中央研究院資通安全管理規範實施要點

中華民國 109 年 12 月 28 日院長核定
中華民國 111 年 4 月 1 日資訊服務字第 1111500201 號函修正
中華民國 112 年 5 月 8 日資訊服務字第 1121500480 號函修正
中華民國 113 年 4 月 19 日資訊服務字第 1131500367 號函修正
中華民國 114 年 5 月 9 日資訊服務字第 1141500452 號函修正
中華民國 114 年 10 月 2 日資訊服務字第 1141501095 號函修正
中華民國 115 年 5 月 28 日資訊服務字第 1151500498 號函修正

第一章　總則

一、本要點依中央研究院資通安全暨個人資料保護政策及規範第五點訂定之。

二、本院各研究所、研究所籌備處、研究中心(以下簡稱各所中心)得依本要點另訂定作業程序。

三、本院資通安全推動組織如下：

本院資通安全暨個人資料保護委員會：推動全院性資通安全管理事宜，並審議相關事項。

單位資安小組：各單位應成立單位內資安組織，負責推行資通安全相關事宜，且應依中央研究院資通安全暨個人資料保護政策及規範第六點規定，指派單位資通安全主管（即單位資安長）與資通安全連絡人，並將名單送院備查，異動時亦同。

院本部資安小組：由資訊服務處擔任。

四、本要點用詞，定義如下：

(一) 電腦機房：包含資訊機房、通訊機房、監控室、媒體儲存區及附屬機電室。

(二) 電腦系統：包含本院網路設備、群組計算設備、伺服主機、資料儲存設備、附設或嵌入於儀器之電腦設備、物聯網設備等，及其作業系統與應用系統。

(三) 敏感性電子資料：係指除公務機密外，涉及單位或個人之權益或隱私，依規定應限制公開或不予提供者。

(四) 重大弱點：具可被利用入侵系統，致造成服務中斷或機密資料洩漏風險之弱點。

第二章　人員管理暨資通安全訓練

五、本院人員應注意下列資通安全事項：

(一) 依相關法規負保守公務機密之義務。

(二) 職務為可接觸機密性或敏感性資料者，應於任務指派前閱讀相關保密條款，並簽名以示認知該職務之資通安全規定。

(三) 重要應用系統之發展、維護、管理及操作之人員，應妥適分工，分散權責，並視需要建立管控機制，實施人員輪調，建立人力備援制度。

(四) 各級主管應督導所屬人員妥為辦理資通作業，以確保資通安全，防範不法及不當行為。

(五) 資通作業人員於離職或職務調動時應辦理資通資產交接或歸還，並應立即辦理權限異動或帳號移除。

六、本院應定期舉辦資通安全相關之教育訓練，促使同仁瞭解資通安全之重要性及各種可能的資通安全風險，以提高同仁資通安全意識，促其確實遵守資通安全規定。

七、本院人員應依資通安全管理法(以下簡稱資安法)及其子法規定，依其職務性質完成相關之資通安全訓練。

若未於當年度十二月一日前完成前項訓練要求，經本院通知後仍未完成，本院將限制其使用資訊服務處所提供之無線網路 AS_Secure、AI 助理、AI 逐字稿及 AI API 服務，待完成訓練要求後，始得恢復其原有服務使用權限。

另當年度曾接獲社交工程演練信件開啟通知後未完成相關教育訓練者，將比照前項限制辦理。

八、委外作業資通安全管理事項：

(一) 本點所稱委外作業，係指委託廠商辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務）；委託單位即指委託廠商辦理上揭受託業務之單位。

