

高雄市政府民政局暨所屬機關
資通安全維護計畫

發行日期：111 年 4 月 27 日

變更紀錄

版次	發行日期	修訂者	說明	核准者
1.0	108年2月18日	高雄市政府民政局	初版文件發行	民政局局長
1.1	108年6月27日	高雄市政府民政局	配合行政院核定資通安全責任等級修正	民政局局長
1.2	109年11月5日	高雄市政府民政局	配合本市戶政事務所組織整併及行政院審查意見修正	民政局局長
1.3	110年6月16日	高雄市政府民政局	<ol style="list-style-type: none"> 1. 配合行政院核定三民戶政事務所資通安全責任等級為D級 2. 配合高雄市忠烈祠資訊網、高雄市八二三台海戰役紀念館資訊網集中至市府機關網站共用模板管理系統 	民政局局長
1.4	111年4月27日	高雄市政府民政局	<ol style="list-style-type: none"> 1. 修正適用範圍格式 2. 修正非核心業務及說明內容 3. 修正專職(責)人力資源之配置第五點資安專職人員專業職能之培養內容 4. 修正資通安全維護計畫實施情形之稽核機制第一點內容 5. 刪除相關法規重複內容 6. 更新對應四階文件編號 	民政局局長

目 錄

壹、 依據及目的	3
貳、 適用範圍	3
參、 民政業務及重要性	4
肆、 資通安全政策及目標	6
伍、 資通安全推動組織	7
陸、 專職（責）人力及經費配置	7
柒、 資訊及資通系統之盤點	8
捌、 資通安全風險評估	8
玖、 資通安全防護及控制措施	8
壹拾、 資通安全事件通報、應變及演練相關機制.....	9
壹拾壹、 資通安全情資之評估及因應	10
壹拾貳、 資通系統或服務委外辦理之管理	11
壹拾參、 資通安全教育訓練	12
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..	13
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..	13
壹拾陸、 資通安全維護計畫實施情形之提出	14
壹拾柒、 相關法規、程序及表單	15

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、高雄市政府民政局組織規程。
- 三、高雄市殯葬管理處組織規程。
- 四、高雄市兵役處組織規程。
- 五、高雄市各戶政事務所組織規程。

貳、適用範圍

本計畫適用範圍涵蓋高雄市政府民政局（以下簡稱本局）暨所屬殯葬管理處、兵役處、本市各戶政事務所全體機關（以下統稱本機關），如下表：

責任等級	機關名稱	
C	高雄市政府民政局	
	高雄市殯葬管理處	高雄市兵役處
D	高雄市鼓山戶政事務所	高雄市左營戶政事務所
	高雄市楠梓戶政事務所	高雄市三民戶政事務所
	高雄市新興戶政事務所	高雄市苓雅戶政事務所
	高雄市前鎮戶政事務所	高雄市小港戶政事務所
	高雄市鳳山戶政事務所	高雄市岡山戶政事務所
	高雄市旗山戶政事務所	高雄市美濃戶政事務所
	高雄市大寮戶政事務所	高雄市仁武戶政事務所
	高雄市鳥松戶政事務所	高雄市路竹戶政事務所
	高雄市茄萣戶政事務所	高雄市梓官戶政事務所

參、民政業務及重要性

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	權責單位	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
戶政	戶籍行政科	高雄市戶政資訊服務網上 e 指通 APP	戶政業務申辦及預約係本局重要推行業務，且涉及民眾個人資料	1. 影響其他機關業務運作： 無法運作恐無法使用戶政線上申辦及預約服務，以及相關業務運作，影響行政效率 2. 違反法遵義務及機關信譽： 依個人資料保護法應善盡個人資料保護責任，如違反該法恐足造成政治議題，影響機關形象	8 小時

