資通安全維護計畫(範本)

目次

壹、依據及目的

本計畫依據下列法規訂定：

資通安全管理法第 13 條（第 20 條第 2 項及第 21 條第 1 項規定）及資通安全管理法施行細則第 9 條。

（其他業務法規名稱）

貳、適用範圍

本計畫適用範圍除本○全機關外，另包含（請依實際情形列出其他機關名稱）機關。

參、核心業務及重要性

撰寫說明：

- 本章重點在揭示組織之核心業務，並說明核心業務失效時對國人日常生活、社會經濟、政府功能之影響。
- 機關核心業務請依據資通安全管理法施行細則第 10 條規定及政府機關組織法列示。
- 資安責任等級為 A 級及 B 級機關如已進行業務營運衝擊分析，亦可援引敘明。
- 另為進行資通安全事件等級判定，機關仍應針對輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等非核心業務進行盤點，並列出最大可容忍中斷時間。
- 為因應「資通安全責任等級分級辦法」修正條文已於 115 年 1 月 7 日施行，其附表十「資通系統防護基準」之營運持續計畫明定須落實資料備份及系統備援，爰於本章節系統盤點表格增列復原時間目標（RTO）及復原點目標（RPO）欄位。

一、核心業務及重要性：

本機關之核心業務、核心資通系統及重要性如下表，並針對全部核心資通系統訂定營運持續計畫，定期辦理業務持續運作演練：

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(MTPD)	復原時間目標(RTO)	復原點目標(RPO)
		□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	財務損失： 民眾生命財產損失： 經濟發展受阻： 影響其他機關業務運作(相依性)： 違反法遵義			

		組織法執掌，足認為重要者	務： 機關信譽： 其他：			
全國公務人員人事管理（範例）	全國公務人員人事管理系統	□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	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		

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條之規定列示。

2. 核心資通系統：請列出支持核心業務運作必要之系統（無可免）。

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：

本機關之非核心業務及說明如下表：

非核心業務	資通系統	業務失效影響說明	最大可容忍中斷時間(MTPD)	復原時間目標(RTO)	復原點目標(RPO)
公文交換（範例）		電子公文無法即時送達機關，影響機關行政效率	○小時		
其他-非屬上開業務範疇及核心業務者（範例）		影響機關行政效率	○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. 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

撰寫說明：

- 本章包含政策內容、目標、核定程序、宣導程序、定期檢討程序等節，機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件，內容可著重一般同仁應遵守之原則性規定。
- 資通安全目標請由各機關依實際需求自行訂定，目標宜包含量化及質化指標；以下內容僅為範例，請依實際情形參考填列。

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） 應強固核心資通系統之韌性，確保機關業務持續營運。

（四） 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。

（五） 針對辦理資通安全業務有功人員應進行獎勵。

（六） 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

（七） 禁止多人共用單一資通系統帳號。

二、資通安全目標

（一）量化型目標

1. 核心資通系統可用性達99.99%以上。（中斷時數/總運作時數≤ 0.1%）
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. 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5%及2%。

（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○○單位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、電子郵件、個人電腦螢幕保護程式等方式，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 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。

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每年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

撰寫說明：

- 本章至少包含資通安全長、資通安全推動小組之組成及分工職掌等內容。機關規模較大者，亦可於資通安全長下設置資通安全指導小組及資通安全推動小組，分別負責資通安全規劃及推動作業。機關針對資通安全推動組織如已有規定及程序者，可直接引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。
- 分工及職掌為例示規定，請各機關依實際情形列出分工與職掌。

一、資通安全長

依本法第 12 條（公務機關）、第 23 條規定（特定非公務機關）之規定，本機關訂定○長（副首長或適當人員[1]）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。

[1] 考量資通安全推動時常涉及機關內相關資源調動及分配等事項，故資通安全長由機關首長指派副首長擔任，如機關首長指派適當人員擔任資通安全長時，該人員應具有督導、橫向協調、整體資源調度之權限者兼任為宜，使資通安全相關業務得以順利推展。

（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業務部門主管/副主管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，並適時更新之[2]：

