伸　港　鄉　公　所

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所全機關及所屬機關(清潔隊、圖書館、鄉立幼兒園、公有零售市場)。

參、 非核心業務及重要性

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
公文交換	電子公文無法即時送達機關，影響機關行政效率	8 小時
路燈管理	無法即時傳送報修訊息	8 小時
郵件服務	影響機關公務推動效率	8 小時
殯葬便民服務網	影響使用者申請效益	8 小時
差勤系統	影響同仁權益	8 小時

肆、 資通安全政策及目標

一、資通安全政策

為使本機關及所屬機關業務順利運作，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. 應強固核心資通系統之韌性，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，以提高本機關及所屬機關同仁之資通安全意識，本機關及所屬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. 使用者需經授權並賦予相關存取權限後，始得使用本機關所提供之各項系統及網路服務，已授權的使用者，僅能在授權範圍內存取系統及網路資源。
9. 落實個人資料保護，合理使用個人資料，避免個人資料外洩。
10. 機密資料檔案的讀取及複製，須符合本機關各業務單位的規定，並經該單位主管或其授權人員核可。
11. 本政策每年應至少評估檢討一次，以反映本機關及所屬機關資訊安全需求、政府法令法規、外在網路環境變化及資訊安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。
12. 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關單位及委外廠商，以利共同遵守。

本政策經資通安全長核准，於公告日施行，並以書面、電子或其他方式通知同仁及與本機關連線作業之有關機關（構）、委外廠商，修正時亦同。

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，未能於 1 小時內完成通報的次數≤0 次。
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 10%及 6%。
4. 全球資訊網內容遭置換未於 10 分鐘內完成靜態網頁置換次數≤0 次。
5. 發生 3 或 4 級資安事件未於知悉後 36 小時內完成損害控制或復原作業的次數≤0 次。
6. 發生 1 或 2 級資安事件未於知悉後 72 小時內完成損害控制或復原作業的次數≤0 次。

(二) 質化型目標

1. 落實資通安全，強化資訊服務品質：由全體同仁貫徹執行資通安全管理，所有資通作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資通安全管理制度的工作，強化服務品質，提升服務水準。
2. 加強資安訓練，符合法令要求規範：督導全體同仁落實資通安全管理工作，每年持續進行適當的資訊安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資訊安全之重要性，促其遵守資通安全規定，藉此提高資通安全認知及緊急應變能力，降低資通安全風險，達持續營運之目標。
3. 規劃持續營運，迅速完成災害復原：訂定重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變

流程的演練，以確保資通系統失效或重大災害事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。

4. 合理利用個資、防範個人資料外洩：對個人資料進行分類，以確定保護的需求和防護措施。建立存取控制機制，在個資傳輸和共享方面採用加密和安全措施，以防止個人資料外洩。
5. 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。
6. 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。
7. 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行政課簽陳資通安全長核定。

四、資通安全政策及目標之宣導

1. 本機關及所屬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。

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監控其執行成效，並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「資通安全管理法」第 11 條之規定，本機關及所屬機關訂定主任

秘書為資通安全長，負責督導機關及所屬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

為推動本機關及所屬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

本機關及所屬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，本機關及所屬機關「資通安全推動小組」分組人員名單及職掌應列冊於「資通安全推動小組名冊」，並適時更新之：

1. 資通安全處理組：
   (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) 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) 資訊及資通系統之盤點及風險評估。
   (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) 其他資通安全事項之規劃、辦理與推動。
2. 資通安全稽核組：
   (1) 辦理資通安全內部稽核，負責訂定及執行內部稽核計畫。
   (2) 執行及追蹤稽核缺失之矯正與預防措施之改善，並追蹤缺失事項之執行情形。
   (3) 評估與檢討資訊安全內部稽核之成效。
   (4) 稽查各種安控機制執行狀況並提出稽核總報告。
   (5) 定期或不定期執行本關之資通安全檢查。
   (6) 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。

