嘉義市崇文國民小學

資通安全維護計畫

機密等級：一般

承辦人簽章：

（資安長）簽章：

中華民國 113 年 7 月 30 日

嘉義市崇文國民小學

資通安全維護計畫

機密等級：一般

承辦人簽章：

(資安長)簽章：

中華民國 113 年 7 月 30 日

資通安全維護計畫

目　　錄

壹、依據及目的

依據資通安全管理法第 10 條及施行細則第 6 條，訂定資通安全維護計畫(以下簡稱本計畫)，作為嘉義市崇文國民小學(以下簡稱本校)資訊安全推動與降低資安風險，並符合法令法規之依循。

貳、適用範圍

本計畫適用範圍涵蓋本校全機關。

參、核心業務及重要性

一、 資通業務及重要性：

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
教務業務	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	24
	全國在職進修網			
	校長暨教師專業發展支持平臺			
學務業務	教育部校園安全暨災害防救通報處理中心	為本校依組織法執掌，足認為重要者	影響學校部分學務業務運作	24
	學生健康資訊系統 SSHIS			
	校園性別事件回復填報及統計管理系統			
	環教終身學習網			
總務業務	政府電子採購網	為本校依組織法執掌，足認為重要者	影響學校部分總務業務運作	24
	雲端公文系統			
	公共工程雲端服務網			
	勞保局 e 化服務			

	系統			
	EMIC - 中央災害應變中心			
	嘉義市政府公有財產管理系統			
輔導業務	教育部特殊教育通報網	為本校依組織法執掌，足認為重要者	影響學校部分輔導業務運作	24
	高級中等以下學校輔導工作成果填報系統			
	教育部學生轉銜輔導及服務系統			
	社會安全網 -關懷ｅ起來			
	國民小學及國民中學學生學習扶助科技化評量			
人事業務	差勤電子表單系統	為本校依組織法執掌，足認為重要者	影響學校部分人事業務運作	24
	公教人員退休撫卹試算系統			
	ｅ等公務園學習平臺			
會計業務	地方發展教育基金會計資訊系統	為本校依組織法執掌，足認為重要者	影響學校部分會計業務運作	24

備註:表格可自行延伸。

各欄位定義：

1. 核心業務名稱：請參考資通安全管理法施行細則第 7 條之規定列示。

2. 作業名稱：該項業務內各項作業程序的名稱。

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，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

4. 最大可容忍中斷時間單位以小時計。

二、 非核心業務及說明：

非核心業務及說明如下表:

非核心業務	非核心資通系統	業務失效影響說明	最大可容忍中斷時間
防火牆	防火牆系統	資安防護部分業務無法運作	24
監視器	監視器等 IOT 系統	監視器部分業務無法運作	24
郵件服務	教育部校園雲端電子郵件	電子郵件部分業務無法運作	24

備註:表格可自行延伸。

各欄位定義：

1. 業務名稱：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. 作業名稱：該項業務內各項作業程序的名稱。

3. 說明：說明該業務之內容。

4. 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：

1. 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。

2. 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。

3. 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。

4. 針對辦理資通安全業務有功人員應進行獎勵。

5. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

6. 禁止多人共用單一資通系統帳號。

7. 校內同仁及外部廠商須簽屬相關資通安全保密切結與同意書。

8. 落實資通安全通報機制。

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惡意郵件開啟率需在 10%(含)以下；惡意郵件點閱率需在 6%(含)以下。

3. 每人每年接受三小時以上之一般資通安全教育訓練。

(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、防止發生中毒或入侵事件。

三、資通安全政策及目標之核定程序

資通安全政策簽陳本校校長核定並公告之。

四、資通安全政策及目標之宣導

1. 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，向所有人員進行宣導，並檢視執行成效。

2. 新職員到職時，應告知閱讀本校資通安全政策及資通安全管理相關規定，並簽署「員工保密暨使用合法軟體切結書」(附件表單一)，克盡保密之責。

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

依資通安全法第 11 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：

1. 資通安全管理政策及目標之核定及督導。

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

(一) 組織

本校設置「資通安全推動小組」負責督導校內資訊安全相關事項，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業務人員代表或各處室主任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。