1. 執行秘書：

負責襄助資通安全長與督導資通安全相關工作事宜，包含召集會議、決議事項追蹤管理、交辦之其他管理事項等。

2. 資通安全處理小組：

A. 風險管理及法律遵循：負責資訊資產盤點風險管理作業，包含資訊資產清冊之維護、弱點與威脅調查、風險評估、風險處理計畫之擬定與進度追蹤等。並負責規劃及辦理資通安全管理適法性之識別、相關爭訟（議）案件之協

[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。

調處理，並配合司法單位調查之進行，提供必要資源等。

B. 推動及執行：負責建置資通安全管理措施、執行安全監控、程序文件修訂及管制、規劃教育訓練計畫及相關宣導事項之辦理、建立資通安全維護計畫等相關規範，推動資通安全業務，彙整實施成果等。

3. 危機應變小組：負責執行資通安全危機應變、管理系統範圍之營運持續管理作業，包含營運衝擊分析、營運持續計畫、事件通報應變程序及相關演練活動等。

4. 稽核小組：負責規劃與執行資通安全稽核作業，包含稽核計畫之撰寫檢查表之擬定、稽核人員之遴選、稽核發現之改善追蹤等。

陸、專職人力及經費配置

撰寫說明：

- 本章至少包含資安人員配置、訓練及證照，以及資通安全經費或資源之規劃及配置等內容，機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

一、專職人力及資源之配置

（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○級，最低應設置資通安全專職人員○人，並應將資通安全人員名單及其職掌列冊及適時更新[3]。

（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，挹注資源以提升其資通安全管理或防護技術能力。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）提供顧問諮詢服務。

（三） 資安專職人員專業職能之培養(如職能訓練證書、證照、專業課程訓練等)，應依據資通安全責任等級分級辦法之規定辦理[4]。

[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。

[4] 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職人員、認知與訓練之要求，

（四） 資安專職人員應各自持有○張以上資通安全專業證照[5]。

（五） 資安專職人員應各自持有○張以上資通安全職能訓練證書[6]。

（六） 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，若涉及機密維護業務，應簽署書面約定，並視需要實施人員輪調，建立人力備援制度。

（七） 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。

（八） 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[7]。

（二） 各單位於規劃通系統建置時，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編列適當經費，分配資通安全預算所佔之比例，以通過各項資安防護檢查及控制措施。

（三） 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[8]，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、資通系統及資訊之盤點

撰寫說明：

■ 本章至少包含資通系統及資訊之分類及盤點之程序，並應包含標示核心資通系統及相關資

配置適當之資源於資安人員專業職能之培養。

5 視各機關之資通安全責任等級之分級要求。

6 視各機關之資通安全責任等級之分級要求。

7 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。

8 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。

產之要求。機關如已有規定及程序者，可直接引述內部文件編號及名稱。

■ 機關得參酌本範本修改為機關適用之文件。

一、資通系統及資訊之盤點

本機關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（分類僅供參考，機關可依實際情形調整）。

（一） 資通系統及資訊資產項目如下：

1. 人員類：內部人員、外部人員（含委外人員）等。
2. 資訊類：作業文件（含系統文件）、合約、電子資料紀錄（含系統紀錄）、稽核紀錄及歸檔之資訊等。
3. 軟體類：作業系統、系統軟體、應用系統、套裝軟體、資安軟體等。
4. 硬體類：個人電腦（含筆記型、平板電腦）、伺服器、其他硬體、網路設備、可攜式儲存媒體（有資料）、可攜式儲存媒體（無資料）、電腦保護設施、物聯網裝置等。
5. 建築與保護類：辦公區域、資訊機房、檔案室區域、倉庫/庫房、建築保護設施等。
6. 服務類：內外部服務、委外服務、雲端服務等。
7. 支援服務類：相關基礎設施及其他機關內部之支援服務，如電力、消防等。

（二） 本機關每年度應依資訊及資通系統盤點結果[9]，製作「資通系統及資訊資產清冊」[10]，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、資產說明、機密性、完整性、可用性、可律遵循性、資產價值等級。

（三） 本機關依前揭盤點結果，倘發現機關有下載、安裝或使用危

[9] 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。

[10] 參資通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。

害國家資通安全產品（含大陸、香港或澳門廠牌資通訊產品）時，應確認下列事項：

1. 自114年12月1日資通安全管理法修正施行後，凡下載、安裝或使用之產品，應依規定向主管機關申請專案核准使用；未經主管機關核定之產品，應即刻移除、解除安裝或停止使用。倘因使用未經核定之產品，致有影響機關資通安全之虞，本機關得依資通安全管理法第28條規定，對相關人員予以懲戒或懲處。
2. 機關現存之危害國家資通安全產品（含軟體、硬體及服務），應依「危害國家資通安全產品審查辦法」第7條規定，採取相關必要之管控措施[11]。

