

高雄市政府新聞局
資通安全管理維護計畫

高雄市政府新聞局資通安全管理維護計畫

目 錄

壹、 依據及目的	4
貳、 適用範圍	4
參、 核心業務及重要性	4
一、 核心業務及重要性：	4
二、 非核心業務及說明：	5
肆、 資通安全政策及目標	5
一、 資通安全政策.....	5
二、 資通安全目標.....	5
三、 資通安全政策及目標之核定程序.....	6
四、 資通安全政策及目標之宣導.....	6
五、 資通安全政策及目標定期檢討程序.....	6
伍、 資通安全推動組織	6
一、 資通安全長.....	6
二、 資通安全推動小組.....	7
陸、 專職(責)人力及經費配置	8
一、 專職(責)人力及資源之配置.....	8
二、 經費之配置.....	9
柒、 資訊及資通系統之盤點	9
一、 資訊及資通系統盤點.....	9
二、 機關資通安全責任等級分級.....	10
捌、 資通安全風險評估	10
一、 資通安全風險評估.....	10
二、 核心資通系統及最大可容忍中斷時間.....	10
玖、 資通安全防護及控制措施	10
一、 資訊及資通系統之管理.....	11
二、 存取控制與加密機制管理.....	12
三、 作業與通訊安全管理.....	14
四、 系統獲取、開發及維護.....	17
五、 業務持續運作演練.....	17
六、 執行資通安全健診.....	18
七、 資通安全防護設備.....	18
壹拾、 資通安全事件通報、應變及演練相關機制	18

高雄市政府新聞局資通安全管理維護計畫

壹拾壹、資通安全情資之評估及因應	19
一、資通安全情資之分類評估.....	19
二、資通安全情資之因應措施.....	20
壹拾貳、資通系統或服務委外辦理之管理	20
一、選任受託者應注意事項.....	21
二、監督受託者資通安全維護情形應注意事項.....	21
壹拾參、資通安全教育訓練	21
一、資通安全教育訓練要求.....	21
二、資通安全教育訓練辦理方式.....	21
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	22
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	22
一、資通安全維護計畫之實施.....	22
二、資通安全維護計畫實施情形之稽核機制.....	22
三、資通安全維護計畫之持續精進及績效管理.....	23
壹拾陸、資通安全維護計畫實施情形之提出	24
壹拾柒、相關法規、程序及表單	24
一、相關法規及參考文件.....	24
二、附件表單.....	25

高雄市政府新聞局資通安全管理維護計畫

壹、依據及目的

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、高雄市政府新聞局組織規程。

貳、適用範圍

本計畫適用範圍涵蓋本局全機關。

參、核心業務及重要性

一、核心業務及重要性：

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
有線電視：有線電視業者管理與輔導、基本頻道收視費用核定、處理有線電視纜線附掛及人民陳情等事項。	無	為本科依組織法執掌，足認為重要者。	可能使本局部份業務中斷，並影響本市有線電視收視戶權益。	無須定義
電影院及錄影帶業：本市電影片映演業者管理及查察業務。	無	為本科依組織法執掌，足認為重要者。	可能使本局部份業務中斷	無須定義
市政行銷、新聞發布、媒體連繫業務： 1、市政行銷、道路交通安全宣導。 2、輿情蒐集。 3、記者會舉辦暨國內外新聞界人士之聯繫與服務事項。 4、市政行程及特定事項新聞發布。	無	為本科依組織法執掌，足認為重要者。	無法即時蒐集緊急危難事件數據，對外發布資訊	無須定義

高雄市政府新聞局資通安全管理維護計畫

二、非核心業務及說明：

本機關之非核心業務及說明如附表 1。

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。

二、資通安全目標

(一) 量化型目標

1. 本局維運之資通系統可用性達 99.97%以上。(非預期中斷時數/總運作時數 $\leq 0.03\%$)
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%。

高雄市政府新聞局資通安全管理維護計畫

(二) 質化型目標：

1. 機密性目標：維護資料在傳輸、儲存、與處理狀態時，不被非授權人員之存取、使用、或竄改。
2. 完整性目標：確保維持資料原來的狀態，只允許有權限的使用者可以修改資料內容。在資料內部與外部均需維持資料的一致性。
3. 可用性目標：確保資訊與系統能夠持續營運、正常使用。
4. 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。
5. 提升人員資安防護意識、有效偵測與預防外部攻擊。

