基隆市立信義國民中學

資通安全維護計畫

版次：V2.2

修訂人核章	
單位主管核章	
資安長核章	

中華民國 114 年 11 月 06 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	修訂內容	修訂單位	修訂人	核定人 （資安長）
V1.0(初版)	107 年 12 月 14 日	新擬訂文件	信義國中	張凱音	莊焙琪
V2.0	112 年 09 月 12 日	柒、二：機關資通安全責任等級分級依據	信義國中	呂協昌	黃明智
V2.1	113 年 10 月 15 日	更新物聯網管理清冊及資通安全自我檢查表	信義國中	呂協昌	黃明智
V2.2	114 年 11 月 06 日	柒、二：機關資通安全責任等級分級內文修正	信義國中	呂協昌	黃明智

目　　錄

壹、 依據及目的 1

貳、 適用範圍 1

參、 核心業務及重要性 1

一、 核心業務及重要性：1

二、 非核心業務及說明：2

肆、 資通安全政策及目標 3

一、 資通安全政策3

二、 資通安全目標3

三、 資通安全政策及目標之核定程序3

四、 資通安全政策及目標之宣導4

五、 資通安全政策及目標定期檢討程序4

伍、 資通安全推動組織 4

一、 資通安全長4

二、 資通安全推動小組5

陸、 專職人力及經費配置 6

一、 專職人力及資源之配置6

二、 經費之配置7

柒、 資訊及資通系統之盤點 7

一、 資訊及資通系統盤點7

二、 機關資通安全責任等級分級8

捌、 資通安全風險評估 9

一、 資通安全風險評估9

玖、 資通安全防護及控制措施 9

一、 資訊及資通設備之管理9

二、 存取控制與加密機制管理9

三、 作業與通訊安全管理12

四、 業務持續運作演練15

五、 資通安全防護設備15

壹拾、 資通安全事件通報、應變及演練相關機制 15

壹拾壹、 資通安全情資之評估及因應 15

一、 資通安全情資之分類評估16

二、 資通安全情資之因應措施16

壹拾貳、 資通系統或服務委外辦理之管理 17
一、 選任受託者應注意事項 17
二、 監督受託者資通安全維護情形應注意事項 18
壹拾參、 資通安全教育訓練 19
一、 資通安全教育訓練要求 19
二、 資通安全教育訓練辦理方式 19
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 19
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 20
一、 資通安全維護計畫之實施 20
二、 資通安全維護計畫實施情形之稽核機制 20
三、 資通安全維護計畫之持續精進及績效管理 21
壹拾陸、 資通安全維護計畫實施情形之提出 22
壹拾柒、 相關法規、程序及表單 22
一、 相關法規及參考文件 22
二、 附件表單 23

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。

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、基隆市政府資通安全政策。

貳、適用範圍

本計畫適用範圍涵蓋本全機關。

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
課程編排、學籍管理、成績評量	校務行政系統	□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ■為本機關依組織法執掌，足認為重要者	財務損失：輕微影響，需要進行系統復原 民眾生命財產損失：無 經濟發展受阻：無 影響其他機關業務運作(相依性)：無 違反法遵義務：違反檔案管理法，將有刑民事責任 機關信譽：將影響本校信譽及形象 其他：無 IP：210.240.24.1(DNS) 系統管理單位：教網中心 系統管理人員：張凱音 系統維護廠商：全誼資訊	4 工作小時

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(對外服務以小時，對內服務以工作小時計)。

5. IP：系統使用者連線 IP

6. 系統管理單位：實際管理單位(處/室)

7. 系統管理人員：實際管理單位負責人

8. 系統維護廠商：負責維護廠商

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	業務失效影響說明	最大可容忍中斷時間
圖書管理系統	圖書館(室)之書籍查詢、借閱、歸還等無法透過資訊系統進行管理，影響行政效率。 IP：210.240.24.1(DNS) 系統管理單位：教務處 系統管理人員：呂協昌 系統維護廠商：全誼資訊系統	4工作小時

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(對外服務以小時，對內服務以工作小時計)。

5. IP：系統使用者連線 IP

6. 系統管理單位：實際管理單位(處/室)

7. 系統管理人員：實際管理單位負責人

8. 系統維護廠商：負責維護廠商

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：

1. 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。

2. 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。

3. 應強固資通系統之韌性，確保機關業務持續營運。

4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本機關同仁之資通安全意識，本機關同仁亦應確實參與訓練。

