臺中市北區篤行國民中小學

資通安全維護計畫

版次：V2.3版

資通安全責任等級	D級
修訂人核章	
單位主管核章	
資安長核章	

中華民國 114 年 08 月 20 日

資通安全維護計畫

文件制/修訂紀錄表

文件版本	修訂日期 會議名稱	修訂內容	修訂單位	修訂人	核定人 (資安長)
V1.0(初版)	108 年 1 月 18 日 行政會議	新擬訂文件	教務處 資訊組		
V2.0 版	109 年 3 月 26 日 行政會議	增修訂文件	教務處 資訊組		
V2.1 版	109 年 5 月 6 日 第 1 次資通安全管理審查會議	增修訂文件	教務處 資訊組		
V~~3.0~~2.2 版	113 年 12 月 31 日 第 1 次資通安全管理審查會議	增修訂文件	教務處 資訊組		
V2.3 版	114 年 08 月 20 日 資通安全管理審查會議	增修訂文件	教務處 資訊組		

資通安全維護計畫

目　　錄

內容

壹、依據及目的

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、教育部109年4月20日臺教資(四)字第1090054520號函頒「公立高級中等以下學校資通安全防護計畫」。

貳、適用範圍

本計畫適用範圍涵蓋臺中市北區篤行國民小學全部範圍，另包含附設幼兒園（以下簡稱本機關）。

參、核心業務及重要性

一、本機關之核心業務及重要性

本機關之核心業務及重要性說明如下表：

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
教務業務：課程發展、課程編排、教學實施、學籍管理、成績評量、教學設備、教具圖書資料供應、教學研究及教學評鑑，並與輔導單位配合實施教育輔導等事項	雲端學務系統（向上集中） 圖書管理系統(向上集中)	為本機關依組織法執掌，足認為重要者。	違反法遵義務:依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	~~4小時~~ 24小時
學生事務：公民教育、道德教育、生活教育、體育衛生保健、學生團體活動及生活管理，並與輔導單位配合實施生活輔導等事項。	雲端學務系統（向上集中） 教育部學生健康資訊系統（向上集中）	為本機關依組織法執掌，足認為重要者。	違反法遵義務:依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	~~4小時~~ 24小時
總務業務：學校文書、事務及出納等事項	雲端學務系統（向上集中）	為本機關依組織法執	違反法遵義務:依個人資料保護法應善盡個人資料保護責	~~8小時~~ 24小時

		掌，足認為重要者。	任，如違反該法致足生損害他人者將依受罰。	
輔導業務：學生資料蒐集與分析、學生智力、性向、人格等測驗之實施，學生興趣、學習成就與志願之調查、輔導諮商之進行，並辦理特殊教育及親職教育等事項。	雲端學務系統（向上集中）	為本機關依組織法執掌，足認為重要者。	違反法遵義務:依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	~~8小時~~ 24小時
人事業務：差勤服務、人事管理等事項。	行政院人事行政總處人事服務網（向上集中） 雲端學務系統差勤模組（向上集中）	為本機關依組織法執掌，足認為重要者。	違反法遵義務:依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	~~8小時~~ 24小時
會計業務：歲計、會計及統計等事項。	教育部地方教育發展基金會計資訊系統（向上集中）	為本機關依組織法執掌，足認為重要者。	違反法遵義務:依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	~~8小時~~ 24小時
校園網路維運: 學校官網 網域名稱服務 電子郵件伺服器	官網 WEB server（向上集中）	為上級機關指定之核心資通系統。	可能使本校部分業務中斷	~~8小時~~ 24小時
	DNS server（向上集中）	為上級機關指定之核心資通系統	可能使本校部分業務中斷	~~4小時~~ 24小時
	教育部校園雲端電子郵件（向上集中）	為上級機關指定之核心資通系統	可能使本校部分業務中斷	~~8小時~~ 24小時