(二) 委託單位應依據資安法及資通安全管理法施行細則等規定，監督受託業務之資通安全維護情形。

(三) 委外契約或建議書徵求說明書應載明下列事項：

1.廠商應遵循之資通安全、保密條款及作業相關之法規要求。

2.各項資通安全控管要求，以明確告知委外廠商應遵循事項。

3.相關資通資產之機密性、完整性、可用性及法規性要求。

4.廠商應就辦理上揭受託業務之相關程序及環境之資通安全管理措施配合委託單位進行自評作業，自評結果送本院委託單位備查，本院得保留對委外廠商進行資通安全稽核之權利。

(四) 本院應於簽約後，提供委外廠商資通安全相關作業方式及規定。

(五) 委外廠商及其相關人員於契約期間出入本院辦公場所時，須佩戴識別證，以供人員安全控管及掌握。

(六) 委外廠商及其相關人員於非上班時間加班作業時，應事先取得相關單位同意，以利管控人員出入。

(七) 委外廠商駐點服務人員、實際參與履行契約人員及經常至本院各單位資訊部門洽公之業務人員，均應簽署保密切結書。

(八) 廠商維護資通系統，應以到場為原則，但遇下列情形者，可例外允許遠端維護，惟應加強防護及管理措施：

1.因疫情、地理限制、處理時效及專案特性（如：屬 7*24 小時提供服務者）、天災或事變等不可抗力因素者。

2.屬特殊狀況經核准者。

第三章　電腦機房安全管理

九、電腦機房(以下簡稱機房)之規劃、設計與建置應依下列原則辦理：

(一) 考量安全與最大之電力容量、空調散熱能力及地板承重。

(二) 室內建材須耐燃且符合國家標準。

(三) 供電設備如變壓器、不斷電系統、電池組等須有安全保護措施。

(四) 裝設無腐蝕性自動滅火設備。

(五) 裝設環境監測或監控設備。

另考量實際可行性，宜參考以下原則辦理：

(一) 機電室與機房其他部分間保留安全距離，並各自具獨立之空氣及水循環系統。

(二) 裝設監控空調水位、主電源斷電等之警示設備。

(三) 考慮不同冷却方式之備援空調設備。

十、機房內所裝置之電腦系統及相關設備，不應超出安全電力容量、空調散熱能力及地板承重；並嚴禁超載使用。

十一、機房內電腦機櫃、單獨系統及相關設備之間，應保留作業及散熱所需之足夠空間。

十二、機房應有門禁管制，防止未經授權者進出；機房進出管制應依下列原則辦理：

(一) 人員進出機房均須登記，非機房管理人員未經許可不得進入機房。

(二) 廠商維護人員進入機房，應由機房管理人員全程陪同。

(三) 不得攜帶非工作所需物品進入機房。

(四) 機房設備送修或修妥送回，均須登記。

十三、機房之日常作業應依下列原則辦理：

(一) 機房定期執行清潔作業。

(二) 機房設施定期保養，定期辦理安全防護演練。

(三) 機房內廢棄物儘速移除。

十四、機房值班人員應辦理下列事項：

(一) 機房門禁及進出管制。

(二) 機房重要設備與設施之監控，異常狀況之通報、聯繫及因應。

(三) 機房內、外電腦相關設備與設施之巡察。

(四) 機房實體環境安全之維護。

