高雄市苓洲國民小學

資通安全維護計畫

機密等級: 一般

承辦人簽章: 張○○

單位主管簽章：何○憲

校長(資安長)簽章： 吳○泰

中華民國 115 年 3 月 20 日

目　錄

壹、 依據 4
貳、 適用範圍 4
參、 核心業務及重要性 4
一、 核心業務及重要性： 4
二、 非核心業務及說明： 4
肆、 資通安全政策及目標 5
一、 資通安全政策 5
二、 資通安全目標 6
三、 資通安全政策及目標之核定程序 6
四、 資通安全政策及目標之宣導 6
五、 資通安全政策及目標定期檢討程序 6
伍、 資通安全推動組織 6
一、 資通安全長 6
二、 資通安全推動小組 7
陸、 專責人力及經費配置 8
一、 專責人力及資源之配置 8
二、 經費之配置 8
柒、 資通系統及資訊之盤點 9
一、 資通系統及資訊盤點 9
二、 機關資通安全責任等級分級 10
捌、 資通安全風險管理 10
一、 資通安全風險評估 10
二、 核心資通系統及最大可容忍中斷時間 10
玖、 資通安全防護及控制措施 10
一、 資通系統及資訊之管理 10
二、 存取控制與加密機制管理 11
三、 作業與通訊安全管理 11
四、 系統獲取、開發及維護 18
五、 業務持續運作演練 18

六、 執行資通安全健診.....18
七、 資通安全防護設備.....18
壹拾、資通安全事件通報、應變及演練相關機制.....19
壹拾壹、資通安全情資之評估及因應.....19
一、 資通安全情資之分類評估.....19
二、 資通安全情資之因應措施.....20
壹拾貳、資通系統或服務委外辦理之管理.....20
一、 選任受託者應注意事項.....20
二、 監督受託者資通安全維護情形應注意事項.....21
壹拾參、資通安全教育訓練.....21
一、 資通安全教育訓練要求.....21
二、 資通安全教育訓練辦理方式.....21
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22
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22
一、 資通安全維護計畫之實施.....22
二、 資通安全維護計畫實施情形之檢查機制.....22
三、 資通安全維護計畫之持續精進及績效管理.....23
壹拾陸、資通安全維護計畫實施情形之提出.....23
壹拾柒、相關法規、程序及表單.....24
一、 相關法規及參考文件.....24
二、 資通安全維護計畫附件表單.....24

壹、依據

本計畫依據下列法規訂定：

一、資通安全管理法第13條及其施行細則第9條。

二、其他相關業務法規名稱。

貳、適用範圍

本計畫適用範圍涵蓋高雄市苓洲國民小學全校 (以下簡稱本校)。

參、核心業務及重要性

一、核心業務及重要性

本校之核心業務及重要性如下表：

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
學校教務業務、學生事務、輔導業務管理	校務管理系統(向上集中)	為本校依組織法執掌，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。	由上級管理單位訂之

各欄位定義：

1. 核心業務：請參考資通安全管理法施行細則第10條之規定。
2. 核心資通系統：請列出支持核心業務運作必要之系統。
3. 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，對其他業務運作影響，法遵循性影響或其他重要性之說明。
4. 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。
5. 最大可容忍中斷時間單位以小時計。

二、非核心業務及說明

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
公文交換	電子公文無法即時送達機關，影響機關行政效率	由上級管理單位訂之
差勤管理	影響機關行政效率	由上級管理單位訂之
其他- 非屬上開業務範疇及核心業務者	影響機關行政效率	由上級管理單位訂之

1. 非核心業務：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。(請依機關實際情形列出)
2. 業務失效影響說明：說明該業務失效時之影響。
3. 最大可容忍中斷時間單位以小時計。

肆、資通安全政策及目標

一、資通安全政策

為使本校業務順利運作，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) 應建立資通安全風險管理機制，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。