各欄位定義：

(一)核心業務：請參考資通安全管理法施行細則第 7 條之規定列示。

(二)核心資通系統：該項核心業務所必須使用之資通系統名

稱。

(三)重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

(四)業務失效影響說明：該項業務使用之系統失效後，機關業務運作有何影響。

(五)最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

二、 非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務系統	業務失效影響說明	最大可容忍中斷時間
防火牆系統	可能使本校資安防護中斷	~~4 小時~~ 24 小時
~~防毒系統~~	~~可能使本校資安防護中斷~~	~~12 小時~~

各欄位定義：

(一)非核心業務系統：公務機關非核心業務相關之資通系統，如公文系統、用戶端服務等。

(二)業務失效影響說明：該項業務使用之系統失效後，機關業務運作有何影響。

(三)最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

肆、資通安全政策及目標

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、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：

(一)~~應因應資通安全威脅情勢變化，~~辦理資通安全教育訓練一般使用者與主管，每人每年三小時以上之一般資通安全教育訓練，以提高本機關同仁之資通安全意識~~，本機關同仁亦應確實參與訓練~~。

(二)應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

(三)針對辦理資通安全業務有功人員~~應~~應依資通安全管理法子法之「公務機關所屬人員資通安全事項獎懲辦法」進行獎勵。

~~(四)勿開啟來路不明或無法明確辨識寄件人之電子郵件。~~

(四) 定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。

(五)禁止多人共用單一資通系統帳號。

~~(六)不可私接網路或網路設備。~~

(六)落實資通安全通報機制。

~~(七)安裝並啟用有版權之防毒系統。~~

(七)建立資通安全防護 (如:防火牆、防毒軟體)

~~(八)應加強監督維護廠商人員，確保符合資安防護要求。~~

二、資通安全目標

(一)量化型目標

1. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
2. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 6%及 5%。

(二)質化型目標

1.適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使

用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

2.達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

3.提升人員資安防護意識、有效偵測與預防外部攻擊等。

三、資通安全政策及目標之核定程序

資通安全政策由本機關~~資通安全管理審查會議研議通過~~教務處簽陳資通安全長核定。

四、資通安全政策及目標之宣導

(一)本機關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，向機關內所有人員進行宣導，並檢視執行成效。

(二)本機關應每年向利害關係人(例如資通設備供應商、資通設備維護廠商~~、志工~~等)進行資安政策及目標宣導，並檢視執行成效。

五、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管理審查會議~~(或內部會議)~~檢討其適切性。

伍、資通安全推動組織

一、資通安全長

依資通安全法第 11 條之規定，本機關訂定教務主任（由機關首長指派副首長或適當人員兼任）為資通安全長，負責督導機關資通安全相關事項，其任務包括：

(一)資通安全管理政策及目標之核定、核轉及督導。

(二)資通安全責任之分配及協調。

(三)資通安全資源分配。

(四)資通安全防護措施之監督。

(五)資通安全事件之檢討及監督。

(六)資通安全相關規章與程序、制度文件核定。

(七)資通安全管理年度工作計畫之核定

(八)資通安全相關工作事項督導及績效管理。

(九)其他資通安全事項之核定。

二、資通安全推動小組

(一)組織

為推動本機關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機關單位主管(處室主任/組長)以上之人員代表成立資通安全推動小組 ，其任務包括：

1.跨部門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。

(二)分工及職掌

本機關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，本機關資通安全推動小組分組人員名單及職掌應列冊~~(如附表 1，參見第 30 頁)~~，並適時更新之：