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資訊單位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。

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，本機關首長指派副局長為資通安全長，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。

高雄市政府新聞局資通安全管理維護計畫

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業務部門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¹：

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。

高雄市政府新聞局資通安全管理維護計畫

(5) 其他資通安全事項之規劃。

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。

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。

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C級，最低應設置資通安全專責人員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。
 - (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及驗證、內部資通安全稽核、機關資安治理成熟度評估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

高雄市政府新聞局資通安全管理維護計畫

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(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。
 - (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，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。
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，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、支援服務資產等
2. 資訊及資通系統資產項目如下：

高雄市政府新聞局資通安全管理維護計畫

- (1) 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。
 - (2) 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。
 - (3) 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。
 - (4) 支援服務資產：相關基礎設施級其他機關內部之支援服務，如電力、消防等。
3. 本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。
 4. 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。
 5. 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產清冊。

二、機關資通安全責任等級分級

本機關無資通安全責任等級分級辦法第 5 條所列之情形，所維運之資通系統係委外開發，為資通安全責任等級 C 級機關。

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系統資產進行風險評估。
2. 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。

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. 本機關同仁使用資訊及資通系統前應經其管理人授權。
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。

(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，僅透過市府(■四維行政中心■鳳山行政中心)上網。
2. 本機關內部區域網路應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。
3. 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。
4. 網域名稱系統(DNS)：本機關係使用市府建置 DNS 伺服器，內部個人電腦及主機位置查詢應指向市府內部 DNS 伺服器。
5. 本機關不得私自另行架設有線或無線網路進行公務連線存取。
6. **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) 無線網路應採用現行技術尚無遭破解疑慮之加密方式，進行加密傳輸。

(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) 通行碼如係由系統或相關承辦人員預設，應告知使用者於首次使用系統時變更通行碼，或由系統強制執行。
 - (4) 使用者通行碼更改時，新通行碼不得與前 3 次舊通行碼重複，至少每 90 天應更換 1 次；可設置一定期間的緩衝期，**或要求於到期後第 1 次登入須立即更改密碼**，以防止使用者長時間未登入系統，未及變更通行碼而導致使用者 ID 被鎖定。
 - (5) 如為特定系統因功能限制，通行碼設定與更改作業無法完全符合前項要求，得經核准後，調整該系統之通行碼設定要求或密碼變更頻率。

高雄市政府新聞局資通安全管理維護計畫

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) 使用者責任

1. 使用者之通行碼應妥善保管，避免他人知悉。

2. 應取消資通系統、瀏覽器或或之密碼自動記憶功能，避免密碼遭截取或竊用。

3. 使用者離開主機或個人電腦時，應關閉電腦螢幕或啟動鎖定功能，以確保資料之安全。若超過 15 分鐘未使用主機或個人電腦，須設定螢幕密碼保護或強制登出措施。

(四) 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。

5. 資通系統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。

(五) 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。

(六) 作業系統存取控制

1. 調整主機或個人電腦安全性設定，以滿足使用者存取管理需求。
2. 依各資料夾(目錄)之用途，設定適當使用權限。
3. 應關閉所有網路資源分享服務，如因公務需求須使用網路資源分享服務，須經權責主管同意。
4. 啟用稽核原則(如：登入失敗之稽核)，保留相關稽核紀錄。
5. 伺服器上之作業系統，應啟動本機防火牆，並以最小且必要之原則開放連線存取服務。
6. 登入伺服器上之作業系統，若超過時限無任何動作時，須設定將使用者 ID 鎖定或登出。

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. 本機關放置於資訊中心機房之資通系統，其操作及維護作業以現場處理為原則；如有緊急需求時，應填寫「網路業務處理申請表」，經權責主管同意後，向資訊中心申請遠距工作防火牆連線開通。
 - (1) 外部網路(External Network)對本機關資通系統之遠距工作防火牆連線期限以不超過 15 天為原則。

- (2) 應明確指定來源 IP 位址、目的 IP 位址、目的通訊埠及協定等選項，避免任一選項設定全部(Any)。
- (3) 資料庫不提供外部網路(External Network)遠端連線存取。

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。

(三) 電子郵件安全管理

- 1. 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。
- 2. 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。
- 3. 使用者不得利用機關所提供之電子郵件服務從事侵害他人權益或違法之行為。
- 4. 使用者應確保電子郵件傳送時之傳遞正確性。
- 5. 使用者使用電子郵件時，應注意電子簽章之要求事項。
- 6. 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. 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. 本機關應每年確認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. 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 15 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。

