內政部消防署暨所屬機關資通安全政策及管理要點第參點、第肆點、第伍點修正規定

參、資通安全目標

建立安全及可信賴之電腦化作業環境，以確保本署電腦資料、系統、設備及網路安全。本署整體性資通安全定量化目標如下：

一、發生「國家資通安全通報應變作業綱要」所定義之 3 級以上資訊安全事件，每年不得高於一件。

二、依國家資通安全會報之「資訊系統分類分級與鑑別機制」所評鑑系統安全等級「中（等級 2）」以上之系統可用性每年（365 天*24 小時）達 99%。

三、提供民眾服務之資訊系統可用性每年（365 天*24 小時）達 97.5%。

肆、資通安全範圍及業務分工

資通安全範圍共分十四大項，業務分工如下：

（一）資通安全政策制定及評估：由資訊安全組織及資訊單位負責。

（二）資通安全組織及權責：由資訊安全組織、人事、政風及資訊單位負責。

（三）資訊資產分類與控管：由資訊及財產管理單位負責。

（四）人員安全管理：由人事及資訊單位負責。

（五）實體及環境安全管理：由資訊單位及秘書室（或總務相關單位）負責。

（六）運作安全：由資訊單位負責。

（七）通訊安全：由資訊單位負責。

（八）存取控制：由資訊及業務單位負責。

（九）加密措施與密碼管理：由資訊單位負責。

（十）系統開發與維護：由資訊單位負責。

（十一）供應商關係：由資訊單位或總務單位負責。

（十二）資安事故管理：由資訊及業務單位負責。

（十三）營運持續管理：由資訊安全組織或資訊單位負責。

（十四）資通安全措施符合性檢查：由政風及資訊單位負責。

伍、資通安全管理

一、資通安全政策評估

資通安全政策評估，應由具專業技術及知識之內部稽核單位、獨立客觀的主管人員或委請公正超然的專業組織或團體辦理，且每年至少評估一次。

二、資通安全組織及權責

（一）資通安全組織

1. 電子化政府發展推動小組

指派本署「電子化政府發展推動小組」為內部最高資通安全組織，負責下列資通安全管理事項：

(1) 資通安全政策之核定、推動及協調。

(2) 資通安全計畫之核定、核轉及督導。

(3) 資通安全責任之分配及協調。

(4) 資訊資產保護事項之監督。

(5) 重大資通安全事件之檢討及監督。

(6) 其他資通安全事項之核定。

本署「電子化政府發展推動小組」由主任秘書擔任召集人，每年至少召開會議一次，研討並評估資通安全政策事宜，以反映政府法令、技術及業務等最新發展現況，確保資通安全實務作業之有效性。

2. 資通安全推行及稽核小組

為順利推展資通安全各項工作，設置「內政部消防署資通安全稽核小組」，由資訊室、政風室各派至少一人組成，負責推動資通安全稽核事項。

（二）資通安全權責分工

1. 資通安全相關政策、計畫、措施及技術規範之研議，以及安全技術之研究、建置及評估相關事項，由資訊室負責辦理。

2. 人員進用安全評估由人事室負責辦理。

3. 資訊機密維護及稽核使用管理事項，由政風室會同資訊室及各相關單位負責辦理。

4. 資料及資訊系統之安全需求研議、使用管理及保護等事項，由各業務單位負責辦理。

三、資訊系統分類與控管

依行政院國家資通安全會報頒布之「資訊系統分級與資安防護基準作業規定」進行系統分類分級，並依系統等級落實資安防護措施。

四、人員安全管理

（一）業務主管對工作職掌須使用及處理敏感性資訊的電腦設備或涉及機密性及敏感性資訊之人員，應依據平常工作之考核，指派或適時調整工作。

（二）人員離（休）職時，應立即取消使用單位內各項資訊資源之所有權限，並列入機關人員職務異動之必要手續。

（三）應要求使用者確實瞭解系統存取的各項條件及要求，只能在授權範圍內存取系統資源。

（四）使用者不得將個人登入身份識別碼與密碼交付他人使用，亦不得以任何方法竊取他人的登入身分識別碼與密碼。

（五）應定期檢查及註銷閒置不用的識別碼及帳號。

（六）使用者應負責保管及定期更換個人密碼，維持密碼的機密性。
（七）當有跡象顯示使用者密碼可能遭破解時，應立即更改密碼。
（八）本署針對不同工作類別之需求，應辦理資通安全教育訓練及宣導，或派員參加外部機構相關訓練，促使員工瞭解資通安全的重要性、各種可能的安全風險，以提高員工資通安全意識，促其遵守資通安全規定。
（九）資通安全教育及訓練的內容應包括資通安全政策、資通安全法令規定、資通安全作業程序、以及如何正確使用資訊科技設施等。

