文件等級：公開

行政院環境保護署

資訊安全管理規範

第 4.2 版

核准文號：環署資字第 1051117374 號函

頒行：89 年 2 月

修訂：105 年 10 月 28 日

行政院環境保護署資訊安全管理規範

壹、 總則

一、訂定目的

行政院環境保護署（以下簡稱本署）為維護資訊系統的正常運作、確保資訊傳輸交易安全，並保障本署電腦處理資料之機密性與完整性，特訂定本規範。

二、訂定參考

（一）經濟部標準檢驗局 CNS 27002、CNS 27001 規範。
（二）ISO/IEC 27001:2013 標準。
（三）行政院所屬各機關資訊安全管理要點。
（四）個人資料保護法。
（五）電子簽章法。

三、適用對象

本署員工、臨時人員及接受本署委辦案派駐本署之人員。

四、適用範圍

（一）資訊安全政策制定及評估。
（六）資訊安全組織及權責。
（七）人員安全管理及教育訓練。
（八）資訊資產之安全管理
（九）系統存取控制。
（十）密碼學管理。
（十一）實體及環境安全管理。
（十二）電腦系統安全管理。
（十三）通訊安全管理。
（十四）系統發展及維護之安全管理。
（十五）供應商關係管理。
（十六）資訊安全事故管理。
（十七）營運持續運作計畫之規劃及管理。
（十八）遵循性。

五、資訊安全管理系統量測指標及量測方法

為有效量測資訊安全管理系統（以下簡稱 ISMS）目標之達成狀況，針對 ISMS 施行範圍之規範、資訊安全政策之要求及風險情形，訂定資訊安全績效指標及量測方法，每年管理審查檢視指標與目標適切性及目標達成情形。

貳、 組織全景及利害關係人鑑別

一、 依據全景及資安需求決定實施範圍

本署依與目的有關且影響達成 ISMS 達成預期成果之內部及外部議題、資訊安全需求，包含相關法律要求，民眾及主管機關政策需求及各項業務之特性,決定本署 ISMS 實施範圍。

二、 定期審核 ISMS 實施範圍

每年管理審查時，重新檢視內部及外部議題、資安需求及業務特性，確認 ISMS 之範圍適切性。

參、 組織與權責

一、 資訊安全工作組

為統籌本署資訊安全管理事宜,於本署「資訊發展推動小組」下設「資訊安全工作組」(以下簡稱本工作組)及「資訊安全稽核小組」(以下簡稱稽核小組)，資訊安全管理組織架構如圖 1。本工作組由本署監資處專門委員擔任工作組主持人。本署監資處及各業務處共同負責本署資訊安全管理工作，資訊系統安全控制技術由本署監資處負責辦理，資料及資訊系統之安全使用及保護事宜由各業務處負責辦理。必要時，本工作組得委請署外學者專家提供資訊安全顧問諮詢服務及技術支援協助，並依規定支給相關費用。

稽核小組由政風室主任擔任稽核小組主持人,稽核業務由政風室及監資處共同辦理。資訊系統安全控制技術稽核由監資處負責辦理，資訊安全稽核得合併於本署年度公務機密檢查由政風室會同相關單位負責辦理。

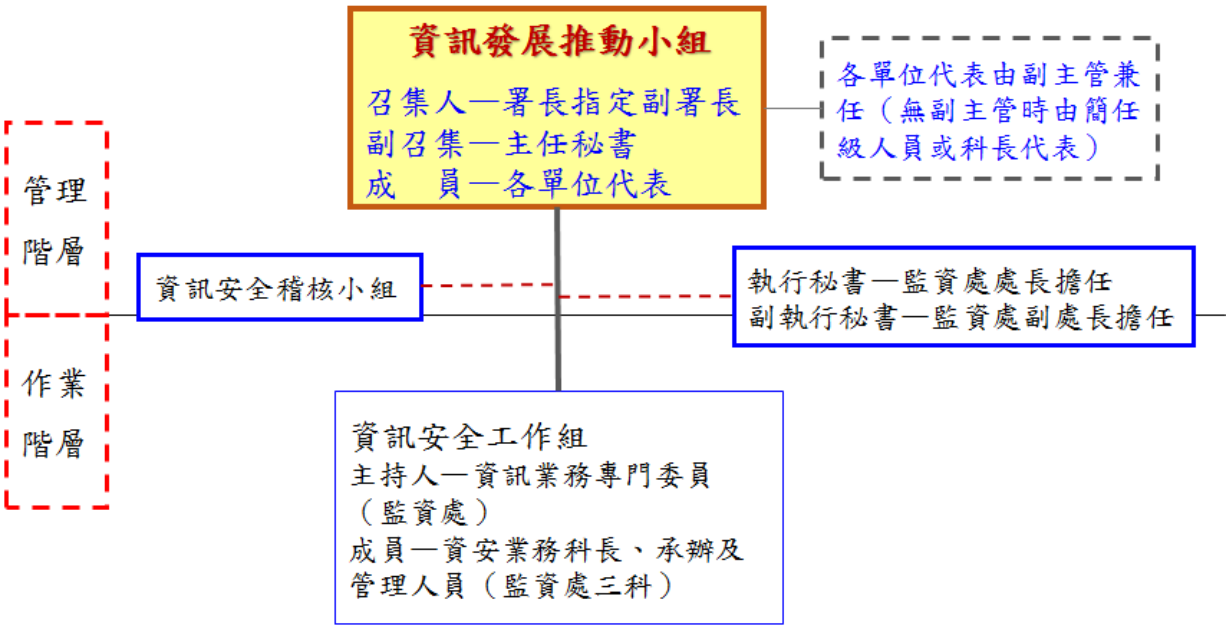

圖 1：資訊安全管理組織架構圖

二、 資訊安全相關人員安全權責

（一）一般人員

1. 使用人員妥善保管個人電腦及磁片，每日下班前關閉電腦及電源。
2. 使用人員設使用權限，進入系統不得任意更改使用權限，以確保系統安全，適時防範操作時之疏失。
3. 使用人員對通行密碼妥慎保管，不得洩漏或借給他人使用，設有特殊權限應用系統，使用人員如需代理人，則需另行申請使用權限及通行密碼。