高雄市政府新聞局資通安全管理維護計畫

(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

(九) 即時通訊軟體之安全管理

1. 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。

2. 使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：

(1) 用戶端應有身分識別及認證機制。

(2) 訊息於傳輸過程應有安全加密機制。

四、系統獲取、開發及維護

1. 本機關之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十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)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、業務持續運作演練

本機關應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

六、執行安全性檢測

本機關應針對核心資通系統每二年辦理一次網站弱點檢測及

高雄市政府新聞局資通安全管理維護計畫

系統滲透測試。

七、執行資通安全健診

1. 本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。

八、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

1. 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及應變管理程序。
2. 通報訂定作業規範，其內容應包括下列事項：
 - (1) 判定事件等級之流程及權責。
 - (2) 事件之影響範圍、損害程度及機關因應能力之評估。
 - (3) 資通安全事件之內部通報流程。
 - (4) 通知受資通安全事件影響之其他機關之時機及方式。
 - (5) 前四款事項之演練。
 - (6) 資通安全事件通報窗口及聯繫方式。
 - (7) 其他資通安全事件通報相關事項
3. 應變作業規範，其內容應包括下列事項：

高雄市政府新聞局資通安全管理維護計畫

- (1) 應變小組之組織。
- (2) 事件發生前之演練作業。
- (3) 事件發生時之損害控制，及向中央目的事業主管機關請求技術支援或其他必要協助之機制。
- (4) 事件發生後之復原、鑑識、調查及改善機制。
- (5) 事件相關紀錄之保全。
- (6) 其他資通安全事件應變相關事項。

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

高雄市政府新聞局資通安全管理維護計畫

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。

高雄市政府新聞局資通安全管理維護計畫

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。

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. 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，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。

高雄市政府新聞局資通安全管理維護計畫

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、高雄市政府及所屬各機關公務人員平時獎懲標準表，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

(一) 稽核機制之實施

1. 資通安全推動小組應定期(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。

高雄市政府新聞局資通安全管理維護計畫

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. 本機關之資通安全推動小組應於 12 月(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。

高雄市政府新聞局資通安全管理維護計畫

- (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，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

本機關依據資通安全管理法第 12 條之規定，須應上級或監督機關要求，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. 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

高雄市政府新聞局資通安全管理維護計畫

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. 本機關資通安全事件通報及應變程序

二、附件表單

1. 本局非核心業務及說明如附表 1
2. 資通安全推動小組成員及分工表
3. 資通安全保密同意書
4. 資通安全需求申請單
5. 資訊及資通系統資產清冊
6. 風險評估表
7. 風險類型暨風險對策參考表
8. 管制區域人員進出登記表
9. 委外廠商執行人員保密切結書、保密同意書
10. 委外廠商查核項目表
11. 年度資通安全教育訓練計畫
12. 資通安全認知宣導及教育訓練簽到表
13. 資通安全維護計畫實施情形
14. 資通安全稽核計畫

高雄市政府新聞局資通安全管理維護計畫

15. 稽核項目紀錄表
16. 稽核結果紀錄表
17. 稽核委員聘任同意保密切結書
18. 稽核結果及改善報告
19. 改善績效追蹤報告

高雄市政府新聞局資通安全管理維護計畫

附表 1：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
高雄市政府新聞局官網	網頁資訊無法瀏覽，影響機關行政效率	24 小時
好理災災害數據網路平台	網頁資訊無法瀏覽，影響機關行政效率	24 小時
公文交換系統	電子公文無法即時送達機關，影響機關行政效率	由系統權管單位訂之。
市府郵件服務系統	電子郵件無法傳遞，影響機關行政效率，影響機關行政效率	由系統權管單位訂之。
WebITR 差勤服務系統	無法即時查詢辦理差勤登記，影響機關行政效率	由系統權管單位訂之。
議員質詢及建決議案系統	無法即時辦理議員質詢及建決議案系統，影響機關行政效率	由系統權管單位訂之。
知識庫管理系統	無法即時辦理市政會議等知識庫相關業務，	由系統權管單位訂之。
線上即時服務系統	無法即時辦理民眾線上陳情案件，影響機關行政效率	由系統權管單位訂之。
WebITR 差勤服務系統	無法即時查詢辦理差勤登記，影響機關行政效率	由系統權管單位訂之。
機關查詢社交工程演練統計系統	無法辦理社交工程演練相關業務，影響機關行政效率	由系統權管單位訂之。
資料開放平台	無法辦理開放資料相關業務，影響機關行政效率	由系統權管單位訂之。
弱掃平台系統	無法辦理網頁弱點掃描，影響機關行政效率	由系統權管單位訂

