國立羅東高級中學

115年度資通安全維護計畫

目　錄

壹、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。

貳、適用範圍

本計畫適用範圍涵蓋本校。

參、核心業務及重要性

一、 核心業務及重要性：

本機關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	資通系統分級
本校學生事務	**校務行政系統(向上集中)**	為主管機關核定資通安全責任等級 D 級機關所涉業務	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。	**48小時**	**中**
本校學生事務	**學生學習歷程系統(向上集中)**	學生學習歷程檔案	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。	**48小時**	**中**
本校事務	**電子郵件(向上集中)**	電子郵件	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。	**48小時**	**中**
本校學生事務	**學校首頁(向上集中)**	學校官方網站	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。	**48小時**	**中**
本校學生事務	**網域解析(向上集中)**	DNS 解析	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。	**48小時**	**中**

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7條之規定列示。

1. 核心資通系統：該項業務內各項作業程序的名稱。

2. 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。

3. 業務失效影響說明：當系統失效時對學校所造成的衝擊及影響。

4. 最大可容忍中斷時間單位以小時計。

5. 資通系統分級：依據資通安全責任等級分級辦法附件九資通系統防護需求分級原則進行分級。

二、 非核心業務及說明：

本機關之非核心業務及說明如下表：(時間採工作日計算)

項次	非核心業務	業務失效影響說明	最大可容忍斷時間	資通系統分級
1	公文系統	電子公文無法即時送達本校，影響機關行政效率	48小時	普
2	主計及零用金系統	無法請購，主計無法作業，影響機關行政效率	48小時	普
3	庶務管理財管系統	影響機關行政效率	48小時	普
4	雲端差勤管理系統(向上集中	人事室差勤管理系統	48小時	普
5	場地預約系統(向上集中)	影響機關行政效率	72小時	普
6	自主學習平台(向上集中)	學生登記自主學習計畫及執行	72小時	普
7	無聲廣播 eSchool	校園電視無聲廣播	72小時	普
8	圖書館館藏管理系統	影響學生借還書與書籍查詢	72小時	普
9	校園刊物平台	校園刊物	72小時	普
10	課表排課系統	課表排課調代課平台失效改為紙本調代課	72小時	普
11	學生刷卡到校	學生刷卡到校無法靠卡失效改為學生點名	72小時	普
12	選課系統	改為人工紙本調查選課	72小時	普

肆、資通安全政策及目標

參考本校「資訊安全政策」(文件編號：LDSH-ISMS-A-001)相關規定。

伍、資通安全推動組織

一、 資通安全長

依本法第11條之規定，本機關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、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、 資訊安全委員會

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，特成立「資訊安全委員會」。委員會之組織架構、任務、分工及職掌參考本校「資訊安全組織程序書」(文件編號：LDSH-ISMS-B-001)之規定辦理。

陸、專職(責)人力及經費配置

一、 專職(責)人力及資源之配置

1. 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D+級，最低應設置資通安全專責人員1人，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[1]。
2. 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。本機關之相關單位於辦理資通安全業務時，如資通安全人力或經驗不

[1]各公務機關應製作「資通安全專職人員分工表」，說明專職人員及相關職掌，格式可參附件：資通安全推動小組成員及分工表。

足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

3. 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[2]。

4. 本機關負責重要資通系統之管理、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[3]，並視需要實施人員輪調，建立人力備援制度。

5. 本機關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。

6. 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

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[4]。

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. 各單位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[5]，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。

柒、資訊及資通系統之盤點

一、 資訊及資通系統盤點

參考本校「資訊資產管理程序書」(文件編號：LDSH-ISMS-B-003)之規定辦理。

[2]各機關應依據其資通安全責任等級分級辦法所規範之資通安全專責人員、認知與訓練之要求，配置適當之資源於資安人員專業職能之培養。

[3]格式可參附件：資通安全保密同意書。

[4]為有效建置機關之資通安全風險防護機制，公務機關應投入相當之資源，故機關之資通安全推動小組於資源規劃或編制預算時，應考量機關之責任等級、資通安全政策及目標。

[5]各機關可填具資通安全需求申請單，格式可參附件：資通安全需求申請單。

二、 機關資通安全責任等級分級

依據臺教國署資字第1130011602號函，本校資通安全等級分類核定為 D 級機關。

捌、資通安全風險評估

一、 資通安全風險評估

參考本校「風險評鑑與管理程序書」(文件編號：LDSH-ISMS-B-004)之規定辦理。

二、 核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	最大可容忍中斷時間	核心資通系統主要功能
校務行政系統	1. 校務行政系統平台 2. 學籍資料庫、成績資料庫	48小時	提供學生學籍管理、成績管理、缺曠管理等服務
學生學習歷程系統	廠商雲端服務	48小時	提供學生上傳學習歷程檔案
電子郵件	教育部 mail 系統	48小時	收發信件
學校首頁	學校官方網站	48小時	訊息傳播
網域解析	DNS 名稱解析	48小時	名稱解析

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核心資通系統之防護基準，採行相關之防護及控制措施，由於本校核心資通系統已依據「教育體系資通安全暨個人資料管理規範」導入資通安全管理制度，相關之防護及控制措施參考本校「實體安全管理程序書」(文件編號：LDSH-ISMS-B-006)、「通信與作業管理程序書」(文件編號：LDSH -ISMS-B-007)、「存取控制管理程序書」(文件編號：LDSH -ISMS-B-008)、「系統開發與維護程序書」(文件編號：LDSH -ISMS-B-009)及「業務永續運作管理程序書」(文件編號：LDSH -ISMS-B-012)之規定辦理。

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，本機關應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序[6]。

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。

[6]各機關應另訂定資通安全事件通報及應變程序。

(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。相關委外作業之安全管理參考本校「委外管理程序書」(文件編號：LDSH -ISMS-B-010)之規定辦理。

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，非資通專責人員之外之資訊人員每兩年接受3小時以上之專業教育訓練。

二、 資通安全教育訓練辦理方式

參考本校「人員安全與教育訓練程序書」(文件編號：LDSH -ISMS-B-005)之規定辦理。

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，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機制

資訊安全稽核小組應定期(至少每二年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，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。本安全維護計畫之稽核及矯正機制，參考本校「資訊安全稽核作業程序書」(文件編號：LDSH-ISMS-B-013)及「矯正管理程序書」(文件編號：LDSH-ISMS-B-014)之規定辦理。

三、 資通安全維護計畫之持續精進及績效管理

本校之資通安全委員會應於三、十月(每年至少二次)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。管理審查會議召開時機、審查議題、決議事項及審查紀錄參考本校「資訊安全組織程序書」(文件編號：LDSH-ISMS-B-001)之規定辦理。

壹拾陸、資通安全維護計畫實施情形之提出

本校依據本法第11(16,17)條之規定，每年應向上級或監督機關提出資

通安全維護計畫實施情形[7]，使其得瞭解本機關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

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. 無線網路安全參考指引
10. 網路架構規劃參考指引
11. 行政裝置資安防護參考指引
12. 政府行動化安全防護規劃報告
13. 安全軟體發展流程指引
14. 安全軟體設計指引
15. 安全軟體測試指引
16. 資訊作業委外安全參考指引
17. 本校資通安全事件通報及應變程序
18. 本校「資訊安全管理系統」(ISMS)相關文件

承辦人:　　資通安全官:　　資通安全長(校長)

[7]資通安全維護計畫實施情形之內容，包含上開定期評估、稽核機制、缺失之消除或改正及機關辦理資通安全計畫之相關實施事項，參附件：資通安全維護計畫實施情形。