(二) 應保護機敏資訊之機密性與完整性，避免未經授權的存取與竄改。

(三) 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。

(四) 針對辦理資通安全業務有功人員應進行獎勵。

(五) 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

(六) 禁止多人共用單一系統帳號。

(七) 落實資通安全通報機制。

二、資通安全目標

(一) 量化型目標：

1. 本校核心資通系統由上級或監督機關兼辦或代管，核心資通系統可用性由上級管理單位訂之。

2. 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。

3. 年度資安通報演練，能於規定時間內完成整備、通報演練及應變演練作業。

(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，有效預防資安事件發生。

三、資通安全政策及目標之核定程序

資通安全政策由本校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，向機關內所有人員進行宣導。

(二) 本校應每年向關注方(例如家長、志工、IT 服務供應商、與機關連線作業有關單位等)進行資安政策及目標宣導。

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中檢討其適切性。

伍、資通安全推動組織

一、資通安全長

依本法第12條之規定，本校訂定校長為資通安全長，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與相關業務人員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

本校之資通安全推動小組，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. 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. 資通安全技術之研究、建置及評估相關事項。

6. 資通安全相關規章與程序、制度之執行。

7. 資通系統及資訊之盤點及風險評估。

8. 資料之安全防護事項之執行。

9. 資通安全事件之通報及應變機制之執行。

10. 每年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。

11. 進行資通安全內部檢查。

12. 其他資通安全事項之規劃、辦理與推動。

陸、專責人力及經費配置

一、專責人力及資源之配置

(一) 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，設置專責人員兼辦資通安全業務，進行下列事項：

1. 資通安全認知與訓練業務，負責推動資通安全教育訓練等業務之推動。

2. 資通安全防護業務，負責資通安全防護設施建置及資通安全事件通報及應變業務之推動。

3. 資通安全管理法法遵事項業務，負責本校對所屬公務機關或所管特定非公務機關之法遵義務執行事宜。

(二) 本校之承辦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機關(構)提供顧問諮詢服務。

(三) 本校負責重要資通系統之管理、操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽署書面約定(資通安全保密同意書)，並視需要實施人員輪調，建立人力備援制度。

(四) 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。

(五) 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、經費之配置

(一) 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。

(二) 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。

(三) 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、資通系統及資訊之盤點

一、資通系統及資訊盤點

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

(二) 資訊資產項目如下：

1. 資料資產：以數位等形式儲存之資訊，如資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、稽核紀錄及歸檔之資料等。

2. 軟體資產：應用軟體、套裝軟體及電腦作業系統等。

3. 硬體資產：電腦及網路通訊設備、可攜式設備(如無人機、行動硬碟)、具連網功能之教學設備(如資訊整合控制器、大型顯示器、投影機)等。

4. 支援服務資產：相關基礎設施及其他機關內部之支援服務(含物聯網)，如監視系統、電力(EMS) 、消防、不斷電系統(UPS)等。

(三) 本校每年應依資通系統及資訊盤點結果，製作「資通系統清冊」及「資訊資產清冊」:

1. 「資通系統清冊」盤點應包含：系統名稱、管理者、使用者、辨別是否為核心資通系統。

2. 「資訊資產清冊」盤點應包含：資產名稱、類別、擁有者、管理者、使用者、廠牌名稱、型號、數量、存放位置。

(四) 資訊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。

(五) 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資通系統清冊及資訊資產清冊。

二、機關資通安全責任等級分級

本校配合資訊資源向上集中管理，資通系統均由上級或監督機關兼辦或代管，為資通安全責任等級 D 級機關。

捌、資通安全風險管理

一、資通安全風險評估

(一) 本校應每年進行資通安全風險評估。

(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「資通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)本校每年應依資通安全風險評估結果，製作「風險評估表」，並進行風險處理計畫。

二、核心資通系統及最大可容忍中斷時間

本校配合資訊資源向上集中管理，核心資通系統均由上級或監督機關兼辦或代管，不再另行訂定。

玖、資通安全防護及控制措施

本校依據前章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及資通系統之防護基準，採行相關之防護及控制措施如下：