（二）網路系統管理人員

1. 定時統計本署網路使用情形並評估網路設備現況，以提高網路速率，提供擴充設備之憑據。
2. 建立及維護本署網路系統使用者帳號。
3. 記錄網路系統異常狀況及維護相關書面資料。

（三）應用系統維護人員

1. 負責使用者代碼管理、權限管理、病毒防制、稽核作業程序等，以落實應用系統安全策略之要求。
2. 維護人員每日進出系統皆有維護紀錄，應用系統本身須提供安全控管功能，以滿足作業時之認證、授

權與稽核之安全管理需求，確保資訊安全。

（四）機房管理人員

1. 負責機房進出人員之管理、機房工作日誌之督導查核及機房異常狀況之管理。
2. 建立及更新機房配備圖，標明每一設備名稱及位置。
3. 建立機房電源操作手冊，以因應特殊狀況緊急開關電源之操作程序及相關耗材清理更換。

（五）委外人員管理者

1. 訂定受委託管理資訊系統存取控制規定，界定存取控制之需求，並以書面或其他電子方式記錄之。
2. 將受委託管理資訊系統之存取控制需求，明確告知委外服務人員，以利其執行及維持有效的存取控制機制。
3. 資訊系統存取控制規定之研擬，考量事項如下：
   (1)個別業務應用系統之安全需求。
   (2)資訊傳佈及資料應用之名義與授權規定。
   (3)相關法規或契約對資料保護及資料存取之規定。
   (4)契約終止時，確保本署資訊及資產安全回收或是銷毀的措施。

（六）委外服務人員

1. 委外網路管理人員
   (1)建立及維護本署網路系統使用者帳號。
   (2)定期記錄網路系統異常狀況及維護相關書面資料。
   (3)建立及維持一份有權存取系統的委外人員名單。
2. 委外系統維護人員
   (1)盡軟硬體系統建置及維護的責任。
   (2)尊重智慧財權及資訊公開的限制。
   (3)系統維護人員每日進出系統皆需填寫維護紀錄，委外應用系統本身須提供安全控管功能，以滿足作業時之認證、授權與稽核之管理需求，確保資訊安全。
3. 委外操作人員

(1)進出系統皆需填寫工作紀錄。

(2)委外操作人員妥善保管個人電腦及磁片，每日下班前關閉電腦及電源。

(3)負責機房之操作，執行進出人員紀錄、填寫機房工作日誌與異常狀況處理情形，以供未來處理之參考。

(4)機房環境管理與控制，確保機房冷氣正常運轉，維持一定之室溫，並建立冷氣故障之緊急處理程序。

（七）資訊安全稽核小組

1. 依據本管理規範及配合上級主管機關所辦理之外部稽核制度，由本署監資處簽奉核定本署年度稽核計畫，對相關部門及人員進行資訊系統及技術應用之安全評估，以確保其遵循機關之資訊安全政策及管理規範。
2. 資訊系統擁有者配合資訊安全稽核小組定期的資訊安全評估作業，檢討相關人員是否遵守機關的資訊安全政策、規範及相關安全規定。
3. 定期或因應突發性、專案性及特殊性之資訊安全稽核需要不定期檢討評估各項軟、硬體設備的安全性，以確保其符合機關的安全標準；評估的內容包括作業系統的評估，以確保系統軟體及硬體的安全控制措施正確地執行。
4. 安全風險評估由具有專業知識及豐富經驗的系統工程人員或委請外界學者專家協助，在權責主管人員的監督下，以人工或是自動化的軟體工具執行安全檢查，產生技術評估報告，以利日後解讀分析。
5. 每年依據本署年度稽核計畫，定期進行資訊安全稽核工作，必要時得不定期視需要進行專案稽核工作。本署內部及所屬機關資訊安全稽核由政風室主辦，本署監資處協辦；本署各單位暨所屬各機關均配合資訊安全稽核工作之進行。

（八）溝通或傳達

為確保 ISMS 的有效執行，各溝通項目權責人員，遵循下表進行 ISMS 相關事項之溝通或傳達以達成溝通預期效果。

溝通項目	溝通時機	溝通對象	權責人員	預期效果	溝通方式
資訊安全政策	管理審查作業製/修訂時	範圍內人員	資訊安全執行秘書	人員對政策認知及了解	制定文件、政策審查，公告
組織角色、責任與職權	製/修訂時	範圍內人員	資訊安全執行秘書	確保責任與職權已溝通及瞭解	制定文件，公告
資訊安全管理目標	管理審查作業製/修訂時	範圍內人員	資訊安全執行秘書	確保管理系統與目標達成之有效性；未符合目標及改善方式	公告、管理審查簽辦、會議
資訊安全風險處理計畫與接受殘留資訊	管理審查作業風險評估完成時	風險擁有者	資訊安全工作組	對風險項目及殘留風險認知	風險評鑑報告
不符合資訊安全管理的事件	管理審查作業	範圍內人員/委外廠商	資訊安全工作組	確保不符合事項處理方式及不再發生	管理審查簽辦、會議
稽核結果	稽核完成管理審查作業	召集人	資訊安全稽核小組	管理系統之落實度、符合性及有效性之確認	稽核報告管理審查簽辦、會議

溝通項目	溝通時機	溝通對象	權責人員	預期效果	溝通方式
ISMS 運作狀況亟需改善之處	管理審查作業	召集人	資訊安全執行秘書	確保管理系統適用性、充足性與有效性	管理審查簽辦、會議
資安事件通報	資安事件發生時	行政院國家資通安全會報	資訊安全工作組	通報資安事件發生之時間、範圍及原因等，必要時尋求協助。	國家資通安全通報應變網站

肆、 規範內容

一、 資訊安全政策的制定及評估

（一）資訊安全政策之制定

1. 資訊安全政策的目的為防禦一切有計畫的、意外的、來自內部的或外部的威脅，以保護本署資訊資產的安全。為表達本署對資訊安全推動之支持與決心，制定資訊安全政策。
2. 制定之資訊安全政策宣達至各階層之同仁，一體遵循。