(三) 資通安全管理審查會議之頻率及時程

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C級，最低應設置資通安全專職人員1人，本機關現有資通安全專職人員名單及職掌應列冊於「資通安全推動小組名冊」，其分工如下，並適時更新。

(1) 資通安全管理面業務 1 人，負責推動資通系統防護需求分級、資通安全管理系統導入、內部資通安全稽核及教育訓練等業務之推動。

(2) 資通系統安全管理業務 1 人，負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。

(3) 資通安全防護業務1人，負責資通安全監控管理機制、政府組態基準導入，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。

(4) 資通安全管理法法遵事項業務1人，負責本機關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。

2. 本機關及所屬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)提供顧問諮詢服務。

3. 資安專職人員專業職能之培養，應依據資通安全責任等級分級辦法之規定。

(1) 資安專職人員總計應持有1張以上資通安全專業證照。

(2) 資安專職人員總計應持有1張以上資通安全職能評量證書。

4. 本機關及所屬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，應簽署「員工保密切結書」，並視需要實施人員輪調，建立人力備援制度。

5. 本機關及所屬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，應考量本機關及所屬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。
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[1]，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. 本機關及所屬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，分別為人員類、資訊類、硬體類、軟體類、環境保護類等五大類，各分類說明如下：

大分類	小分類	範例
人員類 （People / PE）	編制內人員	正式編制人員、臨時人員、工讀生、專案人員、委外廠商……等。
	臨時人員	

[1]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。

	委外廠商駐點人員	
	委外廠商	
資訊類（Information / IF）	作業文件	資料庫與資料檔案、備份資料、原始程式碼、網路架構圖、系統文件、操作或支援程序、使用手冊、教育訓練教材、管理制度文件、緊急應變&復原計畫、營運持續計劃（BCP）、稽核日誌、契約與協議、報表、表單記錄……等。
	系統文件	
	契約	
	資訊紀錄（電子/紙本）	
	系統紀錄（Log）	
硬體類（Hardware / HW）	個人電腦	一般硬體：包含電腦設備（伺服器、筆記型電腦、個人電腦、工作站）、CD/DVD 燒錄器、CD/DVD 光碟機、磁帶機、軟碟機、投影機、PDA、印表機……等。 通訊設備：集線器、橋接器、網路交換器、路由器、數據機、電話自動交換機（PBX）、網路纜線、防火牆、入侵偵測系統、視訊會議設備、傳真機、手機。 儲存媒體：CD/DVD（空白）、硬碟（無資料）、磁片（空白）、磁帶（空白）、移動式硬碟（空白）、錄音/影帶（無資料）……等。
	可攜式電腦	
	伺服器	
	資安設備	
	網路設備	
	可攜式儲存媒體	
	電腦保護設施	
	其他硬體	
軟體類（Software / SW）	作業系統	應用系統軟體、作業系統軟體、開發工具、套裝軟體、公用程式、防火牆軟體、防毒軟體、驗證軟體、資料庫管理系統（DBMS）、加密軟體、文件管理系統、內部開發程式、內部發展系統……等。
	應用系統	
	套裝軟體	
	軟體開發工具	
	資訊安全系統	
環境保護類（Environment / EV）	一般辦公區域	建築類：電腦機房、會議室、辦公室、監控室、接待區、交貨區/裝載區……等。 環境保護設施：不斷電系統、第二電力供應迴路、穩壓器、機櫃、避雷裝置、警報系統、備用發電系統、環境控制系統（火偵測、熱偵測、水偵測、溫濕度偵測、自動消防滅火系統）……等。
	特殊辦公區域	
	資訊機房	
	倉庫/庫房	
	建築保護設施	

2. 本機關及所屬機關每年度應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。
3. 資訊及資通系統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。核心資通系統及相關資產，並應加註標示。
4. 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訊資產清冊。