(五) 其他交辦之機房管理事項。

十五、機房各電腦系統及重要設備應指派專責人員，辦理下列事項：

(一) 定期監控系統或設備，確保正常運作。

(二) 系統或設備發生異常狀況時，應即到場、透過安全連線或通訊指導值班人員等方式予以處理；必要時通知維護廠商依約處理。

(三) 異常狀況及其處理情形應即登載於機房工作日誌。

(四) 其他交辦之系統或設備管理事項。

第四章　電腦系統安全管理

十六、電腦系統應與標準時鐘同步或定期對時，以確保系統時間之一致

性。

十七、安裝電腦作業系統應依下列原則辦理：

(一) 作業系統應僅安裝系統運作所需之套件，各套件應僅啟用所需之服務，如須使用遠端登入、網路芳鄰等服務，應加強資安防護及管理措施。

(二) 作業系統修補，如需連接網路以安裝系統修正檔時應先評估其風險。

(三) 作業系統安裝完成後，應即完整備份。

十八、安裝於電腦系統之程式，未能確認其功能與安全性者應先行測試，測試作業應依下列原則辦理：

(一) 不得於系統正式作業環境進行測試，測試電腦之網段應與正式作業網段適度區隔。

(二) 如委由廠商進行測試，應嚴格規定其範圍、權限及程序；並責成廠商提供測試報告，必要時要求廠商先行提交測試計畫。

十九、電腦系統上線時應建立組態資訊，包含軟硬體版本、型號、系統啟用服務及相關參數設定等，並持續維護。

二十、對運作中之電腦系統進行異動，包含系統升級、變更設定、安裝安全性修補程式及組態變更等，應依下列原則辦理：

(一) 異動前應先評估所需資源，包括軟硬體容量、效能、人員、時程及廠商支援等。

(二) 應評估對相關電腦系統、應用程式之相容性及對整體資通作業環境之影響，確保異動之內容符合需求，需要時得要求相關系統管理人員協助評估。

(三) 組態設定檔於變更前及變更後，均應匯出備份，並至少維持最近三個版本。

(四) 異動過程中應詳細記錄所遭遇之問題及解決方法。

(五) 異動前應進行備份及回復準備，避免無法復原造成電腦系統不可預期之損害。

二十一、各電腦系統應監控其硬體資源使用、作業系統、資料庫管理系統及網路服務等。

二十二、為強化電腦系統之安全防護，電腦系統除應定期更新安全性修補程式外，另應依下列原則辦理弱點修補：

(一) 接獲政府機關資安弱點通報或外部情資公告之弱點，應就受影響之電腦系統，安排期程落實修補。

(二) 資安健診、滲透測試、弱點掃描發現之前二高等級弱點應儘速修補並列冊追踪；其餘等級之弱點，經風險評估後認定風險為可接受者，得免予修補。

(三) 修補期限如下：

1.各級行政單位官方網站、涉及不公開之研究內容或機敏資訊之網站、使用動態網頁技術之網站，以及提供高效能運算服務之系統，於一週內完成修補作業或採取替代防護措施並保存相關紀錄備查。

2.非屬前點所列之網站、路由器、網路交換器、獨立功能之防火牆、獨立功能之虛擬私人網路、獨立功能之入侵防禦/偵測系統、獨立功能之網站應用程式防火牆、無線網路控制器及存取點等設備，於二週內完成修補作業或採取替代防護措施並保存相關紀錄備查。

