本校仍設置3人負責處理資訊安全業務，現有資通安全人員名單及職掌應列冊，並適時更新。
- 2.本校之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升學校內資通安全業務人員之資通安全管理能力。本校之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業學校(構)提供顧問諮詢服務。
- 3.本校負責重要資通設備之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。
- 4.本校之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。
- 5.專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

(二) 經費配置

- 1.資通安全推動小組於規劃配置相關經費及資源時，應考量本校之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。
- 2.各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。
- 3.本校如有資通安全資源之需求，應配合學校預算規劃期程向資通安全推動小組提出，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。
- 4.資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

七、資訊及資通系統之盤點

(一) 資訊及資通系統盤點

- 1.依「臺北市政府資通訊資產及電子資料安全作業指引」及「臺北市政府使用物聯網安全作業指引」各規定辦理。

2.本校每年度應依資訊及資通系統盤點結果，並落實填報管考系統。

(二) 學校資通安全責任等級分級：本校自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D 級。

八、資通安全風險評估

依「臺北市政府資通訊資產及電子資料安全作業指引」各規定辦理。

九、資通安全防護及控制措施

本校依據資通安全風險評估結果、自身資通安全責任等級之應辦事項，全學校之防護及控制措施詳如本校資通安全維護計畫，採行相關之防護及控制措施如下：

(一) 資訊及資通設備之管理

依「臺北市政府資通系統安全作業指引」、「臺北市政府資通訊資產及電子資料安全作業指引」及「臺北市政府資通訊業務委外作業指引」規定及相關程序辦理。

(二) 存取控制與加密機制管理

依「臺北市政府資通系統安全作業指引」規定及相關程序辦理。

(三) 作業與通訊安全管理

依教育部「臺灣學術網路管理規範」及「臺北市政府資通系統安全作業指引」規定及相關程序辦理。

(四) 資通安全防護設備

網路安全防護應依教育部「臺灣學術網路管理規範」辦理。

十、資通安全事件通報、應變及演練相關機制

依「臺灣學術網路各級學校資通安全通報應變作業程序」規定辦理。

十一、資通安全情資之評估及因應

依「臺灣學術網路各級學校資通安全通報應變作業程序」與「臺北市政府資通安全管理規定」辦理。

十二、資通系統或服務委外辦理之管理

依「臺北市政府資通訊業務委外作業指引」及「臺北市政府資通安全管理規定」玖、受託業務之資通安全管理規定辦理。

十三、資通安全教育訓練

依「資通安全責任等級 D 級之各機關應辦事項」資通安全教育訓練規定辦理。

十四、公務學校所屬人員辦理業務涉及資通安全事項之考核機制

本校資訊相關人員其獎懲系依據「公務學校所屬人員資通安全事項獎懲辦法」辦理。

十五、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

(一) 資通安全維護計畫之實施

為落實本安全維護計畫，本校執行資通安全管理應與本校之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

(二) 資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全推動小組應每年至少一次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，確保其持續適切性、合宜性及有效性。

2. 管理審查議題應包含下列討論事項：

(1) 與資通安全管理業務有關之內部及外部議題的變更，如法令變更、上級學校要求、資通安全推動小組決議事項等。

(2) 資通安全維護計畫內容之適切性。

(3) 資通安全績效之回饋，包括：

(a) 政策及目標之實施情形。

(b) 人力及資源之配置之實施情形。

(c) 防護及控制措施之實施情形。

(4) 資訊及資通系統之盤點及風險評估。

(5) 重大資通安全事件之處理及改善情形。

(6) 利害關係人之回饋。

(7) 持續改善之機會。

3. 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

十六、資通安全維護計畫實施情形之提出

本校依據資通安全管理法第 12 條之規定，應向上級或監督機關，提出資通安全維護計畫實施情形，使其得瞭解本校之年度資通安全計畫實施情形。

十七、相關法規、程序及表單

為使本校資通安全管理有效運作，本校應依相關文件、流程、程序或控制措施確實執行，並應保存相關之執行紀錄；如本校已有資通安全管理系統之文件，應與本校資通安全政策、目標及本安全維護計畫之內容相符。

(一) 相關法規

1. 資通安全管理法

- 2.資通安全管理法施行細則
- 3.資通安全責任等級分級辦法
- 4.臺北市政府資通安全管理規定
- 5.臺北市政府資通訊業務委外作業指引
- 6.臺北市政府使用物聯網安全作業指引
- 7.臺北市政府資通系統安全作業指引
- 8.臺北市政府資通訊資產及電子資料安全作業指引
- 9.臺灣學術網路管理規
- 10.臺灣學術網路各級學校資通安全通報應變作業程序

(二)附件表單

- 1.資通安全推動小組成員及分工表
- 2.資通安全保密切結書與個人資料提供同意書
- 3.風險評估表
- 4.風險類型暨風險對策參考表
- 5.管制區域人員進出登記表
- 6.委外廠商執行人員保密切結書
- 7.委外廠商執行人員保密同意書
- 8.委外廠商保密切結書
- 9.委外廠商查核項目自評表
- 10.申請遠距工作保密切結書
- 11.資通安全教育訓練計畫
- 12.資通安全認知宣導及教育訓練簽到表

