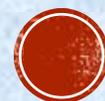


資通安全維護計畫填寫說明



大綱

- 依據
- 資通安全維護計畫填寫重點



依據

■ 資通安全管理法

- §5：主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。
- §12：公務機關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；無上級機關者，其資通安全維護計畫



依據

- 資通安全管理法實行細則
- §6I(1)

- 一、核心業務及其重要性。
- 二、資通安全政策及目標。
- 三、資通安全推動組織。
- 四、專責人力及經費之配置。
- 五、公務機關資通安全長之配置。
- 六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。
- 七、資通安全風險評估。

- 八、資通安全防護及控制措施。
- 九、資通安全事件通報、應變及演練相關機制。
- 十、資通安全情資之評估及因應機制。
- 十一、資通系統或服務委外辦理之管理措施。
- 十二、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。
- 十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

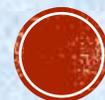
資通安全維護計畫填寫重點

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○○全機關，以及所屬○○機關(E級)。請填寫單位名稱



資通安全維護計畫填寫重點

■ 參、核心業務及重要性

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。

■ 依據資通安全管理法施行細則第7條規定核心業務與系統

- 依其組織法規：地政事務所（土地管理-地政系統）、戶政事務所（戶籍管理-戶役政系統）
- 維運所必要之業務：縣府（公文系統、全球資訊網）

■ 最大可容忍中斷時間

當資通系統停止提供服務時，組織可忍受的最大時間。應以小時計算。



資通安全維護計畫填寫重點

■ 一、核心業務及重要性

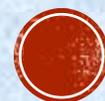
核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍 中斷時間
地方行政機關 業務	公文系統(由上 級機關維護)	<input type="checkbox"/> 為主管機關指定之 關鍵基礎設施 <input type="checkbox"/> 為主管機關核定資 通安全責任等級A級 或B級機關所涉業務 <input checked="" type="checkbox"/> 為本機關依組織法 執掌，足認為重要者 <input type="checkbox"/> 機關維運必要之業 務	如業務失效可能造成本單位及 相關單位行政效能降低	48小時



資通安全維護計畫填寫重點

■ 二、非核心業務及說明：

非核心業務	業務失效影響說明	最大可容忍中斷時間
行政電腦管理維護 (範例)	行政電腦故障時，影響機關行政效率	48小時
機關網路管理維護 (範例)	網路服務中斷時，影響機關連線作業	48小時
機關網站服務-網站系統 (範例)	網站服務中斷時，影響機關對外服務	24小時



資通安全維護計畫填寫重點

■肆、資通安全政策及目標

■ 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. 應因應資通安全威脅情勢變化，本機關同仁應參與資通安全教育訓練，以提高資通安全意識。
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. 定期進行內部稽核，確保相關作業皆能確實落實。



資通安全維護計畫填寫重點

■肆、資通安全政策及目標

■目標

- 1.本機關同仁皆完成3小時資通安全教育訓練。
- 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。(年度3級事件發生 ≤ 1 次)。
- 3.前次內部稽核發現事項，未完成改善之件數應 ≤ 2 件。

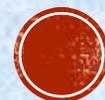


資通安全維護計畫填寫重點

■肆、資通安全政策及目標

■實施重點

1. 資通安全政策由本機關○○單位簽陳資通安全長核定。
2. 於單位公布欄公告



資通安全維護計畫填寫重點

■ 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○○長（副首長或適當人員）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...(後略)



資通安全維護計畫填寫重點

■ 伍、資通安全推動組織

■ 二、資通安全推動小組

- 依本法第11條之規定，本機關訂定○○長（副首長或適當人員）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
- 每年定期召開資通安全管理審查會議，或在內部行政會議中提報資通安全事項執行情形並進行管理審查。會議紀錄應包含
 - 1. 資通安全實施情形完成進度
 - 2. 資通安全應辦事項完成進度
 - 3. 宣導事項(如教育訓練)