1. 策略規劃組：

(1) 資通安全政策及目標之研議。

(2) 訂定機關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機關年度工作計畫。

(4) 傳達機關資通安全政策與目標。

(5) 其他資通安全事項之規劃。

2. 資安防護組：

(1) 資通安全技術之研究、建置及評估相關事項。

(2) 資通安全相關規章與程序、制度之執行。

(3) 資訊及資通系統之盤點及風險評估。

(4) 資料及資通系統之安全防護事項之執行。

(5) 資通安全事件之通報及應變機制之執行。

(6) 其他資通安全事項之辦理與推動。

3. 績效管理組：

(1) 辦理資通安全內部~~稽核自我檢查作業~~自我檢查。

(2) ~~每年最少召開1次定期召開~~資通安全管理審查會議，提報資通安全事項執行情形。

陸、~~專職(責)~~人力及經費配置

一、~~專職(責)~~人力及資源之配置

(一)本機關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~~調降為~~D級，~~設置一名~~專責~~正式人員~~兼辦~~資通安全業務負責本機關之法遵義務、教育訓練及資通安全事件通報及應變等業務之推動。本機關現有資通安全專責人員名單及職掌應列冊，並適時更新(名冊如附表1-1，請參見第30頁)~~無需設置資通安全專職(責)人員。

(二)本機關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，並提升機關內資通安全專業人員之資通安全管理能力。本機關之相關處室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機關（構）提供顧問諮詢服務。

(三)本機關之首長及資安業務處室主任（組長），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。

(四)~~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。

~~(五)資安專責人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。~~

~~1.資安專責人員總計應持有0張以上資通安全專業證照。~~

~~2.資安專職(責)人員總計應持有0張以上資通安全職能評量證書。~~

二、經費配置

(一)本機關的經費配置如附表2~~(請參見第31頁)。~~

(二)資通安全推動小組於規劃配置相關經費及資源時，應考量本機關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 。

(三)各處室如有資通安全資源之需求，應配合機關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。

(四)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。

柒、資訊及資通系統之盤點

一、 資訊及資通系統盤點

(一)本機關每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產、支援服務資產等。

(二)本機關每年度應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」，欄位應包含資產名稱、資產類別、擁有者、管理者、使用者、存放位置等。

(三)資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。

(四)本機關資訊及資通系統資產清冊請見~~附表 3(參見第 31 頁)~~：

項次	財產編號	資產名稱	系統屬性	版本類別註1	系統建置方式	系統主管機關註2	系統管理者(部門)	系統使用者(部門)	核心系統(Y/N)	含機敏資料(Y/N)	防護需求等級	是否符合防護基準(資通安全責任等級分級辦法附表10)	不符合防護基準項目(資通安全責任等級分級辦法附表10)	是否導入ISMS註3	建置廠商註3	維運廠商註3	最大可容忍中斷時間註3
1			1.行政 2.業務	1.共用 2.公版 3.機關自用	1.自行委外 2.租用服務 3.套裝軟體 4.自行開發 5.主管/上級機關提供 6.其他						1.普 2.中 3.高 4.系統建置於主管/上級機關處	1.符合 2.部分符合 3.不符合					

(五)各單位管理之資訊或資通系統如有異動，應即時通知資訊安全推動委員會更新~~(附表 3)~~資產清冊。

二、機關資通安全責任等級分級

本機關資安責任等級依據「資通安全責任等級分級辦法第 6 條辦理，並考量機關已有核心系統向上集中規劃，依同法第 10 條第 4 款調整等級為 D 級。」

捌、資通安全風險評估

一、資通安全風險評估

(一)本機關應每年針對資訊及資通系統資產進行風險評估，若配合資訊資源向上集中計畫，資訊系統已規劃由教育局兼辦或代管，校內尚有資通系統，故需針對資訊及資通系統資產進行風險評估。

(二)執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。

(三)本機關應每年依據資通安全責任等級分級辦法（附表九）之規定，分別就機密性、完整性、可用性、法律遵

循性等構面評估自行或委外開發之資通系統防護需求分級，~~每年並最少定期~~檢視~~1次~~資通系統分級妥適性。

二、非核心資通系統及最大可容忍中斷時間(機關可依實際情形調整)

非核心資通系統	資訊資產	最大可容忍中斷時間	非核心資通系統主要功能
1.防火牆兼dhcp服務 ~~3.防毒服務~~	1. 網路防火牆(Forti~~200d~~100f) ~~2. 網路防毒系統(Officescan XG)~~	~~4小時~~ 24小時	提供網路連線、資通安全防護及教學或公務檔案儲存用。