貳、附件

一、臺北市立第一女子高級中學資訊安全推動小組成員及分工表

臺北市立第一女子高級中學資訊安全推動小組成員及分工表

單位職級	組別	職掌事項	分機
校長	資通安全長	執掌事項詳列於本校資通安全管理計畫中。	200
教務主任 (組長)	策略規劃組	1. 資通安全政策及目標之研議。 2. 訂定學校資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。 3. 依據資通安全目標擬定學校年度工作計畫。 4. 傳達學校資通安全政策與目標。 5. 其他資通安全事項之規劃。	300
學務主任			500
總務主任			600
輔導主任			700
圖書館主任			800
秘書			201
人室主任			210
會計主任			220
文書組長			610
圖書館主任 (組長)			資安防護組
資訊組長	850		
系統管理師	852		

保密切結書

本人 _____ 將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責，保護所接觸到的個人資料，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負法律責任。

此致

臺北市立第一女子高級中學

立同意書人：_____

身分證字號：_____

電 話：_____

住 址：_____

中 華 民 國 年 月 日

《後續--個人資料提供同意書》

個人資料提供同意書

本同意書說明臺北市立第一女子高級中學（以下簡稱本校）將如何處理本表單所蒐集到的個人資料，當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。

1. 本校因執行業務蒐集您的個人資料包括姓名、身分證字號、電話、地址等。
2. 若您的個人資料有任何異動，請主動向本校人事室申請更正，使其保持正確、最新及完整。
3. 若您提供錯誤、不實、過時或不完整或具誤導性的資料，您將損失相關權益。
4. 您可依中華民國「個人資料保護法」，就您的個人資料行使以下權利：
 - (1) 請求查詢或閱覽。
 - (2) 製給複製本。
 - (3) 請求補充或更正。
 - (4) 請求停止蒐集、處理及利用。
 - (5) 請求刪求。
5. 本校利用您的個人資料期間為即日起至_____年，利用地區為臺灣地區。
6. 除非取得您的同意或其他法令之特別規定，本校絕不會將您的個人資料揭露予第三人或使用。
7. 僅有經過授權的人員才能接觸您的個人資料，相關處理人員皆簽有保密合約，如有違反保密義務者，將會受到相關的法律處分。
8. 本同意書可能會因應個人資料保護法或其他相關法規、以及實際需求進行修正。

我瞭解與同意以上文字

_____ 簽章

中 華 民 國 年 月 日

臺北市立第一女子高級中學風險評估表

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				

承辦人員：

單位主管：

臺北市立第一女子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密與透過具有憑證檢驗功能的身份驗證機制
	802.1X 攻擊	<ul style="list-style-type: none"> • 檢測 X.509 憑證是否有效。 • 指定合法驗證者（RADIUS 伺服器）之一般名稱值。 • 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	<ul style="list-style-type: none"> • 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。 • 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	<ul style="list-style-type: none"> • 如果沒有明確要求，應關閉 IPv6。 • 取消對 ICMP 重導向的支援。 • 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	<ul style="list-style-type: none"> • 停用無加密傳輸安全性的 Telnet、FTP、SNMP、VNC 等。 • 遠端操作維護須透過安全的身份驗證連接。 • 建構封閉的管理網路。
	SSH 伺服器攻擊	<ul style="list-style-type: none"> • 強制使用 2.0 版本的協定，禁止向下相容特性。 • 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	<ul style="list-style-type: none"> • 停止支援來自不受信任來源的遞回查詢。 • 確保區域檔案不含多餘或敏感資訊。
	Kerberos 伺服器攻擊	<p>停止支援較弱的 HMAC 演算法。</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 確認 VPN 伺服器的維護作業，並修補到最新版本。

		<ul style="list-style-type: none"> • 強制使用 AH 和 ESP 功能身份驗證及機密性服務。 • 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。 • 過濾內連的 VPN 流量，以便在發生入侵事件時限制網路存取。 • 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	<ul style="list-style-type: none"> • 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。 • 禁止將管理介面或特權功能公開在不受信任的網路上。 • 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	<ul style="list-style-type: none"> • 限制資料服務只與經授權的對象往來，特別是雲端環境中。 • 避免使用不支援身份驗證的儲存系統和協定。 • 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。 • 確保密碼強度。 • 限制只有受信任的網路才能存取管理服務。 • 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。
<p>參考來源：資安風險評估指南，第三版，Chris McNab，江湖海譯。</p>		

五、臺北市立第一女子高級中學管制區域人員進出登記表

臺北市立第一女子高級中學管制區域人員進出登記表

製表日期： 年 月 日

編號	單位及姓名	配同人員	日期	進出時間	事由	進出設備 (物品)
1	單位： 姓名：			進： 出：		
2	單位： 姓名：			進： 出：		
3	單位： 姓名：			進： 出：		
4	單位： 姓名：			進： 出：		
5	單位： 姓名：			進： 出：		
6	單位： 姓名：			進： 出：		
7	單位： 姓名：			進： 出：		
8	單位： 姓名：			進： 出：		
9	單位： 姓名：			進： 出：		