(二) 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(附件表單二)，並適時更新之：

1. 資通安全推動小組：

(1) 資通安全政策及目標之研議。

(2) 訂定本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年度工作計畫。

(4) 傳達資通安全政策與目標。

(5) 其他資通安全事項之規劃。

(6) 資訊及資通系統之盤點及風險評估。

(7) 資通安全相關規章與程序、制度之執行。

(8) 資料及資通系統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

陸、專責人力及經費配置

一、專責人力及資源之配置

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，本校現有資通安全人員名單及職掌列於「資通安全推動小組成員及分工表」(附件表單二)。

2. 本校之承辦單位於辦理資通安全業務時，應加強資通安全人員之培訓，並提升校內資通安全專業人員之資通安全管理能力。如資通安全人力或經驗不足，得洽請嘉義市教育處或相關專業機關（構）之人員，提供顧問諮詢服務。

3. 本校校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。

4. 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

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. 資通安全經費、資源之配置情形應每年定期檢討並填寫「經費配置表」(附件表單三)，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

1. 本校每年辦理資訊及資通系統資產盤點，依管理責任及使用人員指定對應之資產管理人，並依資產屬性進行分類，分別為資訊類、硬體類、軟體類、服務類、人員類等 5 大類。

2. 資訊及資通系統資產項目如下：

資產類別	資產項目
資訊類資產	1. 業務資料檔案，例如：XX 業務檔案。 2. 系統資料檔案，例如：資料庫檔案、應用程式檔案及備份檔案等。 3. 電子化儲存之文件檔案，例如：系統或軟體使用手冊及教育訓練教材等。 4. 書面管理文件，例如：系統文件、使用手冊、各種程序及指引辦法等。 5. 書面紀錄，例如：申請表單及採購等。
硬體類資產	1. 電腦設備，例如：伺服器、工作站、個人主機、筆記型電腦及 PDA 等。 2. 通訊設備，例如：路由器、網路交換器、數據機、傳真機、印表機、影印機及物聯網設備等。 3. 儲存媒體，例如：隨身碟、磁帶、磁帶機、磁帶櫃、光碟及光碟機等。 4. 其他支援設備，例如：監視器、不斷電系統、空調系

資產類別	資產項目
	統、消防系統、環控系統及機房用發電機等。
軟體類資產	1. 系統軟體，例如：公文系統、官網系統等。 2. 資料庫軟體，例如：ORACLE、SQL Server 等。 3. 套裝軟體，例如：Windows 10、 Windows Office 等。
服務類資產	1. 一般維運支援性服務，例如：中華電信網路專線、市電系統、供水服務等。 2. 委外服務，例如：XX 公司網路安全服務、XX 公司設備主機維護服務等。
人員類資產	1. 內部同仁，例如：資訊處同仁、專案工作人員及計畫約聘人員等。 2. 外部(常駐型)人員，例如：XX 公司駐點人員等。

3. 本校每年度應依資訊及資通系統盤點結果，製作「資通資產清冊」(附件表單四)，如資產有異動，應即時更新。

4. 資訊及資通系統之硬體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。

5. 對於大陸品牌資通訊設備，應造冊並列管(附件表單五)。

二、機關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，資通安全責任等級為 D 級。

捌、資通安全風險評估

一、資通安全風險評估

1.本校應每年針對資訊及資通系統資產進行風險評估，將結果填寫於「風險評鑑彙整表」(附件表單六)。

2. 資通資產價值評分定義參考如下：

防護需求等級 / 構面	高(3)	中(2)	普(1)
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，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。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，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。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，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。	產生嚴重之影響。	產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

資產價值＝取四構面最高值（機密性價值，完整性價值，可用性價值，法律遵循性價值)。

3. 鑑別風險:

針對單一資產失效情境分析，依據下方之等級表分析其對資產所可能造成的威脅發生可能性等級及脆弱性利用難易度，風險值＝資產總價值 X 脆弱性利用難易度 X 威脅發生可能性等。

表：脆弱性利用難易度等級表

等級	脆弱性利用難易度分級原則
普(1)	● 僅限深入了解脆弱性技術，並於特定條件或環境下方能利用脆弱性 ● 不會損害資訊及資通系統資產，或是受到損害後能立即回復 ● 必須運用特殊的方法才能利用脆弱性進行攻擊 ● 威脅來源必須花費長時間（可能需一個月以上）的資料蒐集，突破各層防護，才能接觸到關鍵資訊