（二）資訊安全政策與管理規範之評估

資訊安全政策、管理規範及相關管理辦法每年定期進行獨立及客觀的評估，以反映政府資訊安全管理政策、法令、技術及機關業務之最新狀況，確保資訊安全實務作業之可行性及有效性。

（三）管理階層審查

為確保資訊安全管理制度持續有效運作，透過管理階層之審查，用以確保制度的適用性、適切性與有效性，並藉由稽核持續加以改善。相關內容及表單請參考預防與改善流程。

（四）文件與記錄管理

為確保文件與紀錄之一致性與可追溯性，進而可再生運用，提昇其價值。相關內容及表單請參考文件與紀錄管理流程。

二、 資訊安全組織及權責。

（一）資訊安全之角色及責任

本署成立資訊安全組織以推動資訊安全事務，並透過正式的組織與管理階層授權，界定資訊安全責任

（二）職務區隔

以實體防護及存取控制管制，以做適當之職權區分，以降低組織資產遭未經授權或非蓄意修改或誤用之機會。

（三）與權責機關之聯繫

本署對於處理資訊安全事件已建立標準處理程序，包含各單位通報窗口的聯繫，以確保在緊急事件發生時，能夠根據事件的情況通報適當的單位。

（四）與特殊關注方之聯繫

資訊人員不定期向委外維護廠商提出諮詢，面對資訊安全事件可能有法律或安全疑慮時，本署已建立與相關權責機關聯繫的管道。

（五）專案管理之資訊安全

如遇重要資訊安全相關專案(例：重要網路設備異動、重要設備系統異動、重大應用系統異動…)時，依採購作業要求，必要時召開專案會議，針對該專案進行時可能的資訊安全風險進行分析評估。

（六）行動裝置及遠距工作

建立使用行動式電腦設備及遠距工作防護措施，以防止未經授權之存取行為或低失竊之風險，以達有效之安全管理。

三、 人員安全管理及教育訓練

（一）人員安全管理

1. 本署進用人員之安全評估由人事室負責，如其工作職責須使用處理敏感性、機密性資訊的科技設施，或須處理機密性及敏感性資訊者，經適當的安全評估程序。
2. 本署新進人員於報到時，需依照本署人事室規定填寫到職單，並簽署保密協定。保密協定涵蓋期間包括從業期間與離職後，均有保密之責任，任何因未遵守本資訊安全管理規範導致之資訊安全意外事件將嚴格懲處。
3. 本署各委外開發維護之廠商人員，必須簽署保密協定及切結遵守本資訊安全管理規範之規範。
4. 本署同仁離職或調任其他單位時，須依照人事室規定填寫離職單，並由本署監資處撤銷帳號核章後，始完成離職程序。
5. 網路使用者如因職務異動而成為非授權使用者時，

相關單位主動通知網路系統管理人員撤銷該使用者帳號。

（二）人員教育訓練

1. 本署新進人員施以適當的系統操作訓練，避免使用者不當之操作。
2. 新系統上線時，對其作業人員、維護人員及網路管理人員施以適當的教育訓練。
3. 每年度對署內同仁辦理資訊安全管理課程訓練，提升其危機意識與資訊安全觀念。課程中必須給予完整之軟體著作權與版權觀念，嚴禁非法使用軟體，而自由軟體(freeware)與共享軟體(shareware)之安裝使用亦必須詳細了解其版權宣告並遵守。
4. 每年度針對署內資訊從業人員辦理資訊安全管理及危機處理防護課程訓練。
5. 參與本署資訊系統開發維護之委外廠商人員，避免開發之軟體帶有易受攻擊之程式碼。
6. 相關內容及表單請參考資安教育訓練管理流程。

四、 資訊資產之安全管理

（一）資訊設備安全管理

1. 本署各項資訊設備除依照相關審計法規財產管理外，各單位自行負責設備之安全，移出本署時經權責單位主管核定始得放行。
2. 本署各項資訊設備報廢時，除依相關財產減損規定辦理外，經本署監資處核定其堪用狀況後始得辦理報廢。
3. 本署同仁如發現有不明人士，未經許可擅接網路之情事，立即通知政風室及本署監資處處理，以掌握本署整體資訊設備之安全。
4. 重要之資訊資產必須上鎖且保存於合於「實體及環境安全管理」中規範之電腦機房安全空間。
5. 相關內容與表單請參考資訊安全風險管理流程、資訊資產風險評鑑作業說明書及資訊分級作業說明書。

（二）機密或敏感資訊之安全管理

機密性或敏感性的資料，不得存放於對外開放的資訊系統中。

五、 系統存取控制

（一）機密性／敏感性系統之作業管控

1. 對機密或敏感性的系統，宜建置獨立的或專屬的電腦作業環境。
2. 應用系統是否屬於機密或敏感性由系統負責單位決定。
3. 機密或敏感性的應用系統須分享相關資源時，經系統負責單位主管核可。

（二）使用者存取管理

1. 本署新進人員及委外服務人員，由本署監資處核發帳號後，啟用電腦系統。帳號及通行碼嚴格禁止交付他人，職務代理時須建立代理帳號，亦不可於電話中告知系統維護人員。
2. 網路使用〔就應用系統維護人員所提之存取權限檢討與評估，提出具體改善建議。

（三）系統存取之責任

1. 人員因故離開座位中斷作業時，必須簽退系統或使用畫面鎖定保護，防止帳號被盜用或資料被竊取。下班或公出離開辦公室前，必須關閉電腦設備並將桌面收拾乾淨，避免有心人士竊取機密資料或侵入系統。
2. 同仁宜保持高度之警戒心，防範不法人士以社交工程方法(Social Engineering)獲取帳號及通行碼入侵。並具備高度之危機意識，如有發現疑似系統安全危機時，迅速通知本署資通安全處理小組人員。
3. 應用系統維護人員之責任：
   (1) 使用者具善盡保護個人密碼之責任;如屬於群組軟體之使用者，確保工作群組的密碼，僅限群組成員使用。
   (2) 密碼之交付應由系統維護人員親自或以安全之