一、資通系統及資訊之管理

(一) 資通系統及資訊之保管

1. 管理人應確保資通系統及資訊已盤點造冊並適切分級，並持續更新以確保其正確性。

2. 管理人應確保資通系統及資訊被妥善的保存或備份。

3. 管理人應確保重要之資通系統及資訊已採取適當之存取控制政策。

(二) 資通系統及資訊之使用

1. 本校同仁使用資通系統及資訊前應經其管理人授權。

2. 本校同仁使用資通系統及資訊時，應留意其資通安全要求事項，並負對應之責任。

3. 本校同仁使用資通系統及資訊後，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. 非本校同仁使用本校之資通系統及資訊，應確實遵守本校之相關資通安全要求，且未經授權不得任意複製資訊。

5. 對於資通系統及資訊，宜識別並以文件記錄及實作可被接受使用之規則。

(三) 資通系統及資訊之刪除或汰除

1. 資通系統及資訊之刪除或汰除前應評估機關是否已無需使用該等資通系統及資訊，或該等資通系統及資訊是否已妥善移轉或備份。

2. 資通系統及資訊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。

(四) 不得使用危害國家資通安全產品(含委外場域)

依據「資通安全管理法」第 11 條辦理。

1. 不得下載、安裝或使用危害國家資通安全產品，自行或委外營運所提供或使用之傳播設備或服務亦同。

2. 機關配發業務使用之資通訊設備，不得下載、安裝或使用危害國家資通安全產品，並應遵守相關法令規範。

3. 因業務需求且無替代方案者，經機關資安長及上級機關資安長核可，得以專案方式使用，並列冊管理，且不得與公務(業務)網路環境介接。

二、存取控制與加密機制管理

(一) 網路安全控管

1. 本校之網路區域劃分如下：

(1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

(2) 內部區域網路 (Local Area Network, LAN) ：機關內部單位人員使用之網路區段。

2. 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的

服務與來源不能進入其他區域。

3. 若有獨立上網線路需求，應向資安推動小組申請並敘明線路用途、權責、使用限制，經資通安全長核准後辦理，並由本校列管。

4. 本校應定期檢視防火牆政策及設定是否適當，並適時進行防火牆軟、硬體之必要更新或升級。若為向上集中管理，則由上級單位辦理更新與升級。

5. 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。若為教育局統一配發或集中管理者，所有記錄均儲存於「資安資訊」平台中。

6. 若需從外部遠端連線，需填寫遠端連線申請單，申請後才可開通，建議每次以4小時為限，若需延長得重新申請，不得24小時全開。網管老師及保全系統則不在此限。

7. 本校內部區域網路應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

8. 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

9. 使用者應依規定之方式存取網路服務，不得於校內私裝電腦及網路通訊等相關設備。

10. 網域名稱系統(DNS)防護：

(1) 本校使用教育局教育網路中心建置 DNS 代管服務。

(2) 防火牆政策針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

(3) 本校內部電腦 DNS 查詢應指向教育網路中心使用者端專用 DNS。

11. 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) 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

(3) 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。

(4) 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. 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大寫小寫、特殊符號或數字三種以上。

   (3) 通行碼如係由系統或相關承辦人員預設，應告知使用者於首次使用系統時變更通行碼，或由系統強制執行。

   (4) 使用者每 90 天應更換一次通行碼。

   (5) 如為特定系統因功能限制，通行碼設定與更改作業無法完全符合前項要求，得經核准後，調整該系統之通行碼設定要求或密碼變更頻率。

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記錄外，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) 使用者責任

1. 使用者之通行碼應妥善保管，避免他人知悉。

2. 應取消資通系統、瀏覽器等之密碼自動記憶功能，避免密碼遭截取或竊用。

3. 使用者離開主機或個人電腦時，應關閉電腦螢幕或啟動鎖定功能，以確保資料之安全。若超過15分鐘未使用主機或個人電腦，須設定螢幕密碼保護或強制登出措施。

(四) 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，其授權及審查紀錄應留存。

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。

(五) 加密管理

1. 本校之機密資訊於儲存或傳輸時應進行加密。

2. 本校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。

(4) 透過網際網路對外提供服務之網站或應用系統，應採用未被破解之公開演算法進行加密傳輸，例如 TLS 1.3 或 IPSEC。

(六) 作業系統存取控制

1. 調整主機或個人電腦安全性設定，以滿足使用者存取管理需求。

2. 依各資料夾(目錄)之用途，設定適當使用權限。

3. 應關閉所有網路資源分享服務，如因業務需求須使用網路資源分享服務，須經權責主管同意。

4. 啟用稽核原則(如：登入失敗之 Windows 稽核)，保留相關稽核紀錄。

5. 主機或個人電腦之作業系統，應啟動本機防火牆，並以最小且必要之原則開放連線存取服務。

6. 登入主機或個人電腦之作業系統，若超過時限無任何動作時，須設定將使用者 ID 鎖定或登出。

三、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本校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) 防毒軟體應設定為自動更新，啟動即時防範機制，並定期執行完整掃描作業。