	● 攻擊成功：可能要 1~數個月以上 ● 可能之原因 – 管理防護機制完備並落實實施（例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統經過完整測試等皆落實進行） – 資訊或處理設備的使用手冊完整或說明清晰 – 使用者或管理者受過完整教育訓練，對資訊處理設備操作熟練 – 使用者或管理者對資訊處理程序熟悉 – 技術性防護機制完備（例如資訊採用加密保護、網路區隔並採用安全設備監控系統效能、容量及安全事件；有效管理入侵/病毒/木馬、備援線路） – 可被利用的方法的技術層次高或技術不容易取得實體環境的特性（例如劃分安全區域並實施監控與出入管控、環境溫濕度控管、建築物或防護設施材質等）讓威脅源被杜絕
中(2)	● 具備了解脆弱性技術知識，方能利用脆弱性 ● 資訊及資通系統資產受到損害，且無法立即回復 ● 不需用特殊的方法就能利用脆弱性進行攻擊 ● 已實施保護的機制，威脅來源必須花費一段時間（可能是數天）進行資料蒐集始能接觸到關鍵資訊 ■ 攻擊成功：可能是數天以上 ● 可能之原因 – 已建立管理防護機制但未落實（例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統測試等） – 資訊或處理設備的使用手冊過於簡單或說明不詳細 – 使用者或管理者雖受過教育訓練，但對資訊處理設備操作不熟練 – 使用者或管理者對資訊處理程序不熟悉

	- 雖實施技術性防護機制（例如資訊採用加密保護、網路區隔並採用安全設備、監控系統效能、容量及安全事件；有效管理入侵/病毒/木馬、備援線路）但是設定或防護能力不足 - 可被利用的方法的技術層次高但技術容易取得 - 實體環境的特性（例如未劃分安全區域出入管控、環境溫濕度控管不足及建築物或防護設施材質等）讓威脅源存在
高(3)	● 任何人不需具備任何能力均能有意或無意的利用脆弱性 ● 資訊及資通系統資產受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊及資通系統資產消失無法復原 ● 利用簡易的方法就能利用脆弱性進行攻擊 ● 未實施保護或保護機制無效，威脅來源於短期內即可攻擊成功 ● 攻擊成功：可能是一天內到數天 ● 可能之原因 - 管理防護機制缺乏（例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統測試等）-缺乏資訊或處理設備的操作手冊或手冊錯誤 - 使用者或管理者未受過教育訓練，或對資訊處理設備操作不熟練 - 使用者或管理者對資訊處理程序不了解 - 缺乏技術性防護機制（例如資訊採用加密保護、網路區隔並採用安全設備、監控系統效能、容量及安全事件；有效管理入侵/病毒/木馬、備援線路） - 可被利用的方法其技術層次低且容易取得 - 實體環境的特性（例如未劃分安全區域出入管控、環境溫濕度控管不足及建築物或防護設施材質等）讓威脅源持續存在

表：威脅發生可能性等級表

等級	威脅發生可能性等級分級原則
普(1)	風險發生可能性低，每年至多可能發生 1 次。
中(2)	風險發生可能性中，每季有可能發生 1 次。
高(3)	風險發生可能性高，每月有能發生 1 次。

二、資通安全風險之因應

本校依風險評鑑結果，決定可接受之風險值，針對超出風險者，擬定並填寫「風險處理計畫表」(附件表單七)進行因應。

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. 本校同仁使用資訊及資通系統前應經其管理人授權。
2. 本校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. 非本校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，並由相關人員監督銷毀過程。

二、存取控制與加密機制管理

(一) 網路安全控管：

1. 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) ：機關內部單位人員及內部伺服器使用之網路區段。

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. 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。

4. 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，均應予確實記錄於「防火牆規則管制表」(附件表單八)；如需新增、異動規則，需填寫「防火牆存取控制申請單」(附件表單九)。

5. 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。

6. 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。

7. 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) 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) 使用者每 90 天應更換一次通行碼。

2. 使用者使用資通系統前應填寫「資通系統帳號註冊/註銷/異動申請單」(附件表單十)經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要(註1)經核准並紀錄外，不得共用 ID。