（四） 伺服器、網路設備、桌上型電腦、筆記型電腦等之硬體類資產，應將可供識別之資產清冊資訊以適當方式或財產標籤標示於硬體外觀（如：財產編號、財產名稱、財產別名、購買日期、年限、保管單位等），以供區別。核心資通系統及相關資產，並應加註標示。

（五） 為確保使用物聯網（IoT）裝置安全，避免不當使用，遭受蓄意資料竊取、遺失或惡意程式入侵等資通安全事件發生，每年度應盤點 IoT 裝置，並針對網路印表機、門禁設備、網路攝影機、無線網路基地台/無線路由器、環控系統、網路儲存伺服器（NAS）等進行資安檢核。

（六） 各單位管理之資通系統或資訊資產如有異動，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

依資通安全責任等級分級辦法第○條第○款至第○款規定，本機關為資通安全責任等級A級機關。（請機關依資通安全責任

[11] 本機關應依資通安全管理法第27條規定，針對所管特定非公務機關，訂定限制或禁止其下載、安裝及使用危害國家資通安全產品之相關管控措施，並報主管機關備查；另應督導該等機關確實依前開管控措施辦理。

等級分級辦法規定自行修改內容）

捌、資通安全風險管理

撰寫說明：

- 本章至少包含風險評估、風險因應等節，機關如已有規定及程序者，可直接引述內部文件編號及名稱。
- 本章參考國家資通安全研究院頒布之「資通系統風險評鑑參考指引」。
- 機關得參酌本範本修改為機關適用之文件。

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。

（二） 執行風險評估時應參考國家資通安全研究院頒布之最新「資通系統風險評鑑參考指引」，並依其中之「詳細風險評鑑」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。

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
○○○網站（範例）	1. 網站前台主機計3台 2. 網站後台主機計1台 3. 負載平衡伺服器 4. 網路交換器（型號） （提供該網站網路服務之網路設備均需列出）	○小時	提供民眾申辦○○○服務

玖、資通安全防護及控制措施

撰寫說明：

- 本章為機關因應資通安全風險，採取之安全防護及控制措施。
- 機關得參酌本範本修改為機關適用之文件。
- 機關如已有對應之規定及程序者，可直接引述內部文件編號及名稱；針對未導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準之機關，可參考包含但不限於 CNS 27002 或

ISO 27002控制措施及國家通安全研究院發布技術指引等文件，並依實際需求增修原則性準則（Standards），並就各項準則訂定相應之程序（Procedures）文件，以完善資通安全管理作業。

■ 本章節所列各面向請依資通安全責任等級辦理，例如：資安A級機關每年應辦理2次內部稽核。

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，由於本機關核心資通系統已通過（導入）CNS 27001驗證（ISO 27001 / 其他具有同等或以上效果之資訊安全管理系統標準），全機關之防護及控制措施詳如○○○文件，本機關之防護及控制措施如下：

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及核心資通系統之防護基準，採行相關之防護及控制措施如下:

一、管理面

（一） 實施資通系統分級及防護基準。

（二） 維護資訊安全管理系統並持續通過公正第三方之驗證。

（三） 每年辦理○次內部稽核，並改善稽核發現事項。

（四） 每年辦理資安治理成熟度評估作業。

（五） 辦理全部核心資通系統業務持續運作演練。

（六） 配置資通安全專職人員。

二、技術面

（一） 定期進行全部核心資通系統安全性檢測（包含弱點掃描、滲透測試及紅隊演練）。

（二） 定期辦理資通安全健診作業。

（三） 完成建置並維護資通安全監控管理機制。

（四） 實施政府組態基準。

（五） 導入並維護資通安全弱點管理機制[12]。

[12] 1.針對資通系統及相關資訊資產（含網通設備），經外部單位資安警訊、辦理安全性檢測及資通安全弱點比對作業等所發現弱點，落實弱點管理作為，明確規範處理時限與相關執行程序，適時修補或採行風險緩解措施。2.本機關應持續追蹤資安警訊、資通安全弱點比對作業及安全性檢測等各項弱點改善處理情形，透過內部稽核、管理審查或其他適當機制，進行檢討與改善，