二、機關資通安全責任等級分級

本機關自行或委外開發之資通系統，為資通安全責任等級 C 級機關。本機關所屬機關(清潔隊、公有零售市場、圖書館、鄉立幼兒園)，為資通安全責任等級 E 級機關。

捌、 資通安全風險評估

1. 本機關及所屬機關應每年針對資訊及資通系統資產進行風險評估，並將評估結果紀錄於「風險評鑑工作表」。
2. 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「資訊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。
3. 本機關及所屬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。

玖、 資通安全防護及控制措施

本機關及所屬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、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. 本機關及所屬機關同仁使用資訊及資通系統前應經其管理人授權。
2. 本機關及所屬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. 本機關及所屬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。

(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。

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. 不得使用私人之通訊設備連接公務電腦。
9. 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 伺服器應設定指向 GSN Cache DNS。

10. 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. 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。

(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. 本機關及所屬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. 本機關及所屬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長同意

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) 進行遠距工作時之安全監視。
   (4) 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. 本機關及所屬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. 本機關及所屬機關應定期舉辦（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) 電腦機房應安裝視訊監視系統，以查看並記錄組織場所內外敏感區域之進出。

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

(4) 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。

(5) 僅於必要時，得准許外部支援人員進入電腦機房。

(6) 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) 電腦機房之溫濕度管控範圍為：溫度範圍 ： 20-25 度
濕度範圍 ： 40-60%

(3) 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、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。

(5) 資通系統主機、重要網路設備應訂定容量管理界限，如 RAM、CPU、HDD，應定期執行檢查資通系統主機、重要網路設備之容量，當超出管制界限時，應採取適當之行動。

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. 重要資料及核心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. 本機關及所屬機關應每年確認非核心資通系統資料備份之有效性。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系統。
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. 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。
3. 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. 個人電腦應設密碼保護，長度至少八碼，並應滿足密碼複雜度要求(英文大寫、小寫、數字、特殊符號四選三)，且至少每 90 天變更一次密碼。
2. 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。

3. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體及大陸品牌軟體。
4. 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。
5. 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。
6. 下班時應關閉電腦及螢幕電源。
7. 如發現資安問題，應主動循機關之通報程序通報。
8. 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。
3. 員工一律禁用私人的可攜式設備及可攜式儲存媒體等設施，如公務上須使用則須提出申請經權責主管核准後方可使用。
4. 可攜式設備及可攜式儲存媒體僅限於公務使用，禁止使用於私人用途，使用時應僅防資訊外洩或中毒。
5. 使用者如需使用外來的可攜式資訊設備或可攜式儲存媒體，必須先進行掃毒，確認其不含病毒與惡意程式，掃毒後方可進行資料之上傳及寫入作業，以避免受到惡意程式的威脅。
6. 將機密資料存放於可攜式儲存媒體上時，應採取適當加密處理或設定密碼保護（如 Word、Excel 或壓縮軟體之密碼功能），避免可攜式儲存媒體遺失時造成資訊外洩。
7. 筆記型電腦應安裝防毒軟體，並定期檢查作業系統修正程式與更

新病毒碼為最新版本。

8. 存有重要機密性資訊之可攜式資訊設備或儲存媒體攜出時，設備管理人員應負保護之責不得離身，且針對相關檔案資料須執行加密或先清除其機密資訊，以避免資料洩露，另作業完成後須徹底抹去媒體上相關資料。
9. 可攜式設備及儲存媒體遺失時應立即通報單位主管，並評估資料遺失是否具有機密性，依情節之重大程度決定是否向上呈報。

(九) 即時通訊軟體之安全管理

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。

四、系統獲取、開發及維護

1. 本機關及所屬機關之資通系統應依「資通安全責任等級分級辦法」附表八之規定完成系統防護需求分級，依分級之結果，完成附表九中資通系統防護基準，並注意下列事項：
   (1) 開發過程請依安全系統發展生命週期（Secure Software Development Life Cycle, SSDLC）、防護基準等級納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。
   (2) 於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。
   (3) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