3.其餘電腦系統於一個月內完成修補作業或採取替代防護措施並保存相關紀錄備查。

4.自行或委外開發之應用程式弱點，因需確認弱點修補方式，得延長修補期限二週。

(四) 前述前二高等級弱點因未修補而下架，嗣後因未通過弱點掃描逕行上架而發生資安事件情節重大者，本院將建請單位予以警告或懲處。

二十三、物聯網設備應遵守一般個人電腦防護原則，預設帳號及密碼應予變更。

二十四、物聯網設備應開啟即時線上韌體更新功能，若無即時線上韌體更新功能者，應定期更新韌體及執行弱點掃描，並進行弱點修補；若無法修補或更新，應訂定汰換期程。

二十五、電腦系統若必須放置於公共或開放區域，應確保設備受到適當

保護，以避免設備遭破壞或竊取等情事。

第五章　應用系統發展及維護安全管理

二十六、本章規定適用於本院自行或委外開發建置、維護之應用系統。

二十七、應用系統發展或維護前，應先評估其資通安全風險，包括對相關電腦系統之安全衝擊。

二十八、應用系統開發與維護之安全管理應涵蓋下列事項：

(一) 訂定安全運作環境，並嚴謹管理與設定，只釋出必要之最小存取權限。

(二) 訂定網路接取安全措施。

(三) 建立有效防止人為疏失、杜絕惡意入侵之安全控管機制。

(四) 具備完整伺服器端安全控管。

(五) 檢測安全弱點及漏洞，包括自行檢測及非發展者之檢測。

(六) 規範及限制廠商可存取之系統與資料範圍。

二十九、發展應用系統，應於規劃階段，即將下列資通安全需求納入考量：

(一) 管理者與使用者之權責。

(二) 使用者身分認證方法。

(三) 對系統及資料之存取控制。

(四) 所有資料項之屬性。

(五) 機密性及敏感性資料保護機制。

(六) 資料備份及系統故障後回復作業需求。

(七) 重要作業之系統紀錄。

(八) 其他需考量之資通安全控制措施。

前項安全需求應儘量轉化為系統功能，自動執行，其餘部分由人工控管，並訂定人工安全控管規範。

三十、應用系統之測試資料不應含有個人真實訊息、機密性或敏感性內容；若需使用真實資料進行測試時，應採行下列保護措施：

(一) 參與測試者對資料負保護及保密之責，非因測試需要，不得閱讀內容。

(二) 適用實際作業之存取控制措施，亦適用於測試作業。

(三) 測試完畢後，真實資料立即刪除。

三十一、應用系統於上線執行或版本異動前應先進行測試，測試作業應依下列原則辦理：

(一) 不得於系統正式作業環境進行測試。

(二) 如委由廠商進行測試，應嚴格規定其範圍、權限及程序；並責成廠商提供測試報告，必要時要求廠商先行提交測試計畫。

三十二、應用系統版本異動前應進行備份及回復準備，避免無法復原造成不可預期之損害，異動過程中應詳細記錄所遭遇之問題及解決方法。

三十三、基於委外開發之實際作業需要，得核發暫時之系統辨識及通行碼供廠商使用，使用完畢後應立即取消其使用權限。

三十四、本院對外服務網站之資安防護須遵守下列規定：

(一) 應提供符合至少 TLS 1.2 安全規定之加密連線方式。

(二) 應用系統設定檔、紀錄檔及備份檔禁止存放於公開網頁目錄中。

(三) 敏感性資料應以加密傳輸，進行加密連線或數位簽章時，不得使用已遭破解或具有高度風險之演算法。

(四) 不得與內部服務系統共用實體或虛擬伺服器。

三十五、資通系統上線前，應依資通安全責任等級分級辦法附表九所定資通系統防護需求分級原則完成資通系統分級，並依該辦法附表十所定資通系統防護基準執行控制措施。

三十六、各單位辦理前點依資通安全責任等級分級辦法附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，系統管理單位應擬定替代防護措施，經本院提報總統府同意並報請數位發展部備查後，得免執行該事項或控制措施。

第六章　應用系統存取控制管理

三十七、本院應用系統帳號、通行碼、使用權限及存取紀錄等，應依本章規定進行管理。

三十八、帳號新增及異動管理應依下列原則辦理：

(一) 帳號新增及異動須經申請，並經權責人員核可後，交由系統管理單位辦理，並保留紀錄。

(二) 帳號、通行碼之通知過程應有保護措施，防止被窺視竊取。

(三) 單一使用者於單一系統上僅能申請及持有單一個人帳號，因業務或特殊原因需使用兩個以上帳號，應提出申請。

(四) 帳號持有人個人資料如有變更時，應依規定更新；人員職務異動、留職停薪或離職時應依規定辦理帳號移交或註銷，未依規定辦理者，系統管理人員得逕行停止該帳號之使用。