五、實體及環境安全管理

（一）設備（含電腦、電力及通訊纜線等）應安置在適當的地點並予以保護，以減少環境不安全引發的危險及減少未經授權存取系統的機會。
（二）電源供應得將不斷電系統失效之後的應變措施納入，對於特別敏感性或是特別重要的系統，應採取額外強化的安全措施。
（三）應妥善地維護設備，以確保設備的完整性及可以持續使用。
（四）可攜式電腦設備應指定專人保管。
（五）處理報廢之電腦設備時，含有儲存媒體的設備項目（如硬碟），應在處理前由使用者或使用單位詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體已經被移除。
（六）機房管制

1. 機房管制區域範圍
   (1) 主機房：指放置電腦主機、通訊設備及重要週邊與設施之所在地。
   (2) 操作室：指放置電腦主機控制端末設備與監控設備之所在地。
   (3) 媒體區：指放置電腦重要資料與資料儲存媒體之所在地，如磁片、磁帶、光碟片等。
   (4) 機電室：指供給電腦機房主要機電設備的所在地如電源穩壓器、不斷電系統、空調設備、電信配線設備等。
2. 機房管制規定：可適用任何進出機房、操作室等管制區域的工作人員。
   (1) 任何人員不得攜帶非工作上所需之物品，如飲料、食物進入機房（辦公區除外）。
   (2) 不得在機房及操作室等管制區域內吸煙。
   (3) 操作台上各種文具、報表、手冊、表單等應整齊，用完後歸定位。
   (4) 機房設備若需外送修理或修妥送回，應填列出入管制

所需之「機房服務申請單」。

(5) 報表及文件應先在「機房服務申請單」登記後，再送出機房以集中焚毀或碎紙機處理。

(6) 機房使用之物品如磁帶、磁碟等應放置於規定地點並貼立標記。

(7) 應定期實施防治鼠害及其他蟲害等措施，以保護電纜、電線及機器設備。

(8) 電腦及儲存媒體需經電腦病毒掃毒合格後，方可攜入機房。

（七）辦公桌面之安全管理

1. 辦公桌面應儘量保持淨空，以減少文件及磁碟片等在辦公時間外，遭人取用、遺失或被破壞的機會。
2. 個人電腦不再使用時，應關機、上鎖或是其他控制措施保護。

（八）重要資訊系統主機（含網路設備）應加裝不斷電系統，以因應不正常的斷電或停電等狀況。

（九）關於本項目之施行細節，由本署資訊室訂定「電腦機房管理要點」，於簽請批核後發送各相關單位及所屬機關參照實施。

六、運作安全

（一）各類電腦主機、伺服器及個人電腦均應指定專人管理，不得任意使用、拆卸及更動零組件。

（二）各類電腦主機、伺服器及個人電腦皆應由管理者或使用者設定密碼。

（三）存放機密性及敏感性資料之電腦主機或伺服器，除作業系統既有的安全設定外，應強化身份辨識之安全機制，防止非法使用者透過遠端撥接或網際網路傳送資料時，被偷窺或截取登入密碼，及防制假冒合法使用者身分登入主機進行偷竊或破壞等情事。

（四）防範電腦病毒及惡意軟體之攻擊

1. 禁止使用未經授權之軟體，並遵守智慧財產權相關規定。
2. 嚴禁使用或開啟來路不明及內容不確定之軟體、磁性媒體或電子郵件。
3. 使用磁性媒體時，應在使用前詳加檢查是否感染電腦病毒。
4. 應安裝防毒軟體以阻絕電腦病毒。
5. 電腦病毒碼及防制軟體應由管理者或使用者定期更新。
6. 應定期修補系統漏洞程式。