(4) 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

五、執行資通安全健診

本機關及所屬機關每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

(1) 網路架構檢視。

(2) 網路惡意活動檢視。

(3) 使用者端電腦惡意活動檢視。

(4) 伺服器主機惡意活動檢視。

(5) 安全設定檢視。

六、資通安全防護設備

1. 本機關及所屬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. 資安設備應留存日誌至少六個月，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

一、本機關之資安通報窗口為行政課，電話：04-7982010 分機 221。

二、本機關所有人員及委外廠商於發現資安事件時均附有通報之責，並應於一小時之內向資安通報窗口進行通報。

三、各資通系統應備好靜態網頁，遇資安攻擊導致顯示畫面遭置換時，應於 10 分鐘內置換靜態畫面，或立即關機。

四、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，依「資通安全事件通報及應變辦法」、「各機關資通安全事件通報及應變處理作業程序」辦

理。

壹拾壹、 資通安全情資之評估及因應

本機關及所屬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

本機關及所屬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。

二、資通安全情資之因應措施

本機關及所屬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。

壹拾貳、 資通系統或服務委外辦理之管理

本機關及所屬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。
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. 本機關於辦理採購時，務必依「大陸廠牌資通訊產品及委外經營公眾場域盤點原則」查證，不可採購大陸廠牌資通訊產品。
5. 本機關採購案內涉資通訊軟體、硬體或服務等相關事務，機關應要求廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。
6. 各機關自行或委外營運，提供公眾活動或使用之場地(場地外租)，不得使用危害國家資通安全產品，且應將相關限制事項納入委外契約或場地使用規定中。

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，應立即通知委託機關及採行之補救措施。
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。
5. 本機關及所屬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。

壹拾參、 資通安全教育訓練

一、資通安全教育訓練要求

1. 本機關依資通安全責任等級分級屬 C 級，資安及資訊人員每年至少 1 名人員接受 12 小時以上之資安專業課程訓練或資安職能訓練。
2. 資通安全專責人員以外之資訊人員每人每二年至少接受 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。
3. 本機關及所屬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（表）」，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上課紀錄（表）。
2. 本機關及所屬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

本機關及所屬機關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彰化縣政府暨所屬機關公務人員平時獎懲標準表等各相關規定辦理之。

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，使本機關及所屬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」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 15 日，通知受稽核單位，並將稽核期程、「稽核項目紀錄表」及稽核流程等相關資訊提供受稽單位。
4. 本機關及所屬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、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. 本機關及所屬機關之資通安全推動小組應於 11 月前（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) 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) 與資訊安全管理系統有關的利害關係方的需求和期望的變化。

(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. 內外部稽核結果。

E. 不符合項目及矯正措施。

(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。

3. 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

本機關及所屬機關依據「資通安全管理法」第 12 條之規定，每年向上級監督機關，提出資通安全維護計畫實施情形，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. 各機關資通安全事件通報及應變處理作業程序
6. 資通安全情資分享辦法
7. 公務機關所屬人員資通安全事項獎懲辦法
8. 資訊系統風險評鑑參考指引
9. 政府資訊作業委外安全參考指引
10. 無線網路安全參考指引
11. 網路架構規劃參考指引
12. 行政裝置資安防護參考指引
13. 政府行動化安全防護規劃報告
14. 安全軟體發展流程指引
15. 安全軟體設計指引
16. 安全軟體測試指引
17. 資訊作業委外安全參考指引
18. 本機關資通安全事件通報及應變程序
19. 彰化縣政府暨所屬機關公務人員平時獎懲標準表

二、附件表單

1. 安全等級評估表
2. 機關資通系統與服務資產清冊
3. 本機關資通安全目標監測記錄
4. 本機關資通安全推動小組名冊
5. 本機關員工保密切結書
6. 資訊及資通系統資產清冊
7. 風險評鑑工作表
8. 本機關教育訓練計畫表

9. 本機關教育訓練上課紀錄表
10. 稽核項目記錄表
11. 矯正及預防處理單
12. 委外廠商資通安全要求查核表