(2) 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。

(3) 電子郵件附件及下載檔案於使用前，宜先掃描有無惡意軟體。

(4) 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. 設備管理及使用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. 本校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：

(1) 以提供遠端桌面或虛擬桌面存取為原則，以防止於私有設備上處理及儲存資訊。

(2) 外部網路(External Network)對本校資通系統之遠距工作防火牆連線期限以不超過 15 天為原則。

(3) 應明確指定來源 IP 位址、目的 IP 位址、目的通訊埠及協定等選項，避免任一選項設定全部(Any)。

(三) 電子郵件安全管理

1. 本校人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。

2. 電子郵件系統管理人應定期進行電子郵件帳號清查。

3. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新，若為向上集中管理，則由上級單位統一辦理。

4. 使用者使用機關所提供電子郵件服務，應僅限於公務用途，且不得使用非公務信箱進行公務郵件收發、不得從事侵害他人權益或違法之行為，亦不得作為商業用途。

5. 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

6. 原則上，不得透過電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

7. 使用者應確保電子郵件傳送時之傳遞正確性。

8. 使用者使用電子郵件時，應注意電子簽章之要求事項。

9. 配合上級機關舉辦電子郵件社交工程演練，並檢討執行情形。

(四) 確保實體與環境安全措施

1. 通訊機房之門禁管理

(1) 通訊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通訊機房，通訊機房管理者並應定期檢視授權人員之名單。

(3) 進入前應先進行身分識別，並隨時注意身分不明或可疑人員。

(4) 僅於必要時，得准許外部支援人員進入通訊機房。

(5) 人員及設備進出通訊機房應留存記錄。

2. 通訊機房之環境控制

(1) 通訊機房之電力應建立備援措施。

(2) 通訊機房應有適當的溫溼度管控措施：機房內應有溫濕度顯示裝置，以觀察實際之溫濕度情況。

(3) 通訊機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、入侵者偵測系統，以減少環境不安全引發之危險。

(4) 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下班時，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. 本校應每季確認資通系統資料備份之有效性。
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，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，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享(P2P)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. 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，應主動循本校通報程序進行通報。
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

(九) 即時通訊軟體之安全管理

1. 使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。

2. 使用於傳遞公務訊息之即時通訊軟體宜考量下列安全性需求：

(1) 用戶端應有身分識別及認證機制。

(2) 訊息於傳輸過程應有安全加密機制。

(3) 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。

(4) 伺服器端之主機設備及通訊紀錄應置於我國境內。

(5) 伺服器通訊紀錄(Log)應至少保存六個月。

四、系統獲取、開發及維護

本校之資通系統依「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，依分級之結果為 D 級，未維運自行或委外開發之資通系統，故不再另行訂定。

五、業務持續運作演練

本校為 D 級機關，無需針對核心資通系統制定業務持續運作計畫與演練。

六、執行資通安全健診

本校為 D 級機關，無需執行資通安全健診。

七、資通安全防護設備

(一) 本校應建置防毒軟體、防火牆，持續使用並適時進行軟、硬體之必要更新或升級。若為向上集中管理，則由上級單位統一辦理更新與升級。

(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。若為向上集中管理，則由上級單位統一辦理。

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，本校應遵循資通安全事件通報、應變及演練相關機制，詳細狀況請參閱「臺灣學術網路各級學校資通安全通報應變作業程序」。

壹拾壹、 資通安全情資之評估及因應

本校接獲臺灣學術網路資安監控系統(南區 SOC、Mini-SOC、TACERT)之資通安全情資，應評估該情資之內容，並視其對本校之影響、本校可接受之風險及本校之資源，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

