財團法人法律扶助基金會　資訊安全管理要點

本會108年9月20日第6屆第7次董事會決議訂定全文46點

壹、目的

一、財團法人法律扶助基金會（以下簡稱本會)為強化本會資訊安全管理，確保資料、系統、設備及網路安全，特訂定本要點。

貳、通則

二、本會應依「資通安全管理法」、「個人資料保護法」及其它有關法令，考量施政目標，進行資訊安全風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資訊安全措施。

三、本會採行資訊安全措施及訂定、修正、實施資通安全維護計畫，應考量下列事項：

（一）資訊安全政策訂定。

（二）資訊安全組織及權責。

（三）人員管理及資訊安全教育訓練。

（四）資訊系統安全管理。

（五）網路安全管理。

（六）系統存取控制管理。

（七）系統發展及維護安全管理。

（八）資訊資產安全管理。

（九）實體及環境安全管理。

（十）業務永續運作計畫。

（十一）其他資訊安全管理事項。

四、本要點所稱資訊安全政策，指本會為達成資訊安全目標，所訂定之資訊安全管理作業原則、措施、要點、注意事項及作業程序等。

參、資訊安全政策訂定

五、本會應依實際業務需求，訂定資訊安全政策，並以書面、電子或其他方式告知本會同仁、兼職人員、志工、實習生、連線作業之公私機構及提供資訊服務之廠商共同遵行。

六、資訊安全政策，應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

肆、資訊安全組織及權責

七、本會應由執行長或其指定之高層主管人員，綜理資訊安全管理事項之協調及推動。

本會應成立跨部門之資訊安全推行小組，統籌資訊安全政策、計畫、資源調度等事項之協調、研議。

前項資訊安全推行小組之幕僚作業，由資訊單位或執行長指定之單位負責。

八、本會應依下列分工原則，配賦有關單位及人員之權責：

（一）資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。

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

（三）資訊機密維護及稽核使用管理事項，由資訊安全推行小組負責辦理。

九、本會對資訊作業，應進行定期或不定期之資訊安全稽核。

伍、人員管理及資訊安全教育訓練

十、本會對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，進行必要之考核。

十一、 本會同仁、兼職人員、志工及實習生因工作職責須使用或處理資訊者，應課予機密維護責任，並儘可能簽署書面約定，以明責任。

十二、 本會應針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升機關資訊安全水準。

十三、 本會負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，並依需要建立制衡機制和人力備援制度。

陸、資訊系統安全管理

十四、 本會開發資訊系統時，應訂定資訊系統作業程序，以確保本會同仁、兼職人員、志工、實習生正確及安全的操作使用電腦，並作為系統發展、維護及測試作業之依據。

十五、 資訊系統作業程序，應載明電腦不正常停機及作業發生錯誤或遭遇非預期的問題時之處理規定。

十六、 本會開發資訊系統時，應將系統測試作業及系統正式作業之軟體，分別安裝在不同主機或不同的目錄下作業，使系統測試與正式作業分開處理，避免作業軟體或資料遭意外竄改。

十七、 資訊設備及系統的變更作業，應建立管控措施，對於資訊系統作業中斷及更正等異常事項，應詳實記錄。

十八、 資訊系統應採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

十九、 重要的資料及軟體應定期執行備份作業。備份機密或敏感性資料，應採行必要的資料安全保護措施。

二十、 本會應規範可攜性電腦媒體（如磁帶、磁碟、隨身碟、光碟及電腦輸出報表等）之使用，防止不當使用。

二十一、 系統文件（包括系統流程、作業流程、資料結構、檔案格式等）應採行妥適的安全保護措施，防止不當使用。

二十二、 與外部單位間進行資料或軟體資訊交換，應採行必要的資料安全保護措施及賦予有關人員安全責任。

柒、網路安全管理

二十三、 本會利用公眾網路傳送資訊或進行交易處理，應評估可能之安全風險，考量資料傳輸之完整性、機密性、身分鑑別及不可否認性等安全需求，並對資料傳輸、撥接線路、網路線路與設備、對外連接介面及路由器等事項，採行妥適的安全控管措施。

二十四、 本會開放外界連線作業之資訊系統，應依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、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。必要時應以代理伺服器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。