玖、資通安全防護及控制措施

本機關依據自身資通安全責任等級之應辦事項，採行相關之防護及控制措施如下:

一、資訊及資通系統之管理

(一) 資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

(二)資訊及資通系統之使用

1. 本機關同仁使用資訊及資通系統前應經其管理人授權。

2. 本機關同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本機關同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。
4. 非本機關同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。
5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

(三)資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。
2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

二、存取控制與加密機制管理

(一)網路安全控管

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主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。
3. 本機關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)用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二)資通系統權限管理

1. 本機關之資通系統應設置通行碼管理，通行碼之要求需滿足：

(1)通行碼長度 8 碼以上。

(2)通行碼複雜度應包含英文、特殊符號或數字~~二~~二種以上。

~~(3)使用者每 180 天應更換一次通行碼。~~

2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

(三)特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 資通系統之特權帳號不得共用。

3. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

4. 資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

5. 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

(四)加密管理

1. 本機關之機密資訊於儲存或傳輸時應進行加密。

2. 本機關之加密保護措施應遵守下列規定：

(1) 應落實使用者更新加密裝置並備份金鑰。

(2) 應避免留存解密資訊。

(3) 一旦加密資訊具遭破解跡象，應立即更改之。

三、作業與通訊安全管理

(一)防範惡意軟體之控制措施

1. 本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

(1)經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

(2)電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

(3)確實執行網頁惡意軟體掃描。

2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

3. 使用者不得私自使用已知或有嫌疑惡意之網站。

4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二)遠距工作之安全措施

1. 本機關資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。

2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

(1) 提供適當通訊設備，並指定遠端存取之方式。

(2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

(3) 進行遠距工作時之安全監視。

(4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三)電子郵件安全管理：

1. 本機關配合向上集中計畫，校內無電子郵件伺服器~~，本校同仁均申請教育部雲端電子郵件為公務信箱~~。

2. 遵循教育部雲端電子郵件使用管理要點。

(四)確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理

(1)~~資料中心及~~電腦機房應進行實體隔離。

~~(2)機關人員或來訪人員應申請及授權後方可進入資料中心及電腦機房，資料中心及電腦機房管理者並應定期檢視授權人員之名單。~~

(~~3~~2)管制區應有公告標示，並隨時注意身分不明或可疑人員。

(43)僅於必要時，得准許外部支援人員進入~~資料中心及~~電腦機房。

~~(5)人員及設備進出資料中心及電腦機房應留存記錄。~~

2. ~~資料中心及~~機房之環境控制

(1)~~資料中心及~~電腦機房之空調、電力應建立備援措施。

(2) ~~資料中心及~~電腦機房之溫濕度管控範圍為：

(3) 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

3.辦公室區域之實體與環境安全措施

(1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

(2) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

(3) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(4) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

(5) 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

(6) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

(五)資料備份

1. 重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。
2. 本機關應每季確認核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統。
3. 敏感或機密性資訊之備份應加密保護。

(六)媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

(七)電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過30分鐘不使用時，應立即登出或啟動螢幕保護功能或取出自然人憑證。