5. 針對辦理資通安全業務有功人員應進行獎勵。

6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

7. 禁止多人共用單一資通系統帳號。

8. 落實資通安全通報機制。

二、 資通安全目標

1. 提報教育機構資安通報平台之資通安全 3、4 級事件不得發生，1、2 級事件發生應為 3 件以下(含)。

2. 系統所提供資訊無缺漏，每年系統所提供資訊，缺漏事件不得發生 2 件以下(含)。

3. 針對非天災、電力中斷、火災引起之資訊安全事故，導致本機關使用網際網路服務停頓，每年小於 2 次(含)以下，每次不得超過可接受服務中斷時間(MTPD)。

4. 鑑別出並符合所須遵循之法令法規，未鑑別出所需遵循法規次數不得發生 2 件以下(含)。

5. 全年不得違反所須遵循之法令法規，違反需遵循法規次數不得發生 2 件以下(含)。

6. 未能依「風險處理計畫」結案之事件每年應小於(含)2 次。

7. 未能依「矯正措施表」結案之事件每年應小於(含)2 次。

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教務處資訊組簽陳資通安全長核定。

四、 資通安全政策及目標之宣導

1. 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。

2. 本機關應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效，宣導之方式可透過教育訓練、會議、網站進行。

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 11 條之規定，本機關訂定校(園)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處室主任成立資通安全推動小組[1]，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，並適時更新之[2]：

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。

(6) 成員由**資通安全業務主管單位**或資通安全長指派之。

[1] 資通安全推動小組成員由機關之資通安全長召集組成，依資通安全長之指示，負責協助或與機關內之相關單位合作推動機關內部之資通安全業務，如機關未成立資通安全推動小組，相關業務則應由資通安全長責承相關資通安全權責人員辦理之。

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

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。

(7) 成員由**資通系統機關窗口**或資通安全長指派之。

3. 績效管理組：

(1) 辦理資通安全內部稽核。

(2) 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。

(3) 成員由**政風人員**或資通安全長指派之。

陸、專職人力及經費配置

一、 專職人力及資源之配置

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兼辦人員 1 人，其分工如下，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[3]。

(1) 負責推動內部資通安全稽核及教育訓練等業務之推動。

(2) 負責資通安全防護設施建置、資通安全事件通報及應變業務之推動。

(3) 負責本機關對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。

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足，得洽請相關學者專家或專業機關（構）提供顧

[3] 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。

問諮詢服務。

3. 本機關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[4]，並視需要實施人員輪調，建立人力備援制度。

4. 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。

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[5]。

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[6]，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

1. 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、服務資產、人員資產、個資資產等。

2. 資訊及資通系統資產項目如下：

資產分類標準表

資產類別	資產項目

[4] 格式可參附件：資通安全保密同意書。

[5] 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。

[6] 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。

資訊資產（未含有個資）	一、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。 二、電子化儲存之文件檔案，例如：系統軟體使用手冊及教育訓練教材等。 三、書面管理文件，例如：排課系統使用手冊。 四、書面紀錄，例如：資訊設備申請表單等。
軟體資產	一、系統軟體，例如：業務資訊系統、公文系統等。 二、資料庫軟體，例如：SQL Server 等。 三、套裝軟體，例如：Windows 7/10、Office 2013/2016 等。
硬體資產	一、電腦設備，例如：伺服器、工作站、個人主機、筆記型電腦及 PDA 等。 二、通訊設備，例如：路由器、網路交換器、數據機、傳真機、印表機及影印機等。 三、儲存媒體，例如：隨身碟、光碟及光碟機等。 四、其他支援設備，例如：監視器、不斷電系統、地震警報系統等。
服務資產	一、一般維運支援性服務，例如：中華電信網路專線、市電系統等。 二、委外服務，例如：曜信公司一般資訊設備維護服務等等。
人員資產	一、內部同仁，例如：全校教職員。 二、外部(常駐型)人員：無。
個資資產	一、紙本個資，例如：通訊錄、報名表等。 二、檔案形式個資，例如：個人電腦中或主機內個人資料檔案等。 三、資料庫個資，例如：資訊系統含有個人資料資料庫等。

3. 本機關每年度應依資訊及資通系統盤點結果[7]，製作「資訊及資通系統資產清冊」[8]。

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. 各單位管理之資訊或資通設備如有異動，應即時通知資通安全推動小組更新資產清冊。

二、 機關資通安全責任等級分級

依據數位發展部 114 年 10 月 28 日數授資法字第 1145000313J 號函核定，本機關自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為 D 級。

[7] 為使公務機關能依其所屬之資通安全責任等級之分級，執行相關之資通安全防護措施，公務機關應先進行機關內部之資訊及資通系統資產之盤點，使其能依據其所擁有之資訊或資通系統依據資通安全責任等級分級辦法進行風險評估。

[8] 參資訊系統風險評鑑參考指引附件詳細風險評鑑空白表單之資訊資產表。

捌、資通安全風險評估

一、 資通安全風險評估

1. 本機關應每年針對資訊及資通設備資產進行風險評估。

2. 執行風險評估時應**參考基隆市政府風險評估程序書**執行相關作業。

3. 本機關應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估。

玖、資通安全防護及控制措施

本機關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，採行相關之防護及控制措施，全機關之防護及控制措施詳如本機關資通安全維護計畫。

本機關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，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

(一)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須遵守系統管理機關相關規範。

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。

二、 存取控制與加密機制管理

(一)網路安全控管

1. 本機關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) 非軍事區(DMZ)：放置機關對外服務伺服器之區段。

(3) 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、非軍事區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。