資通安全維護計畫填寫重點

- 伍、資通安全推動組織
- 二、資通安全推動小組
- 實施重點：填寫或修正「資通安全推動小組成員及分工表」並進行陳核

職稱	職級	名稱	職掌事項	分機	備註	代理人
資通安全 長	主任	王○○	督導機關資通安全相關 事項	○○		陳○○
資通安全 推動小組	技士	林○○	推動資通安全相關政策 落實資通安全事件通報 及相關應變處理		資通 安全 專責 人員	李○○



資通安全維護計畫填寫重點

■陸、人力及經費配置

■實施重點

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(須以專職人員配置之)

2.證照要求

(1) 1張以上資通安全專業證照

(2) 1張以上資通安全職能評量證書

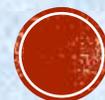


資通安全維護計畫填寫重點

■陸、人力及經費配置

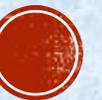
■實施重點：委外廠商人員(含駐點、叫修)需要簽屬

1. 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「資通安全保密同意書」



資通安全維護計畫填寫重點

- 柒、資訊及資通系統之盤點
 - 一、資產盤點
 - 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、人員資產等。



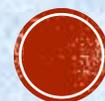
資通安全維護計畫填寫重點(C)

資產編號	資產類別	資產名稱	權責單位	存放位置	數量	資訊及資通系統名稱
HW-001	HW	差勤系統主機	人事室	機房A機櫃	1	差勤系統
HW-002	HW	防火牆	資訊室	機房A機櫃	1	N/A
HW-003	HW	全球資訊網主機	資訊室	機房A機櫃	1	全球資訊網
HW-004	HW	監視器(OO廠牌)	資訊室	機房外	2	
SW-001	SW	差勤系統	人事室	差勤系統主機	1	差勤系統
SW-002	SW	作業系統(Windows Server 2016)	人事室	差勤系統主機	2	差勤系統 全球資訊網
SW-003	SW	MS-SQL Server 2016	人事室	差勤系統主機	1	差勤系統
SW-005	SW	防毒軟體(NOD32)	人事室	差勤系統主機	1	差勤系統
SW-006	SW	商合行考勤讀卡機系統	人事室	差勤系統主機	1	差勤系統
SW-007	SW	全球資訊網	資訊室	全球資訊網主機	1	全球資訊網
ID-001	ID	差勤系統資料	人事室	差勤系統主機	1	差勤系統
PE-001	PE	系統管理人員	人事室	人事室	1	差勤系統



資通安全維護計畫填寫重點(D)

資產編號	資產類別	資產名稱	權責單位	存放位置	數量	備註
HW-001	HW	個人電腦	秘書室	辦公室	10	
HW-002	HW	防火牆	秘書室	辦公室	1	
SW-001	SW	防毒軟體	秘書室	個人電腦	10	
SW-002	SW	作業系統 (Windows 10)	秘書室	個人電腦	4	
SW-003	SW	作業系統 (Windows7)	秘書室	個人電腦	6	
SW-004	SW	作業系統 (WindowsXP)	秘書室	個人電腦	6	
PE-001	PE	資訊設備管理 者	秘書室	秘書室	1	



資通安全維護計畫填寫重點

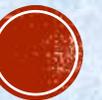
■ 柒、資訊及資通系統之盤點

■ 二、機關資通安全責任等級分級

B：本機關因區域性或地區性民眾個人資料檔案之持有及處理，為資通安全責任等級B級機關。

C：本機關因維運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。

D：本機關因自行辦理資通業務，未維運自行或委外開發之資通系統，為資通安全責任等級D級機關。



資通安全維護計畫填寫重點

■捌、資通安全風險評估

■實施重點

- 1.本機關應每年針對資訊及資通系統資產進行風險評估，並填寫「風險評估表」。
- 2.當資產風險為高風險時，應填寫「風險改善計畫表」進行風險改善作業。



資通安全維護計畫填寫重點(C)