（五）資料安全管理

1. 應保護重要的資料檔案，以防止遺失、毀壞、被偽造或竄改。
2. 應落實定期備份及電腦媒體異地儲存等作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

3. 重要資料須區分機密等級並依權限使用。
4. 應依使用者所負責業務性質及職掌，賦予不同資料存取權限，避免重要資料外漏或遭不經意之更動。
5. 儲存媒體應依媒體保存規格，存放在安全的環境以加強電腦媒體與資料文件之安全管理。
6. 可重複使用的資料儲存媒體，不再繼續使用時，應將儲存的內容消除。
7. 對高敏感性的資料，應在傳輸或儲存過程中以加密方法保護。
8. 存放民眾申請或註冊的私人資料檔案，應研究以安全方式處理，以防止資料遭不當（非法）使用、洩漏、竄改、竊取、破壞。
9. 禁止使用即時通訊軟體（例如：Line）傳輸機密公務資料。

七、通訊安全

（一）被授權的網路使用者，只能在授權範圍內存取網路資源，不得將自己的登入身份識別與登入網路的密碼交付他人使用。

（二）經由網際網路下載軟體或資料檔案，得視業務特性及需要，由使用單位事前測試及掃瞄，在確認安全無虞及不違反智慧財產權前提下，方得下載執行。

（三）對外開放的資訊系統中不得存放機密性及敏感性資料或文件。

（四）內部使用的瀏覽器，對下載的每一檔案應做電腦病毒的掃描。

（五）機密性資料或文件，不得以電子郵件傳送。

（六）各單位開放外界連線作業之資訊系統，必要時應以代理伺服器或資料庫隔離等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。

（七）應考量網際網路新技術的可能安全弱點，並採取適當的防護措施以確保內部網路安全。

（八）網路系統中各主要主機伺服器應評量其對業務之急迫性設立備援主機，以備主要作業主機無法正常運作時之用。

（九）網路系統中各主機應定期（或異動時）做系統備份，包括完整系統備份，系統架構設定備份。

（十）網路主機應關閉非必要的服務程式，並隨時更新程式版本。

（十一）關於本項目之施行細節，由本署資訊室訂定「網路使用管理規範」，於簽請批核後發送各相關單位及所屬機關參照實施。

八、存取控制

（一）對委外廠商或系統維護人員基於實際作業需要，資訊單位得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。但使用完畢後應立即取消其使用權限。

（二）應用系統之存取控制

1. 配賦應用系統的使用者與業務需求相稱的資料存取及應用系統使

用權限（例如限定使用者僅能執行唯讀、寫入、刪除或執行等功能）。

2. 處理敏感性資訊的應用系統，系統輸出的資料，應僅限於與使用目的有關者。

3. 各單位之重要資料委外建檔者，不論在單位內外執行，均應採取適當及足夠之安全管控措施，防止資料被竊取、竄改、販售、洩露及不當備份等情形發生。

（三）系統存取控制與管理

1. 業務系統應將其存取控制需求，明確告知系統服務提供者，以利其執行及維持有效的存取控制機制。

2. 業務應用系統擁有者，應訂定系統存取控制規定，並明定使用單位及使用人員的系統存取權利。

3. 使用者通行碼應適時更新。

4. 系統存取權限之配賦，應以執行業務及職務所必需者為限，當使用者調整職務及離（休）職時，應儘速註銷其系統存取權限。

5. 本署及各處電腦主機及應用系統使用者之識別碼及通行碼，均應限制使用，並嚴禁轉知他人，若已為他人知悉者，應即通知資訊單位適時更新；因故被冒用致造成不良後果，應負洩密之責。

6. 各單位應盡量避免允許系統服務廠商以遠端登入方式進行系統維修，否則應經審慎評估簽報機關首長權責主管核可，並應加強安全控管，建立人員名冊，課其相關安全保密責任。