文書方式交付給使用者，避免經由第三者，或是以未受保護的電子郵遞等電子方式交付，並確認使用者是否收到密碼。

(3) 自動化登入系統之密碼，不宜存放在巨集或是功能鍵中。

（四）網路系統之存取控制

網路使用者遵守本署之網路安全規定，於授權範圍內存取網路資源，不得以任何方式竊取他人之登入帳號、密碼，不得使用任何軟體、設備竊聽網路上之通訊，不得使用任何手段干擾或妨害網路之正常運作，不得嘗試入侵防火牆主機，亦不得於本署網路上儲存、建置或傳播色情文字、圖片、影像、聲音等資訊。如有違反以上情事，移送政風室依相關法規查處。

（五）電腦系統之存取控制

系統公用程式需進行安全管控，其機制如下：

1. 嚴格限制及控制電腦公用程式之使用。
2. 設定使用者密碼以保護系統公用程式。
3. 將系統公用程式與應用系統分離。
4. 將有權使用系統公用程式的人數限制到最小的數目。
5. 移除非必要的公用程式及系統軟體。

（六）應用系統之存取控制

1. 應依資訊存取規定，配賦應用系統使用人員與業務需求相稱的資料存取及應用系統使用權限。
2. 資訊存取的控制機制如下：
   (1) 以選單方式控制使用者僅能使用系統的部分功能。
   (2) 適當的編輯作業手冊，限制使用者僅能獲知或取得授權範圍內的資料。
   (3) 控制使用者存取系統的能力（例如限定使用者僅能執行唯讀、寫入、刪除或執行等功能）。
   (4) 處理敏感性資訊的應用系統，系統輸出的資料，僅限於與使用目的有關者。

3. 有關應用系統之使用，請參考電腦軟體管理作業說明書。

（七）系統存取之應用與監督

1. 應用系統維護人員宜建立及製作例外事件與資訊安全事項的稽核記錄，以作為日後調查及監督之用。
2. 定期校正電腦系統作業時間，以維持系統稽核紀錄的正確性及可信度，俾作為事後法律上或是紀律處理上的重要依據。
3. 建立系統使用情形之監督程序，確保使用者只能執行授權範圍內的事項。
4. 應用系統於正式上線後,由該應用系統發展單位(委外者則為原委託單位）進行系統存取安全的風險評估，並由本署監資處協助提供相關意見。
5. 系統使用之監督作業，由應用系統維護人員依風險評估結果，定期建立監督紀錄作為日後稽核之用。

（八）機關外部人員存取資訊之安全管理

1. 對機關外部提供資料查詢或檔案傳輸服務，需評估風險，並簽訂正式的契約或協定以規範連線單位需遵守之規定及限定作業範圍與服務內容後始得提供服務。
2. 對於機關外部存取之第三者風險評估，宜考量下列事項：
   (1)第三者需要存取的資訊類型及資訊的價值等。
   (2)第三者採行的資訊安全措施及安全保護水準。
   (3)第三者之存取對本署資訊架構可能產生的安全風險及影響。

六、 密碼學管理

（一）郵件系統使用 SSL 方式進行加密處理。

（二）機敏性資料進行網路交換與儲存時依資料機敏性，考量加密處理控制。

七、 實體及環境安全管理

（一）電腦機房安全管理

1. 電腦機房分為終端作業室、電腦主機房、電力機房及網路管理室等區域由本署監資處負責管理，每月排定機房管理人員輪值表，呈處長核定後實施。
2. 相關內容與表單請參考辦公室安全管理作業說明書及電腦機房管理作業手冊。

（二）實體設備之採購、租借與維護安全管理

1. 本署正式之微軟網域名稱為 EPAIS，新購置、升級或新安裝建置之微軟平台系統均加入此網域，以便監控整體網路安全。
2. 新建置或安裝之軟體，安裝完成後立即更新廠商預設之密碼。

（三）實體設備及環境之安全管理

1. 電腦主機系統及其相關儲存與網路連結設備必須安置於設有安全門禁管制（磁卡、IC 卡、電子密碼鎖或其他保護裝置）之專屬機房，對於人員之進出必須嚴格控管並填寫於機房日誌。電腦機房須具備溫度偵測裝置與警鈴警示，並設置滅火裝置，防火設備定期檢查與更新。
2. 電腦主機系統及其相關儲存與網路連結設備必須使用穩壓與不斷電(Uninterruptible Power Supply)系統供應電力，以避免電壓不穩定或瞬間斷電造成損害。
3. 機房內禁止抽煙、飲用食物及攜入未經核准之電器或物品。
4. 網路連結設備必須嚴格之管控，集線器之各插孔必須清楚標示連結之目的地。
5. 如發現有不明人士，未經許可擅接網路之情事，立即通知政風室及本署監資處處理，以掌握本署整體資訊設備之安全。
6. 設備之搬遷必須嚴格管控與授權，被授權之搬遷人員必須負責遷移設備之使用安全與內存系統資料安全。

（四）媒體、文件安全管理

1. 涉及機密性或敏感性之相關媒體、文件由業務單位指定專人設置保管箱列冊保管，媒體須以牛皮紙袋密封加蓋騎縫章，其傳遞與與使用均須獲得單位主管授權始得使用。
2. 系統文件妥善保管，使用時於管理紀錄本登錄。如係委外操作之系統，於合約規範於契約解除時歸還本署。
3. 每年定期檢討機密性／敏感性資料，並專案簽報銷毀，並指定專人監督辦理。報廢之設備執行儲存媒體重新格式化(format)，移除相關作業軟體、資料及具有版權之系統軟體；報廢之磁帶、磁碟或光碟片等媒體進行實體銷毀；含有機密性資料之書面文件，使用碎紙機予以銷毀。

八、 電腦系統安全管理

（一）電腦系統作業程序及責任

1. 電腦主機所規劃之磁碟儲存空間，實體區分為系統磁碟與資料磁碟。所安裝之作業系統，安裝於系統磁碟區。
2. 實體硬碟採用 RAID 方式規劃。
3. 各電腦系統負責人，訂定電腦系統作業手冊，並以書面、電子或其他方式載明之，以確保員工正確及安全地操作及使用電腦，並以其作為系統發展、維護及測試作業的依據。
4. 電腦系統作業手冊載明執行電腦作業的詳細規定：
   (1) 如何正確地處理資料檔案。
   (2) 電腦系統作業時程的需求，包括與其他系統的相互關係、作業啟動的最早時間及作業結束的最晚時間。
   (3) 系統當機或發生錯誤之處理規定及回復正常作業之程序，以及作業之限制。
   (4) 遭遇非預期的電腦系統作業技術問題時，與支援人員聯繫之方式。
   (5) 資料輸出處理的特別規定，例如：使用特別的