5. 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。

6. 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。

7. 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。

8. 網域名稱系統(DNS)防護

(1) 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

(2) DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

(3) DNS 伺服器應設定**指向本市教育網路中心 DNS**。

(4) 內部主機位置查詢應指向機關內部 DNS 伺服器。

9. 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. 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. 資通設備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. 資通設備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. 資通設備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. 資通設備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) 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。

4. 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。

5. 原則不得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。

6. 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

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. 本機關應定期舉辦(或配合上級機關舉辦)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. 電腦機房之門禁管理

(1) 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電腦機房[9]，電腦機房管理者並應定期檢視授權人員之名單。

(3) 人員進入管制區應配載身分識別之標示，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電腦機房。

(5) 人員及設備進出電腦機房應留存記錄。

2. 電腦機房之環境控制

(1) 電腦機房之空調、電力應建立備援措施。

(2) 電腦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、入侵者偵測系統，以減少環境不安全引發之危險。

(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。

[9] 未具進出管制區權限之人員來訪時，應填具進出登記表，格式可參附件：管制區域人員進出登記表。

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.本機關應每季確認重要資料備份之有效性。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設備。

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、 業務持續運作演練

本機關應針對網際網路服務制定業務持續運作計畫，並每二年辦理一次持續運作演練。

五、 資通安全防護設備

1. 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。

2. 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**[10]。

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

[10] 各機關應另訂定資通安全事件通報及應變程序。

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

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[11]。

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。

3. 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。

4. 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

[11] 委外單位之管理措施是否完善，可視其人員資格是否具有相關證照、訓練或認證（如 ISO 27001、CISSP、SSCP、各資安教育訓練單位所辦之課程等）做為參考。

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。

5. 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

1. 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。

2. 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。

（1）資訊資料遭洩漏。
（2）資訊系統遭竄改。
（3）系統之運作受影響或停頓。

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. 受託者應採取之其他資通安全相關維護措施[12]。

5. 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，以稽核或其他適當方式確認受託業務之執行情形[13]。

[12] 公務機關與委外廠商簽訂契約時，應審查契約中保密條款，並要求委外廠商之業務執行人員簽署委外廠商執行人員保密切結書、保密同意書，格式可參附件：委外廠商執行人員保密切結書、保密同意書。

[13] 稽核項目可參委外廠商查核項目表。

壹拾參、資通安全教育訓練

一、 資通安全教育訓練要求

1. 資安兼任人員每人每年至少接受 6 小時以上之資安專業課程訓練或資安職能訓練。

2. 資訊人員每人每年至少接受 6 小時以上之資安專業課程訓練。

3. 本機關之一般使用者與主管，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. 承辦單位應於每學年年初，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[14]，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[15]。

2. 本機關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，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

4. 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、基隆市政府及所屬各機關學校公務人員平時獎懲標準表，及**基隆市國民小學組織規程/基隆市國民中學組織規程/基隆市立高級中學組織規程準則**規定辦理之。

[14] 格式可參附件：年度資通安全教育訓練計畫。

[15] 公務機關辦理教育訓練時，參加人員應簽名留存紀錄，格式可參附件：資通安全認知宣導及教育訓練簽到表。

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

(一)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)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。

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[16]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[17]、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、稽核項目紀錄表[18]及稽核流程等相關資訊提供受稽單位。

4. 本機關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，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告[19]中，並提供給受稽單位填寫辦理情形。

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. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（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）。

[16] 格式可參附件：資通安全稽核計畫。
[17] 格式可參附件：稽核委員聘任同意暨保密切結書。
[18] 格式可參附件：稽核項目紀錄表
[19] 格式可參附件：稽核結果及改善報告。

(二)稽核改善報告

1. 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研議改善措施、改善進度規劃，並落實執行。

2. 受稽單位於稽核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

1. 本機關之資通安全推動小組應於**每年 10 月底前**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) 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。

3.持續改善機制之管理審查應做成改善績效追蹤報告[20]，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，應於**每年 11 月中向基隆市教育網路中心**，提出資通安全維護計畫實施情形[21]，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

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. 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

[20] 格式可參附件：改善績效追蹤報告。

[21] 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。

15. 安全軟體測試指引

16. 資訊作業委外安全參考指引

17. 本機關資通安全事件通報及應變程序

二、 附件表單

1. 資通安全推動小組成員及分工表

2. 資通安全保密同意書

3. 資通安全需求申請單

4. 資訊及資通系統資產清冊

5. 風險評估表

6. 風險類型暨風險對策參考表

7. 管制區域人員進出登記表

8. 委外廠商執行人員保密切結書、保密同意書

9. 委外廠商查核項目表

10. 年度資通安全教育訓練計畫

11. 資通安全認知宣導及教育訓練簽到表

12. 資通安全維護計畫實施情形

13. 資通安全稽核計畫

14. 稽核項目紀錄表

15. 稽核結果紀錄表

16. 稽核委員聘任同意保密切結書

17. 稽核結果及改善報告

18. 改善績效追蹤報告