二、非核心業務及說明：

1. 本局之非核心業務及說明如下表：

非核心業務	非核心資通系統	業務失效影響說明	最大可容忍中斷時間
調解	線上調解聲請服務系統	無法運作恐無法使用區公所調解資料登錄，以及相關業務運作，影響行政效率	9 小時
區政	區政資訊系統	無法運作恐無法使用區政資料登錄，以及相關業務運作，影響行政效率	9 小時
	高雄市區政線上 e 指通	無法運作恐導致無法使用區政線上申辦及預約服務，以及相關業務運作，影響行政效率	9 小時

里政	高雄市里政資訊網 (含里政線上 e 指通 APP)	無法運作恐無法使用里政資訊網服務，以及相關業務運作，影響行政效率	9 小時
宗教	高雄祈福 e 指通	無法運作恐導致無法瀏覽及查詢祈福資訊，影響民眾權益	9 小時
資訊	民政局官網	無法運作恐導致無法瀏覽及查詢本局官網資訊，影響民眾權益	9 小時
	局內系統 EIP	無法運作恐影響相關系統案件資料登錄，以及其他機關與本局相關業務運作，影響行政效率	9 小時
行政	區公所及戶政填報資料系統	無法運作恐影響機關內部資訊傳遞，影響行政效率	24 小時
	會計業務線上彙報系統	無法運作恐影響機關內部資訊傳遞，影響行政效率	24 小時
	洗錢資恐風險系統	無法運作恐影響機關內部資訊傳遞，影響行政效率	24 小時

2. 殯葬管理處之非核心業務及說明如下表：

非核心業務	非核心資通系統	業務失效影響說明	最大可容忍中斷時間
殯儀館	大高雄殯葬業務資訊系統	無法運作恐導致無法使用殯葬業務相關功能，影響民眾權益	8 小時
	殯儀館、火化場便民 E 化服務網	無法運作恐導致無法使用殯儀館及火化場便民 e 化服務相關功能，影響民眾權益	9 小時
	電子輓聯平台	無法運作恐導致無法使用電子輓聯相關功能，影響民眾權益	9 小時
墓政	大高雄墓政資訊系統	無法運作恐導致無法使用墓政業務相關功能，影響民眾權益	9 小時
	墓政業務多元入口網	無法運作恐導致無法使用墓政業務相關功能，影響民眾權益	9 小時

	宗祠生命追憶館	無法運作恐導致無法使用宗祠生命追憶館網站，影響民眾權益	9 小時
--	---------	-----------------------------	------

3. 兵役處之非核心業務及說明如下表：

非核心業務	非核心資通系統	業務失效影響說明	最大可容忍中斷時間
軍人忠靈祠	高雄市軍人忠靈祠資訊網	無法運作恐導致無法瀏覽及查詢高雄市軍人忠靈祠資訊網資訊，影響民眾權益	9 小時

肆、資通安全政策及目標

一、資通安全政策

強化人員認知、避免資料外洩

落實日常維運、確保服務可用

二、資通安全目標

1. 依據資通安全政策願景，特訂定資通安全目標如下：

- (1) 辦理資通安全教育訓練，推廣員工資通安全之意識與強化其對相關責任之認知。
- (2) 保護本局暨所屬機關業務活動資訊，避免未經授權的存取與修改，確保其正確完整。
- (3) 定期進行內部稽核，確保有效實作及維持管理制度。
- (4) 確保本局暨所屬機關關鍵核心系統維持一定水準的系統可用性。

2. 資通安全政策及資通安全目標，詳參「IS-01-001 資通安全政策」。

3. 資訊安全績效及資訊安全管理系統之監督與量測程序，詳參「IS-02-016 監督與量測管理程序書」及「IS-04-045 資通安全目標有效性量測表」。

伍、資通安全推動組織

依資通安全管理法第 11 條之規定，本局副局長為資通安全長，殯葬管理處、兵役處及本市各戶政事務所應由其首長指派副首長或適當人員擔任其資通安全長，詳參「IS-02-002 資通安全組織程序書」。