文具，或是對機密資料輸出之管理、電腦當機或作業錯誤時，輸出資訊之安全處理規定等。

(6) 電腦及網路之日常管理作業，例如：開關機程序、資料備援、設備維護、電腦機房之安全管理；電腦系統作業手冊視為正式文件，作業程序的更改必須經權責單位核准。

5. 電腦稽核軌跡及相關的證據，以適當的方法保護，作為問題研析及判斷是否違反契約或資訊安全規範的證據與協商補償之依據。
6. 為降低因人為疏忽或故意，導致資料或系統遭不法或不當之使用，在人力資源許可條件下，儘可能將人員依業務及功能之不同區分角色，如：網路管理、系統行政、系統發展維護、變更管理、安全管理、安全稽核及作業人員。

7. 相關內容與表單請參考辦公室安全管理作業說明書。

（二）電腦病毒及惡意軟體之防範

1. 病毒防護軟體由本署監資處統一進行定期規劃評估與建置安裝。
2. 本署同仁須使用具合法版權軟體，避免上網下載來路不明之軟體。
3. 相關內容與表單請參考本署員工使用資訊設備及資料安全管理作業說明書。

（三）作業權限與帳號管理

1. 核發使用者帳號、密碼前，查核使用者是否已取得使用資訊系統之正式授權，及其授權之程度是否與業務目的相對稱。在未完成正式授權前，不得對該使用者提供存取服務。
2. 網路系統管理人員及應用系統維護人員定期檢查及撤銷閒置不用的帳號，並不得將其重新配給其他的使用者。
3. 完善保管應用系統使用人員之註冊資料及授權紀錄，以備日後查考。
4. 使用者帳號名稱不宜帶有足以辨識使用者權限的資

訊。

5. 管控應用系統之特別權限，視個別執行業務之需求，逐項考量賦予使用者系統特別權限之存取。
6. 應用系統設計使用者帳號、密碼時遵循以下之原則：
   (1)要求使用者必須使用密碼，以釐清使用責任。
   (2)設計於使用者第一次登入時，強制更改臨時性密碼之功能，並要求使用者定期修改密碼。
   (3)設計使用者自行選擇及更改密碼之功能，並具備弱密碼檢核排除功能。
   (4)應用系統登入程序中，不顯示使用者密碼資料。
   (5)使用之密碼必須至少 12 個字元，密碼組成須有英文大寫、英文小寫、數字、特殊符號等 4 種中之 3 種所組成但不包含帳號。
7. 相關內容與表單請參照使用者註冊管理流程。

（四）個人隱私之保護

1. 資訊系統處理個人隱私資料時，依據「個人資料保護法」相關規定，審慎處理個人資料，非公務用途嚴禁調閱使用。
2. 相關內容與表單請參照本署員工使用資訊設備及資料安全管理作業說明書。

（五）系統登入安全管理

1. 系統登入程序須於使用者完成登入資料輸入後，始開始查驗登入資訊的正確性，登入失敗時，系統不提供訊息告知使用者錯誤之資料項目。
2. 在既定時段內未有使用鍵盤或滑鼠(15 分鐘內未使用，視同使用者已停止使用電腦資源或離開座位)，進入螢幕保護並上鎖。

（六）資訊安全事件通報處理程序

1. 建立處理資訊安全事件之作業程序，並課予相關人員必要的責任，以便迅速有效處理資訊安全事件。
2. 資訊安全事件處理程序，至少含括電腦當機及中斷服務、業務資料不完整或資料不正確導致的作業錯誤、及機密性資料外洩。

3. 以審慎及正式的行政程序，處理資訊安全及電腦當機事件。作業程序包括下列事項：
   (1) 在最短的時間內，確認已回復正常作業的系統及安全控制系統是否完整及正確。
   (2) 向管理階層報告緊急處理情形，並對資訊安全事件詳加檢討評估，以找出原因及檢討改正。
   (3) 限定只有被授權的人員，才可使用已回復正常作業的系統及資料。
   (4) 緊急處理的各項行動，詳細記載，以備日後查考。
4. 相關內容與表單請參考資訊安全事件管理流程、服務持續性管理流程、矯正與改善流程。

（七）日常作業之安全管理

1. 網路系統管理人員未經權責主管人員許可，不得閱覽、增加、刪除或修改其他網路使用者之私人檔案。如發現有可疑之網路安全情事（如病毒或特洛依木馬等），得經請示本署監資處處長核可後，使用適當的工具追蹤檢查相關檔案，採取必要處理措施，事後再行知會該檔案擁有者。如確定為感染病毒，為避免病毒擴散，得經主管科長同意後，逕行掃毒或隔離檔案再行知會該檔案擁有者。
2. 網路系統管理人員登入主機系統時，保留登出入系統紀錄，不得新增、刪除或修改稽核資料檔案，避免於安全事件發生後造成追蹤查詢之困擾。
3. 網路系統、主機系統需保有登出入系統紀錄與異常狀況之紀錄，以利日後追查分析使用。
4. 各主機如有異常狀況，由該應用系統維護人員儘速排除，如各應用系統維護人員休假，由指定職務代理人員待命，以確保各主機之正常運作。
5. 各應用系統維護人員需提交所需磁碟機容量、各項軟體名稱、系統操作及備份程序等，交予網路系統管理人員彙整管理。
6. 應用系統維護人員宜每日注意觀察系統資源使用狀

況及應用系統使用情形，有異常狀況時即時反應。

7. 機房管理人員執行電腦機房環境監測，每日填寫機房日誌，定期紀錄溫溼度，上下班需注意照明等相關電器設備之開關，並特別注意冷氣及除濕機運轉狀況，於必要時進行相關耗材清理更換，每季工作日誌呈本署監資處處長核定。
8. 相關內容與表單請參考文件與紀錄管理流程。
9. 有關電腦軟體的使用規則請參考電腦軟體管理作業說明書。
10. 有關電腦軟體智慧財產權之查核請參考電腦軟體智慧財產權查核管理流程。
11. 有關機房管理作業請參照電腦機房管理作業手冊。