2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

5. 下班時應關閉電腦及螢幕電源。

6. 如發現資安問題，應主動循機關之通報程序通報。

7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

(八)行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。

2. 機敏會議或場所不得攜帶未經許可之行動設備進入。

四、獲取、開發及維護

本機關之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十之資通系統防護基準，並注意下列事項：

(一)開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展

流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

(二)於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

(三)於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

(四)執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

五、業務持續運作演練及安全性檢測

（一）本機關全部核心資通系統已向上集中至教育局或教育部等政府機關，將配合教育局規定參與持續運作演練計畫。

（二）本機關全部核心資通系統已向上集中至教育局或教育部等政府機關，將配合教育局網站安全弱點檢測及系統滲透測試結果，修補漏洞及更新相關修正程式。

~~六、執行資通安全健診~~

~~本機關仍維運非核心資通系統配合教育部規定每二年應辦理資通安全健診1次，其至少應包含下列項目，並檢討執行情形：~~

~~(一)網路架構檢視。~~

~~(二)網路惡意活動檢視。~~

~~(三)使用者端電腦惡意活動檢視。~~

~~(四)具有伺服器主機者，應進行伺服器惡意活動檢視。~~

~~(五)具有目錄伺服器者，應檢視目錄伺服器設定。~~

~~(六)具有防火牆者，應檢視防火牆連線設定。~~

~~七~~六、資通安全防護設備

(一)本機關應建置防毒軟體、網路防火牆、~~電子郵件過濾裝~~置，持續使用並適時進行軟、硬體之必要更新或升級。

(二)資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本機關依「臺灣學術網路各級學校資通安全通報應變作業程序」辦理資通安全事件通報、應變及演練。

壹拾壹、資通安全情資之評估及因應

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本機關接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一)資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二)入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(三)機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及

其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四)涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

二、 資通安全情資之因應措施

本機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一)資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二)入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三)機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四)涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、資通系統或服務委外辦理之管理

本機關委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、選任受託者應注意事項

(一)受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

(二)受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

(三)受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

(四)受託業務涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，於招標公告、招標文件及契約中，註明受託者辦理該項業務人員及可能接觸該國家機密人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

(五)前點適任性查核得在必要範圍內就下列事項查核，查核前應經當事人書面同意：

1. 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案者。
2. 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。
3. 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。

4. 其他與國家機密保護相關之具體項目。

二、監督受託者資通安全維護情形應注意事項

(一)受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

(二)受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

(三)委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

(四)受託者應採取之其他資通安全相關維護措施 。

(五)本機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核自我檢查作業或其他適當方式確認受託業務之執行情形。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

~~(一)本機關依資通安全責任等級分級屬調整D級，資安及資訊人員每年至少1名人員接受12小時以上之資安專業課程訓練或資安職能訓練。~~

~~(二)~~本機關~~之~~依資通安全責任等級分級屬 D 級，一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

二、資通安全教育訓練辦理方式

（未自行辦理資通安全教育訓練者，請保留下列說明）

(一)每年參加教育部、各大專院校、臺中市政府、教育局辦理之資通安全教育訓練或利用數位學習以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

(二)員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

(三)資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

(自行辦理資通安全教育訓練者，請寫保留下列說明)

(四)承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

1. 本機關資通安全認知宣導及教育訓練計畫如附件1~~(參見第35頁)~~，訓練內容得包含：資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
2. 資通安全法令規定。
3. 資通安全作業內容。
4. 資通安全技術訓練。

(五)員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

(六)資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

壹拾肆、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

本機關所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、臺中市政府及所屬各機關學校公務人員平時獎懲案件處理要點，及本機關各相關規定辦理之。

壹拾伍、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，使本機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本機關之資通安全政策、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、資通安全維護計畫實施情形之稽核自我檢查作業機制

(一)稽核自我檢查作業機制之實施

1. 資通安全推動小組應~~於12月前(至少每年一次)或於系統重大變更或組織改造後定期~~執行~~1次~~內部~~稽核作業(~~自我檢查作業~~)~~，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

2. 辦理~~稽核~~自我檢查作業前資通安全推動小組應擬定資通安全~~稽核~~自我檢查作業計畫並安排~~稽核~~自我檢查作業成員，~~稽核~~自我檢查作業計畫應包括~~稽核~~自我檢查作業之依據與目的、期間、重點領域、~~稽核~~自我檢查作業小組組成方式、保密義務、~~稽核~~自我檢查作業方式、基準與項目及受~~稽~~檢單位協助事項，並應將前次~~稽核~~自我檢查作業之結果納入~~稽核~~自我檢查作業範圍。