陸、專職（責）人力及經費配置

一、專職（責）人力資源之配置

1. 依資通安全責任等級分級辦法之規定，本局、殯葬管理處、兵役處，係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，負責推動所轄機關之法遵義務執行及資訊安全管理系統之導入，並配合本局推動資通安全相關活動。
2. 依資通安全責任等級分級辦法之規定，各戶政事務所係屬資通安全責任等級 D 級，必須配合本局推動資通安全相關活動。
3. 本機關現有資通安全專職（責）人員名單應列冊，並適時更新。
4. 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職（責）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。
5. 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：
 - 至少一名資通安全專職人員，分別持有證照及證書各一張以上，並持續維持證照及證書之有效性。
6. 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，應簽署書面約定，並視需要實施人員輪調，建立人力備援制度。
7. 各機關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。
8. 資通安全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. 資通安全管理推動委員會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委員會提出，由資通安全委員會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

本機關應每年辦理資訊及資通系統資產盤點及標示，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，詳參「IS-02-004 資訊資產管理程序書」。

二、機關資通安全責任等級分級

本局、殯葬管理處、兵役處屬資通安全責任等級C級；其餘各戶政事務所屬資通安全責任等級D級。

捌、資通安全風險評估

本機關應每年針對資訊及資通系統資產進行風險評估，詳參「IS-02-005 風險評鑑與管理程序書」。

玖、資通安全防護及控制措施

1. 「IS-02-006 人員安全與教育訓練程序書」。
2. 「IS-02-007 實體安全管理程序書」。
3. 「IS-02-008 通信與作業管理程序書」。
4. 「IS-02-009 存取控制管理程序書」。
5. 「IS-02-010 系統開發與維護程序書」。

6. 「IS-02-011 委外管理程序書」。
7. 「IS-02-012 安全事件管理程序書」。
8. 「IS-02-013 營運持續運作管理程序書」。
9. 「IS-02-014 資訊安全稽核作業程序書」。
10. 「IS-02-015 矯正及持續改善管理程序書」。
11. 「IS-02-016 監督與量測管理程序書」。
12. 「IS-03-001 資訊資產管理說明書」。
13. 「IS-03-002 帳號及通行密碼管理說明書」。
14. 「IS-03-003 系統開發與維護作業說明書」。
15. 「IS-03-004 資訊備份管理說明書」。

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，詳參「高雄市政府民政局暨所屬機關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：
 - (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(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及系統弱點修補作業，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，進行必要之系統弱點修補作業，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，選任及監督受託者，應注意下列事項：

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安全性檢測證明，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。
- ## 三、委外人員之管理規範，詳參「IS-02-010 委外管理程序書」。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

1. 本局、殯葬管理處、兵役處之資通安全專職人員每年至少接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練。
2. 本局、殯葬管理處、兵役處之資通安全專職人員以外之資訊人員每二年至少接受 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. 本機關之一般使用者與主管，每人每年接受 3 小時以上之資通安全通識教育訓練。

二、資通安全教育訓練辦理方式

1. 本機關應每年考量管理、業務及資訊等不同工作類別之需求，擬定年度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認知宣導及教育訓練紀錄。

2. 本機關資通安全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，詳參「IS-04-013 人員資訊安全守則」。
4. 資通安全教育訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。
5. 資通安全教育訓練規範，詳參「IS-02-006 人員安全與教育訓練程序書」。

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

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

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

1. 本局暨所屬機關應定期（本局、殯葬管理處、兵役處至少每二年一次）或於系統重大變更或組織改造後執行一次內部實地稽核作業，且每年除內部實地受稽機關外，其餘本局暨各所屬機關應辦理書面稽核作業。
2. 本局、殯葬管理處、兵役處應視需要不定期針對委外服務供應商（包含委外服務廠商及協力廠商）執行外部稽核或專案稽核。