（八）資料及媒體交換安全管理

1. 公文電子資料交換依行政院頒訂之「機關公文電子交換作業辦法」及相關規定辦理。
2. 本署及所屬機關公文電子資料交換，收文後需標明電子公文，並依收文處理作業程序辦理。
3. 本署與行政院公文電子資料交換，須採用認證與加解密之安全管制措施，始可進行公文收發。
4. 署外機關如因業務需求，必須透過網路與本署交換資料，經簽會本署監資處，奉核定後，採以下方式擇一辦理：
   (1) 透過網際網路(Internet)與本署連線作業者，依申請之連線項目由本署監資處事先於防火牆設定存取規則，以過濾網路之傳輸作業。
   (2) 透過獨立之網路路由與本署特定主機連線作業者，為網路安全考量，此主機避免與署內網路連線。
   (3) 使用磁帶、磁碟或光碟片等媒體進行資料交換時，宜有妥善之包裝與安全措施，以防止運作過程中受到損害、破壞或未經授權之取用。
5. 進行媒體資料交換時，需透過安全評估程序慎選安全可信賴之廠商或人員，並報請各處室主管同意。

6.機密性之資料若需使用傳真設備傳送時，傳真設備必須有保護之措施，避免明文資料外洩。

7.相關內容與表單請參考文件與紀錄管理流程。

（九）系統稽核

1. 應用系統維護人員對系統進行查核之稽核需求及實際稽核作業，經權責單位主管同意始得為之，以免影響業務正常運作。
2. 應用系統維護人員定期執行稽核作業，稽核作業時的系統存取需留下記錄，以備日後查考。
3. 系統稽核考量事項如下：
   (1)稽核需求及查核範圍，經權責單位主管核定。
   (2)限定以唯讀方式存取軟體及資料。
   (3)不能以唯讀方式進行系統存取時，獨立複製另外一份系統檔案供稽核作業之用，且稽核作業完成後，立即消除檔案。
   (4)執行查核所需的技術資源，於事前明確界定，並準備妥當。
   (5)執行特別及例外的查核，於事前明確界定需求及範圍。
4. 系統稽核紀錄，包括下列事項：
   (1)使用者帳號控管狀況。
   (2)檢查系統登入的模式，確定使用者帳號是否有不正常使用或是被重新使用的情形。
   (3)查核系統存取特別權限的帳號使用情形及配置情形。
   (4)系統所需硬碟空間需求及使用情形。
   (5)系統存取失敗情形。
   (6)追蹤特定的系統交易處理事項。
   (7)敏感性資源的使用情形。
   (8)例外事件及資訊安全事項的稽核紀錄。
5. 保護系統稽核工具（例如軟體及資料檔案）以防止誤用或被破解，並與發展中或是實作的系統分隔，且存放在安全的地點。

九、 通訊安全管理

（一）網路安全規劃與管理

1. 為維持本署網路能正常持續地運作，主要網路設備宜考慮或準備備援設備即時替換。
2. 本署網路安全管理人員由本署監資處指派合格且適任之人員擔任。
3. 本署內部網路、DMZ 網段與外部網路之連線存取均需透過防火牆之安全管控，防火牆之運作維護由本署監資處指派專人負責。
4. 聯外網路宜安裝入侵偵測系統，網路系統管理人員須隨時監控非法入侵之犯罪行為，並收集入侵證據以作為法律控訴之證物。
5. 如需新增或遷移資訊系統主機時，應用系統維護人員，審度該系統之使用者性質、作業特性、作業公開程度及資料更新機制等因素，並會簽本署監資處後，會同本署監資處人員安裝至適當網段。資訊系統廢止時，亦需知會本署監資處註銷紀錄。
6. 本署及附屬單位同仁如因業務特殊需求，需於防火牆對外開放特殊服務(如遠端登入 Telnet 或檔案傳輸 FTP 等)，在不影響本署網路安全條件下(如採用 VPN tunnel 技術)，經會簽本署監資處並奉核可後，由本署監資處設定開放權限。
7. 本署個人電腦需透過網卡位置(MAC Address)之比對，方可取得 IP 位址。
8. 本署同仁利用微軟視窗作業系統之檔案分享功能提供他人存取檔案時，僅針對必要對象開放使用權限，避免將權限完全開放。
9. 相關內容與表單請參考網路通訊管理作業說明書、設備在外地使用的安全管理作業說明書。

（二）電子郵件安全管理

1. 本署之網路使用者禁止以電子郵件騷擾他人、發送匿名郵件、偽造他人名義發送郵件或惡意發送大量不當郵件，如有違反之情事，由本署政風室查處，

必要時由本署監資處提供技術支援。

2. 機密之公文及資料，不得以電子郵件傳遞。
3. 為防範假冒機關員工名義發送電子郵件，以電子郵件發送重要訊息時宜考慮以電子簽章簽發，以達到身分辨識及不可否認的目的。
4. 收到電子郵件時須先經過郵件掃毒軟體掃描，確保資料附件並未夾帶惡意程式後，再轉送至電子郵件伺服器供使用者讀取。
5. 關閉電子郵件軟體對電子郵件「自動預覽」與「自動開啟下一封」之功能，關閉或限制電子郵件軟體執行 ActiveX、Java applets、Active Scripting 之功能。
6. 不開啟不明來源寄件者或信件標題異常之電子郵件，不開啟用途不明之附件，不開啟廣告信或垃圾信件，不點選電子郵件內容中不明連結。
7. 電子郵件寄件前請檢查收件者是否正確，避免誤寄敏感或機密資訊給不適當的收件者。