（六） 導入並維護端點偵測及應變機制。

（七） 完成啟用並維護資通安全防護措施（包括防毒軟體、網路防火牆、電子郵件過濾機制、入侵偵測及防禦機制、應用程式防火牆、進階持續性威脅攻擊防禦措施）。

（八） 電子資料安全管理措施[13]。

三、認知與訓練

（一） 實施資通安全教育訓練。

（二） 維持資通安全專業證照及資安職能訓練證書之有效性。

四、存取控制與加密機制管理

依本機關○○○程序書辦理，以確保資通作業其所運用之系統與資料的存取權限及存取密碼，經適當的授權及控管，以防止不當存取。

五、作業與通訊安全管理

依本機關○○○程序書辦理，確保資通設備及資通系統之變更、備份及監控管理等作業安全，並有效管理網路服務與設備安全，包括核心網路設備之變更、備份、資訊交換及監控管理，建立適當通訊安全控制措施，以維護內部與任何外部單位間傳輸資訊之安全。

六、資通系統獲取、開發及維護

依本機關○○○程序書辦理，以確保有效管理資通系統之獲取、開發及維護過程中應注意之安全要求與資料保護，並維持系統安全與正常運作作業安全管理相關作業。

七、實體與環境安全管理程序

依本機關○○○程序書辦理，以確保機房、操作室、外部租

確保資安防護之有效性與持續性。

[13] 建立電子資料資產清冊，盤點各類電子資料並依CIAL評定防護需求等級，參考相關指引訂定防護基準；另得依實際需求導入檔案與資料庫加密、資料洩漏預防（DLP）、資料遮蔽及雲端資料保護等技術，強化機敏資料之儲存、傳輸與存取安全。

借之 IDC 機房及辦公區域之實體環境安全，並保護相關資產之安全。

八、人員安全管理

依本機關○○○程序書辦理，以確保人員於進用、任職及職務終止等各階段均了解其資通安全責任，並進行相關教育訓練以降低因人為因素所造成的安全風險。

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[14]。

壹拾壹、資通安全情資之評估及因應機制

撰寫說明：

- 本章為機關接受情資後應採取之評估及因應措施，其內容包括情資分類及情資因應。機關如已有對應之規定及程序者，可直接引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

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並留下文件化紀錄，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

[14] 各機關應另訂定資通安全事件通報及應變程序。

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、國民身分證、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措施

撰寫說明：

- 本章為機關辦理資通系統或服務委外時應注意之事項，其內容包括委外前之選任及委外後之監督。資通安全管理法第 10 條第 2 項及資通安全管理法施行細則第 7 條中除已規範應注意事項外，機關亦可參考「資訊服務採購作業指引」、「政府資訊作業委外資安參考指引」、「資訊服務採購契約範本」及「資訊雲端服務採購契約範本」調整相關內容，並於資訊委外各階段，訂定具體安全需求。
- 機關如已有對應之規定及程序者，可直接引述內部文件編號及名稱。

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，應選任適當之受託者，要求受託者建立有效之資通安全管理機制，並監督該機制之實施。

一、選任受託者應注意事項

（一） 資通安全管理措施：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公正第三方驗證[15]。

（二） 資安人力配置：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相關實務經驗之資通安全專業人員。

（三） 複委託管理：明訂受託業務得否複委託、其範圍與對象，及複委託對象應具備之資通安全維護措施。

（四） 國家機密保護：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

[15] 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。

制其出境。

二、監督受託者資通安全維護情形應注意事項

（一） 安全性檢測要求：受託業務涉及客製化資通系統開發者，受託者應提供系統安全性檢測證明；涉及核心資通系統或委託金額達新臺幣一千萬元以上者，本機關應自行或另行委託第三方進行安全性檢測。涉及利用非自行開發之系統或資源者，受託者應標示其內容來源並提供授權證明

（二） 通報與應處機制：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，應立即通知本機關並採行應處措施。

（三） 資料處理與移轉：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） 稽核與監督：本機關應定期或於知悉受託者發生可能影響業務之資安事件時，以稽核或其他適當方式確認受託業務執行情形。[16]

（五） 其他資安維護措施：受託者應採取之其他資通安全相關維護措施[17]。

壹拾參、資通安全教育訓練

撰寫說明：

- 本章為機關辦理資通安全教育訓練事宜，內容包含教育訓練之要求及辦理方式。機關如已有對應之規定及程序者，可直接引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