3. 辦理~~稽核~~自我檢查作業時，資通安全推動小組應於執行~~稽核~~自我檢查作業前30日，通知受~~稽核~~檢單位，並將~~稽核~~自我檢查作業期程、~~稽核~~自我檢查作業項目紀錄表及~~稽核~~自我檢查作業流程等相關資訊提供受~~稽~~檢單位。

4. 本機關之~~稽核~~自我檢查作業人員應受適當培訓並具備~~稽核~~自我檢查作業能力，且不得~~稽核~~自我檢查作業自身經辦業務，以確保~~稽核~~自我檢查作業過程之客觀性及公平性；另，於執行~~稽核~~自我檢查作業時，應填具~~稽核~~自我檢查作業項目紀錄表，待~~稽核~~自我檢查作業結束後，應將~~稽核~~自我檢查作業項目紀錄表內容彙整至~~稽核~~自我檢查作

業結果及改善報告 中，並提供給受稽檢單位填寫辦理情形。

5. 稽核自我檢查作業結果應對相關管理階層(含資安長)報告，並留存稽核自我檢查作業過程之相關紀錄以作為資通安全稽核自我檢查作業計畫及稽核自我檢查作業事件之證據。
6. 稽核自我檢查作業人員於執行稽核自我檢查作業時，應至少執行一項特定之稽核自我檢查作業項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼)。
7. 本機關稽核自我檢查作業得併同政風單位電腦稽核自我檢查作業或主計單位內控稽核自我檢查作業辦理，惟稽核自我檢查作業項目應參照本機關資通安全維護計畫，檢視機關實施情形及績效。
8. 本機關應配合上級或監督機關之規定辦理查核作業，以確認人員是否遵循本計畫與機關之管理程序要求，並有效實作及維持管理制度。

(二)稽核自我檢查作業改善報告

1. 受稽檢單位於稽核自我檢查作業實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。
2. 受稽檢單位於稽核自我檢查作業實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。
3. 受稽檢單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

4. 機關應定期審查受稽檢單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

5. 受稽檢單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核自我檢查作業結果及改善報告。

三、 資通安全維護計畫之持續精進及績效管理

(一)機關之資通安全推動小組應~~於九月前(每年至少一次)~~定期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。

(二)管理審查議題應包含下列討論事項：

1.過往管理審查議案之處理狀態。

2.與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

3.資通安全維護計畫內容之適切性。

4.資通安全績效之回饋，包括：

(1) 過往管理審查議案之處理狀態。

(2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

(3) 資通安全維護計畫內容之適切性。

(4) 資通安全績效之回饋，包括：

A. 資通安全政策及目標之實施情形。

B. 資通安全人力及資源之配置之實施情形。

C. 資通安全防護及控制措施之實施情形。

D. 內外部稽核自我檢查作業結果。

E. 不符合項目及矯正措施。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 持續改善之機會。

(三)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。

壹拾陸、資通安全維護計畫實施情形之提出

本機關依據本法第 12 條之規定，依主管機關~~(行政院)~~規定期限向上級或監督機關，提出資通安全維護計畫實施情形，使其得瞭解本機關之年度資通安全計畫實施情形。

壹拾柒、附表及附件

附表1資通安全推動小組成員及分工表

臺中市北區篤行國民小學資通安全推動小組成員及分工表				
NO	組別	處室	職稱	職掌分工（機關內部自訂）
1		校長室	校長	指派副首長或適當人員兼任資通安全長
2	策略規劃組	教務處	教務主任 資訊組長	訂定資通安全維護計畫 執行資通安全維護計畫、資通安全事件通報
3	資安防護組	學務處 總務處 輔導室 幼兒園 ~~學年代表~~	學務主任 總務主任 輔導主任 幼兒園主任 ~~學年主任~~	資通安全事件演練 資產盤點及委外廠商資安稽核 家長會及志工資安教育訓練 幼兒園資通系統安全維護 ~~自我檢查作業~~ ~~班級及科任資通系統安全維護~~
4	績效管理組	人事室 會計室	人事主任 會計主任	權限控管、資通安全獎懲考核 控管資安經費預算、內部~~稽核~~ 自我檢查作業