高雄市政府新聞局資通安全管理維護計畫

		之。
行政院主計總處 預算編製資訊系統(直轄市版)	影響支付款項予廠商或同仁及預算決算編送	由系統權管單位訂之。
高雄銀行電子支付系統	影響支付款項予廠商或同仁及庫款支付之核對作業	由系統權管單位訂之。
高雄銀行公庫服務網	影響每月對帳單核對列印	由系統權管單位訂之。
CGSS 民間團體補(捐)助系統	影響補助民間團體款項之申請與結報	由系統權管單位訂之。
災準金支用情形填報系統	影響災準金動支數、發包數及實支數等之填報	由系統權管單位訂之。
社會經濟資料庫決策應用系統	影響統計報表(月報、季報、半年報、年報)之上傳及審核	由系統權管單位訂之。
主計處線上管理系統	影響主計處所需表報之填列(如每月歲入歲出執行狀況表等)	由系統權管單位訂之。
政府電子採購網	無法辦理採購案招標、決標、下訂及查詢等作業，影響機關行政效率。	由系統權管單位訂之。
資訊設備預算先期審議系統	無法申請、查詢各年度資訊設備市府核定結果，影響機關行政效率。	由系統權管單位訂之。
帳號管理系統	無法查詢員工帳號及管理機關帳號，影響機關行政效率。	由系統權管單位訂之。
市府第二代職工人事系統(KPSN2)	無法辦理職工各項人事作業，影響機關行政效率。	由系統權管單位訂之。
行政院人事行政總處人事服務網(ECPA)	無法定期填報職工、臨時人員、勞務承攬派駐人數及退休職工三節慰問金等，影響機關行政效率。	由系統權管單位訂之。

高雄市政府新聞局資通安全管理維護計畫

優先採購網路資訊平台	無法查詢及填報採購身障團體、庇護工場服務與產品之成果，影響機關行政效率。	由系統權管單位訂之。
綠色生活資訊網	無法查詢環保產品、填報綠色採購之成果，影響機關行政效率。	由系統權管單位訂之。
國民旅遊卡檢核系統	無法辦理職工國民旅遊卡檢核作業，影響機關行政效率。	由系統權管單位訂之。
薪資系統	無法即時作業，影響薪資作業	由系統權管單位訂之。
高雄銀行整批轉帳網路作業	無法即時作業，影響薪資、退休金等相關轉帳作業	由系統權管單位訂之。
郵局薪資轉存系統	無法即時作業，影響退休金作業	由系統權管單位訂之。
郵局業務資料傳輸系統	無法即時作業，影響退休金轉帳作業	由系統權管單位訂之。
高雄銀行公庫服務網	無法即時作業，影響機關行政效率	由系統權管單位訂之。
高雄銀行支付系統	無法即時作業，影響支付作業	由系統權管單位訂之。
高雄市政府收據規費暨行政罰鍰管理系統	無法即時作業，影響機關行政效率	由系統權管單位訂之。
各類所得憑單資料電子申報系統	無法即時作業，影響各類所得申報作業	由系統權管單位訂之。
稅務入口網自繳繳款書	無法即時作業，影響稅款繳款作業	由系統權管單位訂

高雄市政府新聞局資通安全管理維護計畫

		之。
多憑證網路承保作業	無法即時作業，影響健保加退保等相關作業	由系統權管單位訂之。
勞保局e化服務系統	無法即時作業，影響勞保、勞退金加退保等相關作業	由系統權管單位訂之。
市有財產管理資訊系統	無法及時登錄財產之增減及轉移，製作各式表單，影響機關行政效率。	由系統權管單位訂之。
市政新聞管理系統	無法即時發布新聞資訊	由系統權管單位訂之。
高雄市財政局規費暨行政罰鍰管理系統	影響機關行政效率	由系統權管單位訂之。
其他-非屬上開業務範疇及核心業務者	影響機關行政效率	由系統權管單位訂之。