(五) 不得共用帳號，以區分安全責任；但職務帳號得與職務代理人共同管理。

三十九、帳號持有人應遵守下列原則：

(一) 尊重他人隱私與使用權。

(二) 不得擅自使用他人帳號或修改他人檔案、資料或通行碼，亦不得置放或散布侵擾其他使用者之程式。

(三) 不得侵入未經授權使用之電腦系統。

(四) 不得傳送或散布具恐嚇性、暴力性或猥褻性之資料，或謾罵、侮辱他人等不當言論。

(五) 不得散布病毒、蠕蟲、木馬、後門等有害程式。

(六) 遵守智慧財產權有關規定，不得重製或散布侵害他人著作權之檔案。

(七) 不得寄送垃圾或廣告郵件。

(八) 不得有其他重大違規行為。

帳號持有人如有違反前項使用原則情事，系統管理人員視情節得為通知改善、縮減使用權限、停止使用或其他必要之處置。

四十、應用系統登入管理應依下列原則辦理：

(一) 宜設定可開放連線之時間或連線逾時自動登出之機制。

(二) 除帳號、通行碼外，應依業務需求考量是否採用其他適切之身分鑑別技術。

(三) 登入作業完成後，宜顯示前一次登入成功或失敗之時間或相

關訊息。

(四) 限制連續登入失敗次數之上限，登入失敗次數達上限者，應暫停該帳號一定時間之登入，或鎖定該帳號直到系統管理人員重新啟動。

(五) 必要時限定使用者之 IP 位址。

四十一、使用者應選擇高安全性通行碼，力求降低被破解之風險，並應妥善保管避免他人知悉。

通行碼應定期更新；重要應用系統之通行碼更新週期應低於六個月。

四十二、應用系統使用存取權限管理應依下列原則辦理：

(一) 使用者權限之申請，應由權責單位依使用者執行職務之需求，以工作所需最小權限之原則核可後，交由系統管理人員執行相關設定。

(二) 未經核可之申請，系統管理人員不得進行授權作業設定。

(三) 系統管理人員進行遠端維護時，應限制其經由本院核可之遠端連線來源。

四十三、重要應用系統應啟動系統紀錄功能，系統管理人員應保存系統紀錄檔並定期備份。

各系統應視其重要性及支援程度將下列事件列入紀錄：

(一) 系統管理人員及具備特殊權限帳號者之登入成功及失敗事件。

(二) 使用者帳號異動及對通行碼檔案之讀取與變更。

(三) 程式原始碼及執行碼之變更。

(四) 直接進入資料庫管理系統變更資料。

(五) 系統設定檔之存取及變更。

四十四、系統管理人員應依下列原則辦理存取控管作業查核：

(一) 定期辦理帳號清查，若發現帳號不當使用或持有人不再符合申請資格，系統管理人員得停止或註銷該帳號。

(二) 監控有無違反系統存取規定之安全事件，並定期檢視紀錄，分析其異常狀況。

(三) 存取紀錄檔須另行查核。

(四) 已註銷帳號之所屬檔案，得保存一定期限，原帳號持有人得於保存期限內申請重製。但儲存重製檔案之媒體應由申請者自備。

四十五、各單位開放外界連線作業之應用系統，應避免人員直接存取應用系統之資料檔，必要時得視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、代理伺服器、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統遭入侵、破壞、竄改、刪除或未經授權之存取，並記錄完整系統使用資料。