二十五、 本會與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與機關內部網路之資料傳輸及資源存取。

本會網路由本會資訊單位統一規劃、建置及管理，不得自行將本會網路與外界網路連接。

本會如為服務民眾，得於公共區域建置無線上網服務，惟必需與本會網路之資訊設備實體隔離。

本會區域網路應設置於本會辦公室內，不得設置於辦公室以外之場所。資訊設備，未經核可，不得連接本會網路及本會資訊系統，或擅自修改本會資訊設備相關系統設定。

同仁自行攜帶之可攜式資、通訊設備（如智慧型手機）得使用無線網路服務功能，惟必需與本會網路實體隔離。

二十六、 本會利用網際網路公布及流通資訊，應實施資料安全等級評估，除法

令另有規定者外，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

本會網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭不當或不法之竊取使用。

二十七、本會採購資訊軟硬體設施，應依國家標準或權責主管機關訂定之政府資訊安全政策，研提資訊安全需求，並列入採購規格。

本會發展及應用加密或電子簽章技術，應採用權責主管機關認可之密碼模組產品。

本會採購密碼模組產品，應請廠商提出輸出許可或相關授權文件，確保密碼模組之安全性，並避免採購金鑰代管或金鑰回復功能之產品。

捌、系統存取控制管理

二十八、本會應依執行法定任務之實際需要，賦予各級人員必要的系統存取權限。

本會同仁、兼職人員、志工及實習生因業務之必要，須於前項授權使用權限外特別授權使用者，應向本會資訊單位提出申請授權。

本會同仁、兼職人員、志工及實習生取得系統及網路使用授權，限於公務使用，並應保持行政中立，禁止發表個人政治立場、或為人身攻擊等非公務用途之利用。

二十九、本會應建立系統使用者註冊管理措施，加強使用者通行密碼管理，本會應依作業系統及安全管理需求，要求使用者定期更新密碼。

對本會內外擁有系統存取特別權限之人員，應建立使用人員名冊，加強安全控管，核心資通系統密碼更新周期最長以不超過三個月為原則。

本會應定期及於系統異動、人員職務異動時，審查使用者之存取權限，並做必要之調整。

三十、　識別碼及密碼使用人僅得為公務之需要查詢資料，不得擅自為公務以外之利用。查詢資料及相關使用規範，依個人資料保護法之規定。

三十一、本會委託廠商建置及維護重要之軟硬體設施，應在本會相關人員監督及陪同下始得為之。

三十二、本會對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

三十三、本會之重要資料委外建檔，不論在本會內外執行，均應採行妥適之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

三十四、 本會應確立資訊系統稽核項目，建立資訊安全稽核措施，定期或不定期進行資訊安全稽核作業；系統中之稽核紀錄檔案，應禁止任意刪除及修改。

玖、系統發展及維護安全管理

三十五、 辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守。

三十六、 自行開發或委外發展系統，應在系統生命週期之初始階段，將資訊安全需求納入考量；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、暗門及電腦病毒等危害系統安全。

三十七、 本會基於實際作業需要，得核發系統通行密碼供軟硬體系統建置及維護廠商使用，並規範及限制其可接觸之系統與資料範圍。契約結束或人員異動時應立即取消其使用授權及通行密碼。

壹拾、 資訊資產安全管理

三十八、 本會應建立重要資訊資產目錄、擁有者及安全等級分類等資料。

三十九、 資訊資產應包括下列項目：

（一）資料資產：如資料庫及資料檔案、系統文件、使用者手冊、訓練教材、業務永續運作計畫等。

（二）軟體資產：如應用軟體、系統軟體、發展工具及公用程式等。

（三）實體資產：如電腦主機、通訊設備、媒體資料及其他技術設施。

（四）技術服務資產：如電腦、通信服務及其他技術性服務。

四十、 本會應依相關法規或契約規定，複製及使用軟體，並建立軟體使用管理措施。

拾壹、實體及環境安全管理

四十一、 本會應就設備安置、周邊環境及人員進出管制等，採行妥適之實體及環境安全管理措施。

四十二、 資訊系統、設備、線路及設施，應實施必要之保護措施及維護，以確保資訊系統正常運作。

四十三、 設備報廢、再利用或移轉，應先清除原有之重要資訊並移除有版權之軟體。

拾貳、業務永續運作計畫

四十四、本會應評估各種人為及天然災害對機關正常業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

四十五、本會應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向權責主管單位或人員通報，採取反應措施，必要時聯繫檢警調單位協助偵查。

拾參、附則

四十六、本要點經董事會決議後實施；修正時，亦同。