備註：機關之資通安全推動小組應~~於12月30日前(每年至少一次)~~定期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。

附表1-1機關專職人力

機關名稱	姓名	職稱	人員屬性(職聘僱或委外)	是否專職	持有之有效專業證照張數	持有之有效職能評量證書張數
~~篤行國小~~	~~呂健聰~~	~~資訊組長~~	~~老師~~	~~否~~	~~0~~	~~0~~

填表說明：

1、請依機關資安責任等級應具備之資安專職人數進行填寫，即調整D級學校至少應填1人(專責人員)，得以兼職方式為之。

2、如已有缺額但待聘，姓名欄位請填「待聘」；如尚待爭取員額，職稱欄位請填「待爭取」，其餘欄位不用填。

附表 2 經費配置（提報年度，千元）

機關名稱	機關年度經費-資本門	機關年度經費-經常門	年度資訊經費-資本門	年度資訊經費-經常門	年度資安經費-資本門	年度資安經費-經常門
篤行國小	240	7573	80	56	0	0

填表說明：

一、資訊經費係指各機關之業務費、設備及投資費。

(一)業務費(經常門)：

1.教育訓練費:凡各機關、學校處理經常一般公務或特定工作計畫所需之各項業務費用屬之。凡對現職員工實施教育訓練所需補貼(補助)有關學分費、雜費、教材、膳宿及交通費等費用屬之。

2.資訊服務費:凡公務所需使用資訊操作、維修、購買雲端等服務費用、金額未達1萬元之軟體購置或屬營業租賃性質之資訊設備租金屬之。

(二)設備及投資(資本門)：

1.資訊軟硬體設備費：凡公務所需各項電腦設施、週邊設備、裝置（含一次購買時所配置之套裝軟體，如作業系統軟體，以及後續2年以上效益之軟體改版、升級與應用系統開發規劃設計）及雲端服務等購置（含資本租賃）費用屬之。

二、資安經費(經常門、資本門)：辦理資通安全管理法及其子法之法遵事項相關經費。

附表 3 機關資通系統資產清冊範例

項次	學校財產編號	資產名稱	系統屬性	版本類別	系統建置方式	系統主管機關	系統管理者	系統使用者	核心系統(Y/N)	含機敏資料(Y/N)	防護需求等級	是否符合防護基準(資通安全責任等級分級辦法附表10)	不符合防護基準項目(資通安全責任等級分級辦法附表10)	是否導入ISMS	建置廠商	維運廠商	最大可容忍中斷時間
1	3000401-09-~~3000091~~3001137	防火牆	1	3	5	教育局	資訊組	資訊組	N	N	中			N			~~4時~~24時
2	~~3140101-03-3000443~~	~~防毒系統~~	~~1~~	~~3~~	~~6~~		~~資訊組~~	~~資訊組~~	~~N~~	~~N~~	~~低~~			~~N~~			~~8時~~

填表說明：

1. 資通系統包含 IT(Information Technology)及 OT(Operational Technology），OT 如影像安全控制管理、門禁監控、物聯設備相關管理等系統；其餘資產由機關自行管理
2. 註 1：
共用：2 個以上機關共同使用之系統（如戶政、地政、財政、人事差勤系統)。
公版：各機關依特定版本自行維運使用(如公務出國報告資訊網)。
3. 註 2：系統建置方式為「5. 主管/上級機關提供」，則於此欄位敘明主管/上級機關；若為「6. 其他」，請於本欄位說明建置方式；其餘建置方式則免填。
4. 註 3：系統建置方式為「5. 主管/上級機關提供」得免填。