第七章　網路安全管理

四十六、本院為維護資通安全或避免非法行為，得依網路服務性質分別規範網路存取、網路服務功能或通訊協定之使用方式。

四十七、各單位以固定或動態方式提供使用之 IP 位址，應保存其使用紀錄以備資通安全事件稽核之需。

四十八、各單位應管理網路系統及相關設備，以維持基礎網路服務系統正常運作。

四十九、各單位網路系統及設備之管理應依權責配發管理帳號並設定適當權限；除因系統限制外，不得多人共享帳號。

五十、各單位應妥適安全控管對外連接網路之線路與設備，必要時得設防火牆或其他安全設施，以控管外界與本院網路之資料傳輸及資源存取。

五十一、各單位利用公眾網路傳送資訊或進行交易處理，應遵守本院相關規定；並應評估可能之安全風險，確定資料傳輸符合完整性、機密性、身分鑑別及不可否認性等安全需求。

五十二、網路之管理

本院網路之路由接續、IP 位址區段之分配管制及網域名稱(Domain Name)登錄等管理事項由本院資訊服務處負責。

本院網路加值服務之協調與整合由資訊服務處負責。本院各單位之網路管理者為執行本章規定，其有關網路之管理事項如下：

(一) 應辦理安全維護事項，防止個人資料遭竊取、竄改、毀損、滅失或洩漏。

(二) 為維護網路安全及效能，應區隔及調節網路流量。

(三) 配合本院處理網路事宜，提供相關資訊。

(四) 自建網域名稱系統（Domain Name System, DNS）之所中心，須將資訊服務處所通知惡意中繼站之網域名稱設定為黑名單。

(五) 本院資訊設備僅限使用本院認可之 DNS 服務。

(六) 不允許從院外直接連線存取宿舍區網段之資訊設備。

(七) 各單位之公務行政區及訪客區網段，不得對院外網路提供連線服務。

(八) 學術研究區網段之資訊設備，原則上不得直接提供院外網路連線服務，若有提供院外網路直接連線需求，各單位應搭配適當防護措施並予以列管。

五十三、物聯網設備之網路規劃

(一) 物聯網設備應設定網路存取控制，並採實體或虛擬網路隔離或以其他網路技術區劃獨立區域。

(二) 若物聯網設備須與其他區域之設備進行連線，應以防火牆進行區隔。若該物聯網設備涉及敏感資料或生物特徵時，應加強管制。

(三) 物聯網設備應關閉不必要的通訊服務，只提供該設備最少必要服務功能。

五十四、禁止濫用網路系統

使用者不得從事下列行為：

(一) 盜用、冒用他人帳號或無故將個人帳號借予他人使用。

(二) 散布電腦病毒、傳送廣告信或無用訊息或其他違反法令之行為。

(三) 以任何方式偷窺、竊取、更改或破壞他人資訊。

(四) 傳送或散布恐嚇、猥褻或違背善良風俗習慣之資料，或謾罵、侮辱他人等不當言論。

(五) 濫用網路資源，影響系統正常運作或危害網路穩定之行為。

五十五、尊重智慧財產權

使用者應尊重智慧財產權，避免下列可能涉及侵害智慧財產權之行為：

(一) 使用未經授權之電腦程式。

(二) 下載或重製未經授權之著作。

(三) 未經著作權人之同意，重製或散布其著作於公開之網站上。

(四) 任意轉載作者明示禁止轉載之網路文章。

(五) 架設網站供公眾下載未經授權之著作。

(六) 其他可能涉及侵害智慧財產權之行為。

五十六、網路隱私權之保護

網路管理者及使用者應尊重網路隱私權，不得任意窺視個人隱私資料或有其他侵犯隱私權之行為。

五十七、違反之處置

使用者違規使用網路，本院得視情節輕重緩急，為通知改善、縮減使用權限、停止使用或必要之處置，其有關處置說明如下：

(一) 年度內第一次違規使用網路，情形輕微者通知改善，未於一週內改善者得限制其對外連線。

(二) 年度內第二次(含以上)違規使用網路，情形輕微者限制對外連線，未於一週內改善者得停止其網路使用權限。

(三) 違規使用網路情形嚴重者，立即停止網路使用權限。

(四) 網路使用權限已被限制或停止者，得視其改善情形恢復網路使用。

惟依本點進行處置前，應予使用者說明之機會。

使用者違規使用網路，其行為違法時，行為人應依民法、刑法、著作權法或其他相關法令自負法律責任。

五十八、申訴機制

如違規使用網路之行為人對本院依前點所為處置有異議時，得向本院資通安全暨個人資料保護委員會申訴。

第八章　電子資料安全管理

五十九、下列電子資料應依本章規定進行管理：

(一) 供研究或行政使用之資料庫、資料檔或文件檔。

(二) 電腦系統中帳號之個人資料、存取與服務紀錄。

六十、電子資料之經管單位，包括：

(一) 行政用電子資料之相關業務掌理單位。

(二) 研究用電子資料之持有單位。

(三) 受託管理電子資料相關資通系統之單位。

各單位應就所經管之電子資料，訂定使用條件及存取權限。

六十一、敏感性電子資料使用及存取，應遵守相關法令或規定。

其他機關非經法定程序要求本院提供敏感性電子資料者，應予拒絕。

六十二、電子資料之存取，應設控制措施，以防止未經授權之竄改或竊取。

敏感性電子資料之存取，應採取較一般帳號通行碼機制更為嚴格之控制措施，並應注意其相關安全事項。

存有敏感性電子資料之個人電腦，應設具相當安全程度之開機通行碼。

六十三、電子資料應有備份，其儲存裝置得有備援措施。

敏感性電子資料應加密儲存；其未經加密者，不得經由公眾網路傳送或儲存於可攜式儲存媒體。

進行電子資料交換時，若需啟用新服務，應先評估其風險。

六十四、各單位使用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估；敏感性及未經當事人同意之個人資料及文件，不得上網公布。