(註 1)：特殊營運或作業必要，例如電腦教室代課老師共用 ID，惟該共用 ID 應確保最小使用之授權原則，以降低 ID 外洩或誤用之風險。

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. 資通系統之管理者應定期清查系統特權帳號，並將結果填寫於「系統帳號權限清單」(附件表單十一)。

(四) 加密管理

1. 機密資訊於儲存或傳輸時應進行加密。

2. 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) 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. 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，應經資通安全推動小組同意後始可開通使用。

2. 遠距工作開放以一日為限。

3. 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。

(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) 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。

(3) 本校同仁之公務信箱不得用於私人事務，並應配合教育部及主管機關進行必要之社交工程演練。

(四) 確保實體與環境安全措施

1. 電腦機房/機櫃之門禁管理

(1) 電腦機房/機櫃應進行實體隔離。

(2) 機關人員或來訪人員應申請及授權後方可進入電腦機房/開啟機櫃，管理者並應定期檢視授權人員之名單。

(3) 人員及設備進出應填寫「電腦機房人員出入/開啟機櫃登記表」(附件表單十二)留存記錄。

(4) 設備應定期執行檢查，並記錄於「 電腦機房設施檢查表」(附件表單十三)。

2. 電腦機房之環境控制

(1) 電腦機房之空調、電力宜建立備援措施。

(2) 機房溫度應維持在 18℃至 28℃，溼度維持在 30%RH 至 70%RH。

(3) 電腦機房應安裝之安全偵測及防護措施，包括溫濕度監控設備、熱度或煙霧偵測設備(或火災警報設備)、入侵者偵測系統等，以減少環境不安全之危險。

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) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(五) 資料備份

1. 重要資料及資通系統應進行資料備份，執行異機或異地存放，定期確認重要資料備份之有效性，並填寫「重要檔案備份檢查表」(附件表單十四)。

2. 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. 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，應主動循本校之通報程序通報。
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

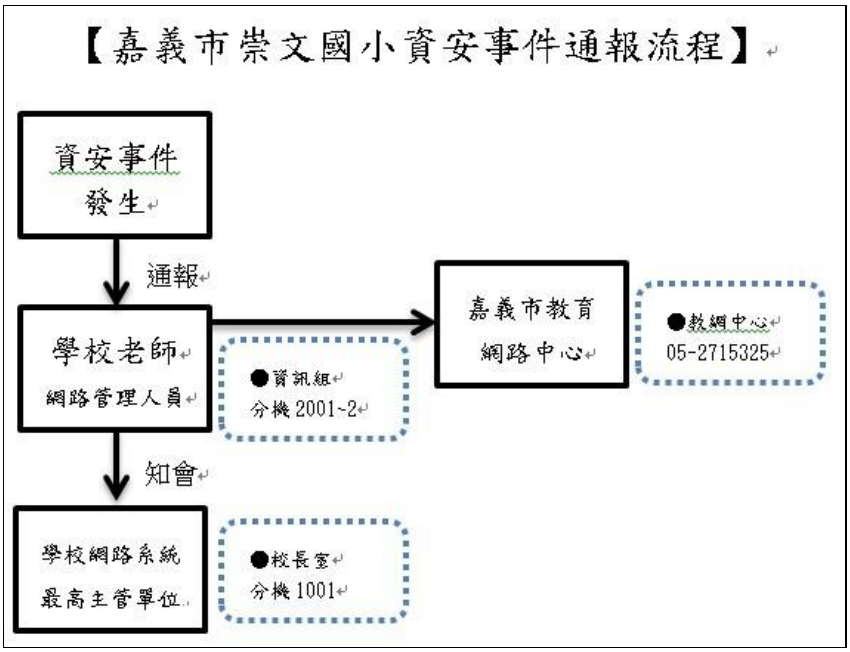
1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入

四、資通安全防護設備

1. 應建置防毒軟體及網路防火牆，持續使用並適時進行軟、硬體之必要更新或升級。
2. 資安設備應定期備份日誌紀錄，定期檢視並檢討執行情形。

壹拾、資通安全事件通報、應變及演練

為即時掌控資通安全事件，並有效降低其所造成之損害，依本校「資通安全事件通報應變程序」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