（四）關於本項目之施行細節，由本署資訊室訂定「存取控制作業程序規範」，於簽請批核後發送各相關單位及所屬機關參照實施。

九、加密措施與密碼管理

（一）如涉及重要資料之傳輸，應使用加密金鑰，加密金鑰應妥善保護。

（二）宜強制資訊系統設定帳號通行密碼之複雜度，並定期變更新密碼。

十、系統開發與維護

（一）應將系統發展測試作業及系統正式作業之軟體，分別在不同處理器或不同的目錄下作業，以便系統測試與正式作業分開處理，並避免作業軟體或資料遭意外竄改，或不當使用。

（二）各單位委商開發或維護軟硬體設施時，應在單位相關人員監督及陪同下為之。

（三）委外發展資訊系統，應在系統生命週期之初始規劃階段，即將資通安全需求納入考量。

（四）資訊系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、後門及電腦病毒等危害系統安全。

（五）重要業務系統，應建立例行性稽核制度，建立稽核軌跡。

（六）對系統服務廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統帳號通行密碼。

（七）應注意系統開發環境安全，避免程式原始碼遭受不當污染。

（八）應使用安全的程式語法及程式元件開發，減低系統漏洞風險

（九）行動裝置應用程式安全

提供行動裝置（係指包含但不限於智慧型手機、平板電腦等具通信及連網功能之隨身設備）服務應注意下列安全要點：

1. 應針對應用程式檢視系統所需最小權限，並進行存取控制。
2. 於行動裝置上如有必要儲存敏感資料，應採取加密或亂碼化等相關機制保護，以防範資料外洩。
3. 應針對應用程式進行原始碼掃描、黑箱測試或滲透測試，並針對中、高風險弱點及可影響敏感資料被竊取或竄改之弱點進行改善。（中、高風險：係依據美國國家標準技術研究所【NIST】所公布或以共同漏洞評分系統【Common Vulnerability Scoring System，CVSS】工具計算出之風險等級）

（十）關於本項目之施行細節，由本署資訊室訂定「系統開發及維護作業程序規範」，於簽請批核後發送各相關單位及所屬機關參照實施。

十一、 供應商管理

（一）委外處理的電腦文件、軟體設計、媒體蒐集及委外處理資料，應慎選有足夠安全管理能力及經驗的機構作為委辦對象。

（二）本署及所屬機關資訊業務委外時，應於事前審慎評估可能的潛在安全風險（例如資料或使用者通行碼被破解、系統被破壞或資料損壞等風險），與廠商簽訂適當的資通安全協定，將相關的安全管理責任納入契約條款。

（三）關於本項目之施行細節，由本署資訊室訂定「資訊委外作業程序規範」，於簽請批核後發送各相關單位及所屬機關參照實施。

十二、 資訊安全事故處理

（一）本署及所屬機關遭受資通安全事件時，應立即陳報，並通知資訊單位依相關規定進行緊急應變處置。

（二）本署及所屬機關每年應至少辦理一次資通安全災害回復演練，其演練項目由各機關自訂。

十三、 營運持續管理

（一）本署及所屬機關應針對其掌管之重要電腦資源（含電腦主機系統、應用系統及資料庫等）擬定資料備份、還原與異地儲存計畫並確實辦理。

（二）應建立跨部門的資訊系統業務持續運作程序，研訂及維護業務持續運作之計畫，以降低人為或是意外因素對重要資訊業務運作可能導致的威脅，使重要資訊業務在系統發生事故、設施受損害時，仍可持續運作。

（三）關於本項目之施行細節，由本署資訊室訂定「業務持續運作程序規範」，於簽請批核後發送各相關單位及所屬機關參照實施。

十四、 資通安全措施符合性之檢核

（一）禁止使用違反著作權、善良風俗或會妨害網路系統的正常運作之不法或不當的資訊。

（二）資通安全稽核

1. 內部稽核：本署及所屬機關應訂定稽核計畫簽報機關首長核准後實施，並得視狀況適時辦理修正。
2. 外部稽核：本署得定期或不定期對所屬機關實施外部稽核作業。
3. 本署及所屬機關實施稽核作業時，應詳實記錄查核情形，並撰寫稽核報告，簽報機關首長核閱。
4. 前項有關查核記錄與檢討報告等，應由查核單位妥為保管，以供本署或相關權責機關實施外部稽核時之參考。
5. 稽核報告之建議事項，應由受稽核之主辦單位負責辦理或改善。
6. 關於本項目之施行細節，由本署政風室會同資訊室訂定相關稽核計畫，於簽請批核後參照實施。