本校接受資通安全情資後，應進行情資分析，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學校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

本校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

本校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) 應與受託者簽訂書面契約，載明雙方之權利義務及違約責任。

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) 本校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) 本校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小時以上之資通安全通識教育訓練。

(二) 資通安全專職人員以外之資訊人員(資訊組長及專責人員)，每二年接受3小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受3小時以上之資通安全通識教育訓練。

二、資通安全教育訓練辦理方式

(一) 承辦單位應於每年辦理資通安全認知宣導及教育訓練，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) 本校資通安全認知宣導及教育訓練之內容得包含：

1. 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。

(三) 員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

(四) 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

本校所屬人員之平時考核或聘用，依據公務機關所屬人員辦理資通安全事項作業辦法，及本校各相關規定辦理之。

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

為落實本法，使本校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、資通安全維護計畫實施情形之檢查機制

(一) 檢查機制之實施

1. 資通安全推動小組應定期(至少每年一次)或於系統重大變更或組織改造後執行自我內部資通安全檢查，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. 資通安全推動小組應配合教育局年度「資訊安全專案檢查實施計畫」及「數位發展部資通安全署資通安全作業管考系統」，參考其檢查項目辦理檢查作業，並應將前次檢查結果納入檢查範圍。

3. 執行檢查後，應依檢查結果填報於當年度教育局「資訊安全專案檢查表」。

4. 檢查結果應對相關管理階層(含資安長)報告並留存檢查過程之相關紀錄。

(二) 檢查改善報告

1. 檢查實施後發現有缺失或待改善項目者，應判定其發生之原因，並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，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。

2. 於執行改善措施時，應留存相關之執行紀錄，並填寫維護計畫實施情形檢查結果及改善報告。

三、資通安全維護計畫之持續精進及績效管理

(一) 本校之資通安全推動小組應每年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) 資通安全政策及目標之實施情形。

(2) 資通安全人力及資源之配置之實施情形。

(3) 資通安全防護及控制措施之實施情形。

(4) 實施情形檢查結果。

(5) 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. 關注方之回饋。

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

本校依據資通安全管理法第 14 條之規定，每年向上級或監督機關，提出上年度資通安全維護計畫實施情形(須填報數位發展部資通安全署資通安全作業管考系統)，使其得瞭解本校之年度資通安全計畫實施情形。

壹拾柒、 相關法規、程序及表單

一、相關法規及參考文件

(一) 資通安全管理法

(二) 資通安全管理法施行細則

(三) 個人資料保護法

(四) 資通安全責任等級分級辦法

(五) 資通安全事件通報應變及演練辦法

(六) 資通安全情資分享辦法

(七) 公務機關所屬人員辦理資通安全事項作業辦法

(八) 資通系統風險評鑑參考指引

(九) 政府資訊作業委外資安參考指引

(十) 無線網路安全參考指引

(十一) 網路架構規劃參考指引

(十二) 行動裝置資安防護參考指引

(十三) 安全軟體發展流程指引

(十四) 安全軟體設計參考指引

(十五) 安全軟體測試參考指引

(十六) 行政院及所屬各機關資料中心設置作業要點

(十七) 高雄市政府內部控制監督作業規範

(十八) 臺灣學術網路各級學校資通安全通報應變作業程序

(十九) 本校資通安全事件通報及應變程序

(二十) 學校使用資通系統或服務蒐集及使用個人資料指引

(二十一) 學校使用生物特徵辨識技術個人資料保護指引

二、資通安全維護計畫附件表單

(一) 資通安全推動小組成員及分工表

(二) 資通安全保密同意書

(三) 資通安全需求申請單

(四) 資訊資產清冊

(五) 資通系統清冊

(六) 風險評估表

(七) 風險類型暨風險對策參考表

(八) 管制區域人員進出登記表

(九) 委外廠商執行人員保密切結書、保密同意書

(十) 委外廠商查核項目表

(十一) 資通安全教育訓練計畫

(十二) 資通安全認知宣導及教育訓練簽到表

(十三) 資通安全維護計畫實施情形

(十四) 維護計畫實施情形檢查結果及改善報告

(十五) 改善績效追蹤報告