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、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，應指定資通安全人員進行情資分析，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。

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。

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

1. 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。

2. 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。

二、監督受託者資通安全維護情形應注意事項

1. 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 1 小時內通知委託機關及採行之補救措施。

2. 受託者於簽約時，需同時交付「委外廠商保密承諾書」(附件表單十五)及「委外廠商人員保密切結書」(附件表單十六)。

3. 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。

4. 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，使用「委外廠商查核項目表」(附件表單十七)進行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

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 小時以上之一般資通安全教育訓練。

二、資通安全教育訓練辦理方式

1. 承辦單位應每年年初，考量管理、業務及資訊等不同工作類別之需求，規劃資通安全認知宣導及教育訓練課程，以建立人員資通安全認知，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。

2. 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。

3. 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。

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資通安全事項獎懲辦法、嘉義市政府及所屬機關學校公務人員平時獎懲標準表、嘉義市政府及所屬機關學校約聘僱人員考核要點辦理之。

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稽核機制

1.稽核機制之實施

(1) 資通安全推動小組應定期(至少每年一次)執行一次內部稽核作業，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。

(2) 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫(附件表單十八)並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

(3) 辦理稽核時，資通安全推動小組應於執行稽核前 14 日，通知受稽核單位，並將稽核期程、稽核項目及稽核流程等相關資訊提供受稽單位。

(4) 本校之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具「資通安全內部稽核表」(附件表單十九)，待稽核結束後，應將稽核表內容彙整至稽核報告中(附件表單二十)，並提供給受稽單位填寫改善辦理情形。

(5) 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

(6) 受稽單位於稽核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，判定其發生之原因、研議改善措施、改善進度規劃，並填寫「資通安全矯正處理單」(附件表單二十一)落實執行。

(7) 資通安全推動小組應審查追蹤受稽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。

三、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。

(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. 資通安全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. 資通安全防護及控制措施之實施情形。

D. 不符合項目及矯正措施。

(4) 風險評鑑結果及風險處理計畫執行進度。

(5) 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(附件表單二十二)，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

依據資通安全管理法第 12 條之規定，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。

壹拾柒、限制使用危害國家資通安全產品

一、 依據「各機關對危害國家資通安全產品限制使用原則」辦理。

二、 資通訊產品使用原則：

1. 各機關辦理採購時，考量資安疑慮，應確實於招標文件規定不允許大陸地區廠商及陸籍人士參與，並不得採購及使用大陸廠牌資通訊產品。
2. 公務設備不得下載安裝大陸地軟體(含 App)，公務活動不得使用大陸地所提供之平臺或服務。
3. 機關應對同仁宣導量避免購買或使用大陸廠牌資通訊產品，並落實要求大陸廠牌資通訊產品一律禁止處理公務事務或介接公務環境。
4. 督導汰換作業推動：本機關資安長應負起督導之責，推動落實汰換作業。

壹拾捌、相關法規、程序及表單

一、相關法規及參考文件

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. 資通安全事件通報及應變辦法
5. 資通安全情資分享辦法
6. 公務機關所屬人員資通安全事項獎懲辦法
7. 資訊系統風險評鑑參考指引
8. 政府資訊作業委外安全參考指引
9. 資訊作業委外安全參考指引
10. 本校資通安全事件通報及應變程序
11. 各機關對危害國家資通安全產品限制使用原則

二、附件表單

1. 員工保密暨使用合法軟體切結書
2. 資通安全推動小組成員及分工表
3. 經費配置表
4. 資通資產清冊
5. 大陸品牌資通訊設備清冊
6. 風險評鑑彙整表
7. 風險處理計畫表
8. 防火牆規則管制表
9. 防火牆存取控制申請單
10. 資通系統帳號註冊註銷異動申請單
11. 系統帳號權限清單
12. 電腦機房人員出入登記表
13. 電腦機房設施檢查表
14. 重要檔案備份檢查表
15. 委外廠商保密承諾書
16. 委外廠商人員保密切結書
17. 委外廠商查核項目表
18. 資通安全內部稽核計畫
19. 資通安全內部稽核表
20. 資訊安全內部稽核報告
21. 資通安全矯正處理單
22. 審查結果及改善報告