（三）聯外網路安全管理

1. 除開放公眾瀏覽與下載之系統外，本署提供外部連結之系統均需建立個別之安全機制（至少需具備基本的使用者登入認證機制），以保障網路的安全性。
2. 本署外部網路（含 DMZ 區）的電腦系統與網路設備，需與內部網路連線作業時，檢附該外部設備之相關文件（如網路協定、提供服務項目及特殊需求等）會簽本署監資處並奉核可後始得進行連線作業，連線作業時，遵守本署網路通訊管理作業說明書辦理。
3. 署外網路欲與本署 DMZ 區或內部網路連線時，需由業務承辦單位填寫申請表，經單位主管核可後，會簽本署監資處承辦科於申請時段內開放防火牆連結設定。

（四）網路安全稽核

1. 本署網路安全稽核工作統一由本署監資處指派專人負責。

2. 網路系統管理人員需每日不定時檢視系統登錄紀錄，並定期產生報表，簽報本署監資處處長核閱。如發現異常狀況，立即通報單位主管，情節重大時，專案簽報並知會政風室。
3. 本署監資處對署內網路建立警示系統，於特定網路安全事件發生時，能立即產生警示訊號通知網路系統管理人員，俾採取有效的防護措施，降低安全事件所產生的危害。

十、 系統發展及維護之安全管理

（一）委外廠商安全管理

1. 資訊服務委外時必須慎選口碑良好與高品質之廠商，訂定符合效能需求及系統安全規範之合約書，並制定違約罰責。
2. 應用系統委外維護運作合約，必須訂定合約期間工作內容與產出之著作權歸屬，並要求廠商與其工作人員簽訂相等之合約。
3. 廠商承包各單位委外設計操作之資訊系統時，凡涉及系統規劃、設計、執行、操作等相關作業之委外服務人員，要求廠商之相關人員簽署保密協定及遵守本管理規範之同意書。
4. 各單位委外計畫若涉及資訊系統設計操作及資訊硬體設備者，於簽核時需知會本署監資處；本署監資處得就作業需求，提出可行性與適用性之資訊專業技術建議。
5. 各單位委外設計操作之資訊系統計畫中，凡屬與公文機密、個人及事業單位權益相關之資料，留在機關內部處理，其它資料若需由承商攜回公司內部處理者，需簽奉核可。
6. 各單位委外設計操作之資訊系統及相關成果，於交付本署完成驗收後即屬本署資產，非經本署同意，承商不得使用。
7. 各單位委外設計操作資訊系統時，需檢討評估委外計畫中各項軟、硬設備及各項作業執行之安全性，

以確保其符合本署的安全標準。

8. 承商如發現有違反資訊安全需立即處理，並同時通報本署。承商需將違反資訊系統安全事件之處理結果完整紀錄，於限期內提交各單位。各單位據此進行查核評估，必要時可實地了解或實施專案稽核，並做成查核報告,簽會政風室及本署監資處後陳核。

（二）系統發展及維護安全管理

1. 系統開發、維護及測試環境必須使用另行建置之專用伺服器，不可與實際運作中之伺服器共用。開發維護伺服器只允許系統開發維護人員登入使用，並須謹慎維護內存程式碼與資料之安全性。進行測試時，宜保護測試資料，避免以機敏資訊及個人隱私資料進行測試；如必要應用，需經授權並考慮將測試資料事前編排、移除或將可辨識之個人資料或機敏訊息修改為無法辨識或將資料予以後始可進行存取。
2. 應用系統之各項系統文件，應用系統維護人員，負責建置並與保管。
3. 應用系統軟體之版本宜管控，如需更新版本時，應用系統維護人員宜考量各版本之系統文件，詳細記錄使用的明確時間，並保存支援應用程式軟體、作業控制、資料定義及操作程序等資訊，本署監資處得視需要，就各應用系統之更新狀況，提出具體評估建議。
4. 有關應用系統之開發、營運及維護請參照資訊系統管理作業說明書。

（三）需求變更管理

1. 本署監資處每年視人力及業務狀況辦理資訊系統之更新作業，如屬業務緊急重大需求，簽奉核可由本署監資處專案辦理。。
2. 因應臨時業務需求，需求單位依據「本署員工使用資訊設備及資料安全管理作業說明書」填具「資訊作業需求單」,由該單位主管核可後向監資處申請，

監資處得視人力、技術及成本考量，提出可行性方案及意見（或辦理情形）回覆原需求單位。

十一、供應商關係管理

（一）供應商關係的資訊安全政策

委外服務交付協議中之安全管控、委外服務之定義、委外廠商之監控審查及服務變更管理。

（二）供應商協議內的安全處理

本署在資訊服務委外給第三方時，於採購合約中明定與第三方服務的範圍與內容，並載明雙方之權利與義務。

（三）ICT 供應鏈

本署部份資訊施備或系統委外進行建置或維護時，宜進行適當的委外資訊與通訊技術服務及產品供應鏈廠商控制機制，以確保受託廠商之設備或服務供應過程中之資訊安全。

（四）供應商服務的監視與審查

委外廠商進行資訊設施與其有關之應用系統維護後，設備負責人會依採購法規定，針對其服務結果進行驗收。

（五）供應商服務變更的管理

供應商服務如變動時，需考量其變動所可能造成的風險，進行必要性之評估及因應。

十二、資訊安全事故管理

（一）責任與程序

本署針對相關人員的權責給予適當的界定，在發生資訊安全事件時，問題得到迅速的解決方案。

（二）通報資訊安全事件

針對資訊安全事件，建立通報系統，分類資訊安全事件的等級，在資訊安全事件發生時，通報適當的層級。

（三）通報資訊安全弱點

根據風險評估的結果教育使用者在注意到系統或服務有任何明顯或可疑的安全弱點或威脅時逕行通報。

（四）資訊安全事件的評鑑、決定及回應

本署針對相關人員的權責給予適當的界定，在發生資訊

安全事件時，問題得到迅速的解決方案。

（五）從資訊安全事故中學習

本署在資訊安全事件發生後，記錄資訊安全事件處理的過程，並且視資訊安全事件的影響程度進行定期與不定期的會議或訓練，討論可能的改善機會，並且運用適當的手法進行矯正、改善措施。