3. 稽核作業程序，詳參「IS-02-014 資訊安全稽核作業程序書」。

三、資通安全維護計畫之持續精進及績效管理

1. 本機關之資通安全委員會應於每年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，必要時得召開臨時會議。
2. 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。
3. 管理審查議題應包含下列討論事項：
 - (1) 先前管理審查之行動的狀態。
 - (2) 資訊安全管理系統內外部議題之變更。
 - (3) 資訊安全績效回饋，包含下列趨勢：
 - A. 稽核結果。
 - B. 不符合項目及矯正措施。
 - C. 資訊安全目標符合度。
 - D. 監視與量測結果。
 - (4) 關注各方之回饋。
 - (5) 風險評鑑結果及風險處理計畫之狀態。
 - (6) 持續改善之機會。
 - (7) ISMS 範圍適切性：
 - A. 內、外部議題分析討論、關注者需求與期望討論。
 - B. 活動間的介面及相依性分析。
 - (8) 資訊安全政策審核。
 - (9) 現有人員職能評估成果。
 - (10) 溝通與傳達規劃。

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，應每年向上級或

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

1. 著作權法
2. 檔案法
3. 檔案法施行細則
4. 中華民國刑法
5. ISO/IEC 27001：2013
6. 公務人員任用法
7. 公務人員任用法施行細則
8. 公務員懲戒法
9. 政府機關（構）資安事件數位證據保全標準作業程序
10. 民法
11. 個人資料保護法
12. 個人資料保護法施行細則
13. 行政院國家資通安全會報設置要點
14. 公務機關所屬人員資通安全事項獎懲辦法
15. 政府資訊公開法
16. 電子簽章法
17. 資通安全管理法
18. 資通安全管理法施行細則
19. 資通安全責任等級分級辦法
20. 資通安全事件通報及應變辦法
21. 資通安全情資分享辦法

22. 高雄市政府所屬各機關資訊系統設置管理要點
23. 高雄市政府民政局暨所屬機關資通安全維護計畫
24. 高雄市政府民政局暨所屬機關資通安全事件通報及應變管理程序

二、相關程序及說明

1. IS-02-001 組織全景分析程序書
2. IS-02-002 資通安全組織程序書
3. IS-02-003 文件管理程序書
4. IS-02-004 資訊資產管理程序書
5. IS-02-005 風險評鑑與管理程序書
6. IS-02-006 人員安全與教育訓練程序書
7. IS-02-007 實體安全管理程序書
8. IS-02-008 通訊與作業管理程序書
9. IS-02-009 存取控制管理程序書
10. IS-02-010 系統開發與維護程序書
11. IS-02-011 委外管理程序書
12. IS-02-012 安全事件管理程序書
13. IS-02-013 營運持續運作管理程序書
14. IS-02-014 資訊安全稽核作業程序書
15. IS-02-015 矯正及持續改善管理程序書
16. IS-02-016 監督與量測管理程序書
17. IS-02-017 法律遵循管理程序書
18. IS-03-001 資訊資產管理說明書
19. IS-03-002 帳號及通行密碼管理說明書
20. IS-03-003 系統開發與維護作業說明書

21. IS-03-004 資訊備份管理說明書

三、附件表單

1. IS-04-003 資通安全組織成員表
2. IS-04-009 資訊資產清單
3. IS-04-010 威脅弱點評估表
4. IS-04-011 風險改善計畫表
5. IS-04-012 風險評估報告
6. IS-04-015 人員職掌清冊
7. IS-04-016 人員保密切結書
8. IS-04-017 教育訓練計畫
9. IS-04-018 教育訓練簽到表
10. IS-04-020 人員進出機房登記表
11. IS-04-021 設備進出及異動紀錄表
12. IS-04-030 委外廠商保密切結書
13. IS-04-031 委外廠商保密同意書
14. IS-04-032 委外廠商稽核計畫
15. IS-04-033 委外廠商稽核查檢表
16. IS-04-034 委外廠商稽核報告
17. IS-04-037 業務流程衝擊分析表
18. IS-04-038 營運持續運作計畫
19. IS-04-039 營運持續演練報告
20. IS-04-040 ISMS 內部稽核計畫
21. IS-04-041 ISMS 內部稽核查檢表
22. IS-04-042 ISMS 內部稽核報告
23. IS-04-045 資通安全目標有效性量測表

24. IS-04-046 ISMS 有效性量測表

25. IS-04-047 法規一覽表