附表4 大陸品牌資通訊設備清冊

項次	財產編號	大陸品牌資通訊設備名稱	廠商名稱(全銜)	購置日期(年/月/日)	設備使用年限	是否與公務環境介接(是/否)	有無其他替代方案(請說明替代方案,若無則填無)	是否列冊管理(是/否)	預計汰換期程	預計汰換作為
~~1~~	~~3140101-03-3000084~~	~~Lenvo Idealpad S10~~	~~聯想~~	~~2009年1月20日~~	~~4年~~	~~否~~	~~預計2020年12月31前報廢~~	~~是~~	~~2022年12月31日~~	~~預計2022年12月31日前報廢~~

填表說明：

1.調查大陸品牌資通訊設備(建議由機關財產系統產出)

2.資通訊設備(參考資通安全管理法第 3 條用詞定義)：用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之硬體設備。

3.欄位說明

(1) 是否與公務環境介接：是否有連接公務網路或公務設備進行資料傳輸等行為。

(2) 有無其他替代方案：是否有其他國家或我國可替代之產品及方案。

(3) 是否列冊管理：是否定期進行盤點作業，執行該設備之安全性檢測或漏洞修補，並於跨部門之資通安全推動會議提出檢討。

(4) 預計汰換期程：請填寫預計汰換日期(年/月/日)。

(5) 預計汰換作為：請填寫預計汰換作為。

附表 5 資通安全責任等級調降為 D 級(D+級)之臺中市公立學校應辦事項執行期程表

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之二年內(預計於 109 年 5 月 5 日前)，針對自行或委外開發之資通系統，依資通安全責任等級分級辦法附表九完成資通系統分級，其後應每年至少檢視一次(預計於 109 年 12 月 31 日前檢視完成)資通系統分級妥適性，並完成全部資通系統附表十普級之控制措施。
	內部資通安全稽核自我檢查作業		結合學校內部管理機制，每年辦理一次(預計 109 年 12 月 31 日前完成)資通安全自我檢查作業。
	資通安全專責人員		初次受核定或等級變更後之一年內，(預計於 109 年 5 月 5 日前完成)配置一人為資訊（組長）兼任。
技術面	資通安全健診	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檢核措施完成 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	
		具有伺服器主機者，應檢視伺服器主機惡意活動	
		具有日錄伺服器者，應檢視日錄伺服器設定	
		具有防火牆者，應檢視防火牆連線設定	
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項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。 (預計於 109 年 12 月 31 日前完成所有電腦及資通系統防毒軟體、網路防火牆更新或升級)
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全人員	每年至少一名資通安全人員（預計於 109 年 12 月 31 日前完成）接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者及主管	每人每年（預計於 109 年 12 月 31 日前完成）接受三小時以上之一般資通安全教育訓練。

附件1年度資通安全教育訓練計畫

臺中市篤行國民小學 ~~109~~ OO 年度資通安全教育訓練計畫

壹、依據

臺中市篤行國民小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（本機關）之資通安全維護計畫，以強化（本機關）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:

本機關所屬人員：

人員類別	人數
資通安全專責人員	~~1~~ 0
一般人員	~~67~~ 73
主管人員（校長及主任）	8
共計	~~76~~ 81

肆、訓練項目（各機關自行定義）

人員類別	訓練課程	應取得時數
~~資通安全專責人員~~	~~電子郵件安全~~	~~12~~
~~資訊人員（系統管理者）~~	~~資訊系統風險管理~~	~~6~~
一般人員	資訊安全通識	3
主管人員	資訊安全通識	3

伍、訓練期程（~~109~~ ~~每~~年 12 月 31 日前完成訓練）

由各機關自行排定教育訓練期程。

陸、訓練方式

一、本機關採行教育訓練方式為實體課程~~及~~或線上課程。

二、未參加實體課程者，需至~~數位學習資源整合平臺「e 等公務園+學習平臺」(https://elearn.hrd.gov.tw)~~ 「edu 磨課師」https://moocs.moe.edu.tw/ 線上修習包含資安管理制度、社交工程攻擊防護、個人資料保護、行動裝置使用安全、物聯網資安威脅等資安課程取得上述應取得之研習時數。