六十五、本院電腦系統存有單位或個人之敏感性電子資料者，應加強安全保護措施，防止該資料遭違法或不當之竊取使用。

六十六、電腦送修，應先拔除硬碟或抹除敏感性電子資料；報廢時，應抹除或銷毀儲存之所有檔案。

可攜式儲存媒體送修或報廢時亦同。

六十七、委託其他機構或廠商蒐集、處理或利用敏感性電子資料時，應於委外契約書載明資通安全控管要求、保密條款、損害賠償等事項。

第九章　資通安全事件通報、應變及演練

六十八、資訊服務處為本院資通安全事件通報總窗口(以下簡稱總窗口)，依資安法及其子法相關規定，負責下列資通安全事件通報與處理事項：

(一) 本院資通安全事件分級確認。

(二) 依相關規定通報本院資通安全事件。

(三) 規劃資通安全事件處理程序，包括調查事件原因、確認其影響範圍並評估損失及執行緊急應變措施。

(四) 協助各單位處理資通安全事件。

(五) 資安事件通報及應變事項之定期演練。

(六) 本院資通安全長交辦事項。

各單位資安小組負責下列資通安全事件通報與處理事項：

(一) 單位內資通安全事件初步分級。

(二) 單位資安事件依本院管道通報總窗口。

(三) 規劃單位內資通安全事件處理程序，包括調查事件原因、確認其影響範圍並評估損失及執行緊急應變措施。

(四) 資安事件通報及應變事項之定期演練。

六十九、本院通報程序如下：

(一) 各單位知悉資通安全事件時，單位資安小組應依資安法相關規定予以初步分級，並立即將事件通報總窗口。

(二) 總窗口接獲資通安全事件通報後，應彙整相關事件並依相關規定確認分級及進行資安事件通報，同時依本院管道通報受影響單位及機關。

七十、本院應變程序如下：

(一) 事件發生前之防護措施規劃

各單位應評估本院資通安全事件預防需求，建置並維護適當設備及相關技術，以加強防範發生資通安全事件之能力。

(二) 損害控制機制

1.資通安全事件發現並通報後，單位資安小組應依資安法及其子法規定時程復原或完成損害控制。單位資安小組可參考各類資通安全事件處理程序，尋求方案自行處理資通安全事件，或會同資訊服務處或資安處理小組處理。

2.單位資安小組針對已受駭之系統，應立即斷網（或採效果等同斷網之控制措施）並採取積極性損害控管措施。經通報資安長後，得視實際受駭情況阻斷該單位（含學術研究區）全部或部分網路，並得預防性擴大斷網範圍。若經資訊服務處評估有災情擴散風險，得報請本院資安長同意後，針對可能遭受駭客入侵之網段（範圍包含全院各單位之網段）進行斷網，以免災情擴大。

3.遇有三級以上資通安全事件時，應即啟動本院資通安全事件處理小組（以下簡稱本院資安處理小組），進行危機處理與緊急應變措施。資安處理小組由資訊服務處處長擔任召集人，其成員由召集人指定之。

4.資通安全事件之原因、影響範圍、損失情況、分類、分級及應變措施等應詳加記錄，作為改善資通安全缺失、因應未來類似事件及修訂各類資通安全事件處理程序之參考。

(三) 重覆發生相同資安事件之狀況，應通知受駭單位之資安長、所長/主任，並副知該學組的副院長及本院資安長知悉。

第十章　資通安全內部稽核

七十一、各單位依政府相關規定或視實際需要，經資通安全長指示或同意辦理資通安全內部稽核作業，每年至少辦理一次。

七十二、各單位資通安全內部稽核小組(以下簡稱資安內稽小組)採任務編組，負責辦理資通安全內部稽核作業相關事宜。

全院性資安內稽小組召集人由本院資通安全長擔任或指派；小組成員三至七人，由資通安全長遴聘，其中一人由本院政風室推薦；聘任成員應至少有一人為符合政府相關規定資格之資通安全稽核員。

本院應培訓合格資通安全稽核員。

七十三、實施資通安全內部稽核前，資安內稽小組應依本院資安及個資相關規定擬定資通安全稽核計畫書以及資通安全稽核檢查表，送請資通安全長審議核定後，函送受稽核對象準備稽核事宜。資通安全稽核計畫書應至少包括：

(一) 實施對象。

(二) 實施時程。

(三) 實施範圍。

(四) 人員配置。

(五) 相關規範、要點或程序。

七十四、實施資通安全內部稽核時，資安內稽小組應就查核情形詳予記錄，並對所獲悉之機密性或敏感性資料負保密責任；受稽核對象應指派專人配合實施。

七十五、實施資通安全內部稽核後，須盡速完成以下事項：

(一) 資安內稽小組應撰寫資通安全稽核報告，並送各受稽核對象確認。

(二) 各受稽核對象應就資通安全稽核報告中所列缺失事項提具矯正措施或改善計畫；資安內稽小組應確認矯正措施之執行結果，並評估改善計畫之預期效果。

(三) 資安內稽小組應彙整資通安全稽核計畫書、資通安全稽核報告、受稽核對象之矯正措施及改善計畫的總結報告，向資通安全長彙報。