（六）證據的收集

在涉及法律行動(民事或刑事)的資訊安全事故後，保存或呈現證據。

十三、業務永續運作計畫之規劃及管理

（一）備援／備份作業之規劃與演練

1. 各單位開發之資訊系統於上線運作後，對該系統之原始程式碼進行備份 2 份，1 份自行保管，另 1 份繳交本署監資處統一進行異地儲存保管。
2. 資訊系統設備故障或損壞時，宜即時執行系統備援回復作業，維持業務之持續運作。
3. 資訊系統作業紀錄每半年由各應用系統維護人員備份、清理。
4. 個人電腦中之重要資料備份，由同仁自行進行備份，並選擇乾燥密閉之環境保管。
5. 每年進行備援設備、回復作業程式及機制之測試演練。
6. 每日進行系統日誌之備份，以防止日誌資料遭受破壞。

（二）業務永續運作規劃

1. 每年進行資訊安全風險評估，其結果作為本署「資訊安全政策」及「資訊安全管理規範」修訂參考。
2. 使用弱點掃瞄之系統安全檢測軟體，定期進行系統安全檢核與弱點掃瞄工作，減少非法人士入侵之機會，並製作系統安全檢查報告(SMSR Reports)。
3. 依據服務持續性管理流程，訂定資訊系統復原計畫，以應付危機處理之需求，並演練以保障其有效可行性。

（三） 突發事件應變依資訊安全事件管理流程與服務持續性管理流程處理。

任何突發之安全事件或造成運作中斷之事件，本署同仁不得隨意接受新聞媒體採訪發言，須依部內行政流程簽核後，統一發言。

十四、遵循性控制管理

（一） 適用於本署資訊安全管理制度相關的法律、法規與契約。

（二） 若法律、法規及相關條款或契約、保密書或切結書的涵意不清楚時，宜與相關單位諮詢或請其解釋。

伍、 保全處理程序

一、 網路入侵處理

（一）發現網路入侵之處理步驟

網路使用者發現網路入侵之情事時需立即通知本署監資處，本署監資處接獲通知後，採取下述任一適當措施以防止災害繼續擴大：

1. 當確定本署網路安全被突破時，被入侵之應用系統暫時設定為「拒絕任何存取」，並切斷入侵者的網路連接，如無法切斷則必須關閉網路防火牆。
2. 如入侵者已被本署監資處嚴密監控，在不危害內部網路安全的前題下，得適度有條件地允許入侵者存取動作，以利追查入侵者。一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。

（二）網路入侵之追蹤調查

1. 檢視記錄檔中是否有不尋常的來源位置或不尋常的操作動作。檢查登入時間、程序的執行記錄以及系統日誌所做的記錄等，以防止入侵者修改記錄檔來隱藏行蹤。
2. 對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並聯合相關單位(如 Hinet 網路服務公司等)追蹤入侵者。
3. 當檢查機器是否被入侵時，必須檢查區域網路上的機器。如一台機器被入侵，同一網段的其它機器也有可能已被入侵；或是入侵者利用其它機器為窗口來入侵本署網路。

（三）網路入侵的事後處理

1. 入侵者之行為若觸犯法律規定，構成犯罪事實，由政風室查處，並立即告知檢調單位，請其處理入侵者之犯罪事實調查。
2. 本署監資處檢討網路安全措施及修正防火牆的設定，尋求適當之解決辦法，以防禦類似的入侵與攻擊。

3. 保留記錄供資訊安全稽核小組執行稽核。

二、 安全稽核流程與獎懲措施

（一）年度稽核計畫

1. 資訊安全稽核小組依據本作業規範及配合上級主管機關所辦理之外部稽核制度，於每年選擇年度重點，訂定本署年度稽核計畫，並落實執行資訊安全稽核工作，以反映政府資訊安全管理政策、法令、技術及機關業務之最新狀況，並確保本署資訊安全實務作業的可行性及有效性。
2. 年度稽核計畫之年度重點內至少包括本署機房安全管理維護、網路安全管理維護、本署三個單位以上共同使用之應用系統安全管理維護、利用網際網路開放外界連線作業之資訊系統安全管理維護、本署委外服務之各項資訊系統安全管理維護、本年度休離職人員管理之各項資訊系統或資料庫、本年度新開發之資訊系統安全管理維護、及上年度專案稽核計畫結果列入待改進之項目。稽核內容則視本規範各相關項目內容及精神，查核是否均按規定辦理並完整記錄及保留需填寫之各項紀錄表。
3. 年度內定期進行之資訊安全稽核結果，除特殊原因得簽奉核可不公開外，彙整相關單位之優缺點及綜合改進建議，簽奉核可後提供相關單位改進，本署各單位及人員不得將相關資訊安全稽核結果資料洩漏給不相關之第三者。
4. 為求資訊安全稽核工作之客觀性及有效性，必要時得運用可行之工具程式等輔助進行稽核，或委請署外專家學者，協助本署進行資訊安全稽核工作。
5. 相關內容與表單請參考內部稽核流程。

（二）專案稽核計畫

1. 資訊安全稽核小組為因應突發性、專案性或特殊性之資訊安全稽核需要，得不定期針對特定目的之項目、單位或人員進行資訊安全專案稽核工作，以確保本署資訊安全實務作業之有效性。

2. 專案稽核計畫之重點以因應特殊目的為主，稽核內容則審視稽核項目是否已按規定辦理,且安全無虞。
3. 每次專案稽核結果，需檢討各項優缺點及綜合改進建議，簽奉核可後提供相關單位改進，並列入年度資訊安全考核獎懲辦理，及下年度年度稽核計畫追蹤。

陸、 附則

一、 獎懲措施

(一)年度稽核及專案稽核之結果，由本署監資處會同政風室進行檢討，對於執行資訊安全作業工作績優者或有缺失部分，擬議予以獎勵或懲處。

(二)本署員工違反本規範之作業規定，情節重大者，依公務人員考績法及環境保護專業人員獎懲標準表辦理懲處。委外管理人員及委外服務人員違反本規範之作業規定，應通知受委託承商更換相關人員，並得視情節依合約規定要求承商賠償本署之損失。

二、 本署所屬機關未訂定資訊安全管理規範者得適用本規範。

三、 本規範未訂定之事項得依行政院所頒訂之「行政院所屬各機關資訊安全管理要點」及相關規定辦理。