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◯級，資通安全專職人員每人每年應接受◯小時以上之資通安全專業課程訓練或資通安全職能訓練。

（二） 本機關之資通安全專職人員以外之資訊人員每人每年應接受◯小時以上之資通安全專業課程訓練或資通安全職能訓練，

16 受託業務稽核可參考「數位發展部辦理政府機關受託者資通安全聯合稽核計畫」辦理。

17 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。

且每年接受○小時以上之資通安全通識教育訓練。

（三） 本機關之一般使用者與主管，每人每年應接受○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

（一） 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教育訓練紀錄[18]。

（二） 本機關資通安全教育訓練之內容得包含：（請視實際情形增列）

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，應使其充分瞭解本機關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、所屬人員辦理業務涉及資通安全事項之考核機制

【公務機關】

本機關所屬人員辦理業務涉及資通安全事項，依資通安全管理法第 18 條第 1 項及第 28 條第 1 項規定，績效優良者，應予獎勵；未依該法規定辦理者，應按其情節輕重，依相關規定予以懲戒或懲處。

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

[18] 公務機關辦理教育訓練時，參加人員應簽名留存紀錄。

辦理資通安全事項作業辦法（請填寫機關內部獎懲辦法或自訂獎懲基準之名稱），及本機關各相關規定辦理之。

【特定非公務機關】

本機關所屬人員辦理業務涉及資通安全事項，依資通安全管理法第 26 條及第 28 條第 3 項規定，績效優良者，應予獎勵；未依該法規定辦理，情節重大者，依規定予以懲處。

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

撰寫說明：

- 本章為機關資通安全維護計畫實施情形之績效管理及持續精進機制，其內容包括維護計畫之實施、稽核及管理審查會議。機關如已有對應之規定及程序者，可直接引述內部文件編號及名稱。
- 機關得參酌本範本修改為機關適用之文件。

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（至少依資通安全責任等級分級辦法應辦事項規定頻率辦理）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. 辦理稽核前應擬定資通安全稽核計畫[19]並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、範圍、稽核小組組成方式、保密義務[20]、稽核方式、基準與項目（須將資通安全管理法及子法之法遵納入）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。

[19] 格式可參附件：資通安全署所公佈之資通安全稽核計畫。

[20] 格式可參附件：稽核委員聘任同意暨保密切結書。

3. 辦理稽核時，應於執行稽核前◯日，通知受稽核單位，並將稽核期程、稽核項目紀錄表[21]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[22]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）。

（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，並處理所造成之後果。
2. 受稽單位於稽核實施後發現有缺失或待改善項目者，應判定其發生原因，評估是否有其類似之缺失或待改善之項目存在，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。
3. 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。
4. 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。

[21] 格式可參附件：稽核項目紀錄表

[22] 格式可參附件：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

（一） 本機關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。

（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. 法遵事項實施情形。
3. 與資通安全管理系統有關之內部及外部議題(組織改造、新辦公地點)的變更，如法令變更(如修法)、上級機關要求、資通安全推動小組決議事項等。
4. 資通安全維護計畫內容之適切性。
5. 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. 內部稽核、外部稽核、演練結果。
   E. 近3年追蹤改善情形(不符合項目、矯正措施與定期追蹤機制)。
6. 風險評鑑結果及風險處理計畫執行進度。
7. 重大資通安全事件之處理及改善情形。
8. 利害關係人之回饋。
9. 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[23]，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14（20、21）條之規定，應於○月前向上

[23] 格式可參附件：改善績效追蹤報告。

級或監督機關（中央目的事業主管機關），提出資通安全維護計畫實施情形[24]，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

（一） 資通安全管理法

（二） 資通安全管理法施行細則

（三） 資通安全責任等級分級辦法

（四） 資通安全事件通報應變及演練辦法

（五） 資通安全維護計畫實施情形稽核辦法

（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） 危害國家資通安全產品審查辦法

（九） 國家資通安全會報設置辦法

二、附件表單

（一） 資通安全推動小組成員及分工表

（二） 資通安全需求申請單

（三） 資通安全維護計畫實施情形

（四） 稽核項目紀錄表

（五） 稽核委員聘任同意保密切結書

（六） 稽核結果及改善報告

（七） 改善績效追蹤報告

[24] 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。