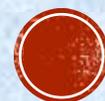
風險評估表										
項次	資產編號	資產名稱	機密性	完整性	可用性	威脅	弱點	可能性	衝擊性	風險值
1	HW-001	差勤系統主機	2	3	3	極端的溫濕度	環境監控不足	2	2	40
2	HW-002	防火牆	3	3	2	技術失能	技術設施維護不恰當	1	3	24
3	HW-003	全球資訊網主機	1	3	3	極端的溫濕度	環境監控不足	3	3	63
4	HW-004	監視器	1	2	2	偷竊	缺少實體安控。	2	2	20
5	SW-001	差勤系統	3	4	4	軟體程式錯誤	缺少有效的型態管理控制	1	3	33
6	SW-002	作業系統(Windows Server 2016)	2	2	1	入侵	未更新或安裝作業系統/軟體的修補程式	1	2	10
7	SW-003	MS-SQL Server 2016	2	2	1	入侵	未更新或安裝作業系統/軟體的修補程式	1	2	10
8	SW-005	防毒軟體(NOD32)	2	2	1	軟體程式錯誤	缺少有效的型態管理控制	1	3	15
9	SW-006	商合行考勤讀卡機系統	3	3	3	軟體程式錯誤	缺少有效的型態管理控制	1	3	27
10	SW-007	全球資訊網	1	3	3	軟體程式錯誤	缺少有效的型態管理控制	1	3	21
11	ID-001	差勤系統資料	3	4	4	未授權存取資料	網路存取規劃不當	1	3	33
12	PE-001	系統管理人員	3	4	4	社交工程	通訊未加密	1	3	33



資通安全維護計畫填寫重點(D)

風險評估表

項次	資產編號	資產名稱	機密性	完整性	可用性	威脅	弱點	可能性	衝擊性	風險值
1	HW-001	個人電腦	3	2	1	作業人員或使用 者錯誤	使用者認知不足	2	3	36
2	HW-002	防火牆	3	3	2	技術失能	技術設施維護不恰當	1	3	24
3	SW-001	防毒軟體	2	2	1	軟體程式錯誤	缺少有效的型態管理 控制	1	3	15
4	SW-002	作業系統 (Windows 10)	2	2	1	入侵	未更新或安裝作業系 統/軟體的修補程式	1	2	10
5	SW-003	作業系統 (Windows7)	2	2	1	入侵	未更新或安裝作業系 統/軟體的修補程式	1	2	10
6	SW-004	作業系統 (WindowsXP)	3	4	2	入侵	未更新或安裝作業系 統/軟體的修補程式	3	3	81
7	PE-001	資訊設備管理者	3	2	2	社交工程	通訊未加密	1	3	21



資通安全維護計畫填寫重點

■ 玖、資通安全防護及控制措施(C)

■ 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，並填入「資通系統清冊」。



資通安全維護計畫填寫重點

■ 資訊系統清冊

編號	資通系統名稱	機密性	完整性	可用性	法律遵循性	系統防護需求等級	承辦(管理)單位	備註
1	差勤系統	中	普	普	普	中	人事室	
2	全球資訊網	普	中	中	普	中	資訊室	



資通安全維護計畫填寫重點

- 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，參閱「資通安全事件通報及應變管理程序」。
- 實施重點：**呈核後資通安全長後公告**



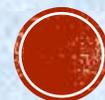
資通安全維護計畫填寫重點

- 壹拾參、資通安全教育訓練(C)
 - 1. 本機關依資通安全責任等級分級屬C級，資通安全專責人員1人(須以專職人員配置之)，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。
- 實施重點：第2項需針對全機關發出通知



資通安全維護計畫填寫重點

- 壹拾參、資通安全教育訓練(D)
 - 1.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。
- 實施重點：需針對全機關發出通知



資通安全維護計畫填寫重點

- 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
- 資通安全推動小組應定期(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
- 實施重點：填寫稽核自評表，並呈資通安全長簽章



資通安全維護計畫填寫重點

- 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
- 本機關應規劃適當之稽核作業，並定期對所屬或所監督之機關進行資通安全維護計畫實施情形稽核。
- 實施重點：要求所屬機關填寫稽核自評表，送上級機關備查。



Q/A

問題與討論

