立法院資通安全管理要點

中華民國九十三年八月十日院長核定
中華民國一〇〇年九月二十九日院長核定修正
中華民國一〇三年十一月二十二日院長核定修正
中華民國一〇四年十一月十九日院長核定修正
中華民國一〇八年十一月十一日院長核定修正
中華民國一一二年十一月二十三日院長核定修正名稱及全文(原名稱：立法院資訊安全管理要點；新名稱：立法院資通安全管理要點)
中華民國一一五年一月六日院長核定修正

一、（目的）

立法院（以下簡稱本院）為維護整體資通安全，強化各項資訊資產之安全管理，確保其機密性、完整性、可用性及法律遵循性，以因應業務運作需要，妥善支援立法委員依法行使職權，特訂定本要點。

二、（名詞定義）

本要點所稱資通安全係防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

本要點所稱資訊資產係本院所收集、產生、運用之資料，以及為完成以上工作所需使用之相關設備。

三、（適用範圍）

本要點適用於本院各項資訊資產及其資訊使用者。

四、（遵循性/法令依據）

本要點及依據本要點所訂定之各項附屬規定，係參考資通安全管理法、個人資料保護法、著作權法、國家機密保護法、電子簽章法等法規及其他相關標準所訂定，資訊使用者應確實遵守，如有違反者，依相關法令辦理。

五、（資通安全組織）

本院資通安全暨個人資料保護管理委員會(以下簡稱本委員會)依據立法院資通安全暨個人資料保護管理委員會設置要點統籌規劃資通安全管理事項。

六、（人力資源安全）

為降低內部人為因素對本院資通安全之影響，各單位應考量人力及工作職掌，實行分工及輪調措施。

本院定期實施資通安全教育訓練及宣導，以提高人員對資通安全之認知。

七、（資訊資產管理安全）

為保護本院資訊資產安全，應建立資訊資產清冊加以分類分級，並訂定相對應之管制措施。

八、（存取控制安全）

為避免本院資訊資產因未授權之存取而使機密性或敏感性資料遭不當使用，應考量人員職務授予相關權限。

為確保本院遠距工作的使用安全，應對遠距工作存取訂定相對應之管制措施。

九、（憑證安全）

本院憑證申請及應用原則，應定期進行評估，以保護資訊的機密性、鑑別性及完整性，必要時得採行加解密及身分鑑別機制，以加強資料之安全。

十、（實體及環境安全）

為確保本院電腦機房維運及資訊資產使用區域之安全，應訂定實體與環境安全管理原則。

為確保本院行動裝置及可攜式儲存媒體的使用安全，應建立行動裝置與可攜式儲存媒體管理原則。

十一、（運作安全）

為確保本院主機作業平台、資料庫與資通處理設施被正確及安全操作，受到防範惡意碼的保護、防護資料損失及竄改、紀錄事件及產生相關證據、保護作業系統的完整並防止技術脆弱性被利用，應訂定運作與通訊管理作業原則。

十二、（通訊安全）

為確保本院網路及其支援資通處理設施上資訊之保護，並維護內部及外部單位資訊傳送之安全，應訂定運作與通訊管理作業原則。

十三、（系統獲取、開發及維護安全）

為確保本院資通系統生命週期的資通安全控管，分析、設計、開發、測試、上線及維護各階段之資通安全，應訂定系統獲取、開發及維護安全管理標準作業原則。

十四、（供應者關係安全）

為確保供應者(含雲瑞服務提供者)可存取的本院資訊資產受到保護，並維持資通安全及服務交付與供應者協議一致，應訂定供應者關係安全管理要

求。

為提高本院委外作業之安全，應要求廠商簽署保密協議書及廠商人員簽署保密切結書，並管理專案人員及駐點人員之各項資訊資產存取權限。

十五、（資通安全事件管理）

為確保本院資通安全事件管理（包括對安全事件及弱點之通報）有一致及有效的作法，應建立資通安全事件通報及處理程序，並加以記錄。

本院應訂定資通安全目標，並確保該目標符合本要點之目的要求。

十六、（營運持續管理之資通安全層面）

為避免本院資訊資產遭受災害而影響業務永續運作，確保資訊處理設施的可用性，資通安全持續性應做為營運持續管理之基礎，且訂定營運持續緊急應變演練及復原計畫，並定期測試演練。

十七、（資通安全稽核管理）

為落實本要點，強化資通安全管理，應建立資通安全稽核機制，並定期執行稽核。

十八、（風險管理）

為有效管理本院各項資訊資產所面臨之威脅、弱點及其衝擊程度，應辦理資訊資產風險評估並實行必要之風險管理。

十九、（每年檢討）

本要點應每年檢討，以反映最新標準規範、技術及組織業務現況。

二十、（宣導）

本要點應定期宣導。

二十一、（施行）

本要點經院長核定後施行，修正時亦同。