10	單位： 姓名：			進： 出：		
----	------------	--	--	----------	--	--

承辦人員：

單位主管：

臺北市立第一女子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應簽署本切結書。

中 華 民 國 年 月 日

臺北市立第一女子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：

- 甲、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。
- 乙、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。
- 丙、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

臺北市立第一女子高級中學委外廠商保密切結書

_____ 公司(以下簡稱乙方) 承攬臺北市立第一女子高級中學(以下簡稱甲方)

「 (填寫服務名稱) 」(以下簡稱本專案)，於執行過程中，乙方自

甲方所取得之公務(機密)資訊，具結依下列規定保密並履行責任：

- 一、乙方應遵守「個人資料保護法」、「刑法」、「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」等相關法令，不私自蒐集本專案範圍外任何資訊。
- 二、乙方於本專案進行期間，依契約所產生或接觸之公務(機密)資料，非經甲方同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三人。對所獲得或知悉之上述公務(機密)資料，乙方須負保密責任。其因法令或主管機關規定需向公務機關提供時，應在第一時間通知甲方。
- 三、公務(機密)資料保密期限，不受本專案工作完成(結案)及乙方不同工作地點及時間之限制。乙方持有或獲知公務(機密)資料，不得洩漏或轉讓於第三人。若因本專案終止，公務(機密)資料無再使用之必要，乙方應進行資料銷毀，不得以任何形式保存。
- 四、乙方違反本資訊安全保密切結書之規定，致造成甲方或第三人之損害或賠償，乙方同意無條件負擔全部責任，包括因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。於第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方應合作提供，絕無異議。

此致

臺北市立第一女子高級中學

立切結書人：

廠商名稱及蓋章：

廠商負責人姓名及簽章：

統一編號：

公司地址：

中 華 民 國 年 月

臺北市立第一女子高級中學委外廠商查核項目自評表

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？				指派副首長擔任資安長。
	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？				機關依規定配置資安人員2人。
	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
	3.4 是否配置適當之資源？				機關並未投入足夠資安資源。
	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。

查核項目	查核內容	查核結果			說明
		符 合	不 符 合	不 適 用	
4. 資訊及資通系統之盤點及風險評估	4.2 各項資產是否有明確之管理者及使用者？				資產依規定指定管理者及使用者。
	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訓練。
	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。
	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。

查核項目	查核內容	查核結果			說明
		符 合	不 符 合	不 適 用	
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?				備份資料均已測試。
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?				均設有加密之保護措施。
5.24	是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)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。
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。

查核項目	查核內容	查核結果			說明
		符 合	不 符 合	不 適 用	
	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	6.1 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。
	6.2 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。
	6.3 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. 資通安全維護計畫實施情形	8.1 是否設有稽核機制？				訂有稽核機制。
	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。

查核項目	查核內容	查核結果			說明
		符 合	不 符 合	不 適 用	
之精進改善機制	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	9.1 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。
	9.2 是否追蹤過去缺失之改善情形？				有追蹤缺失改善之情形。
	9.3 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。

廠商名稱及蓋章：

廠商負責人姓名及簽章：

十、 臺北市立第一女子高級中學申請遠距工作保密切結書

臺北市立第一女子高級中學申請遠距工作保密切結書

編號：_____ - _____

具保密切結（人員） _____（以下簡稱乙方）於民國 _____ 年 _____ 月 _____ 日起於
臺北市立第一女子高級中學執行因行政業務（或專案）需求，申請使用電腦遠端連線服務
「 _____（請填軟體或服務名稱）」（以下簡稱本服務），使用期
間接觸公務（機密）資料，將恪遵以下保密規定：

- 一、乙方不得將公務（機密）資料以任何形式利用或洩漏、告知、交付、移轉予任何第三人，如有違誤願負法律上之責任。
- 二、本服務僅限乙方個人使用，乙方應嚴守資安規定，不得將本服務以任何形式轉予第三人使用，如有違誤願負法律上之責任。

此致

臺北市立第一女子高級中學

具切結書委外（人員）：

（簽章）

十一、臺北市立第一女子高級中學資通安全教育訓練計畫

臺北市立第一女子高級中學資通安全教育訓練計畫

壹、依據

臺北市立第一女子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
資通安全人員		
一般主管		
一般使用者	教師(不含兼任資通人員)	
	職員	
	技工及工友	
	警衛	
共計		

肆、訓練項目

人員類別	訓練課程	時數
資通安全人員	資通安全管理制度 資訊系統風險管理 資通安全稽核 資安事故處理 業務持續運作管理	
一般主管、使用者	資通安全基本認知 資通安全管理制度	

伍、訓練期程

由本校自行排定教育訓練期程或配合上級單位政策辦理訓練。

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、線上課程等等)。

十二、臺北市立第一女子高級中學資通安全認知宣導及教育訓練簽到表

臺北市立第一女子高級中學資通安全認知宣導及教育訓練簽到表

課程名稱：_____

時 間：_____

地 點：_____

單 位	職 稱	姓 名	簽 名