廉政防貪指引

資訊安全篇

114 年 10 月

目　錄

壹、序言

「資安即國安」，隨著數位化科技時代的來臨，本部暨所屬機關（構）於積極推動衛福業務數位轉型服務的同時，亦持續強化資安治理和營運韌性，以提升資安防護能力，確保系統及資料安全。

然而對於資安的輕忽更是最大的國安風險來源，為深化本部暨所屬機關（構）同仁對於資訊安全之認知，預防公務機密資料外洩及個人資料遭不當查詢等風險，本處秉持「興利優於防弊、預防重於查處」之精神，蒐集實務曾發生之違失或不法案例 10 則，以「妨礙使用」、「不當查詢」及「資料外洩」等 3 種態樣編寫「防貪指引手冊—資訊安全篇」，內容包含分析風險態樣、發生緣由、可能涉及之法律責任，並提出防制措施，期能提醒同仁建立正確的資安意識，共同築起守護機關資訊安全的堅實防線，以確保全民的健康福祉。

衛生福利部政風處　謹誌

貳、妨礙使用態樣

案例 1：遠端連線，危機浮現

➢案情概述

A、B 皆為某部立醫院護理師，A 某日應 B 之請求，使用家中電腦遠端連線至 B 所使用之公務電腦，協助 B 處理醫囑系統列印問題；又於某日 A 因休假無法立即登打醫師查房紀錄，遂要求 B 開啟護理站公務電腦，並透過家中電腦遠端連線進行登錄作業。

A 兩次遠端連線行為均未經醫院許可授權，且涉及登入限定院內網域 IP 方可存取的護理資訊系統(下稱 NIS 系統)，A 的行為已違反醫院網路使用管理程序書，經該院移送考績委員會追究行政責任。

➢風險評估

❶未遵循機關資訊安全政策

目前遠端連線環境及存取機制仍存在資安疑慮，易成為駭客攻擊機關資訊系統的途徑。A 未經醫院許可，擅自使用非授權設備遠端登入醫院資訊系統，不僅違反網路使用管理程序，增加病患個資外洩風險，稍有不慎，亦可能影響醫療業務運作，造成難以想像之損失。

❷缺乏對機敏資料保密意識

病患醫療資料屬於《個人資料保護法》之特種個人資料，具機敏性，A 貪圖一時方便，使用私人設備連線登入 NIS 系統，將病患個資曝露於不安全的網路環境，缺乏個資保護意識。

❸未落實資安事件通報機制

B 明知 A 未經許可，仍要求及協助 A 利用私人設備遠

端連線操作公務電腦，對於 A 違反院內網路使用管理規範，未依規定進行異常事件通報作業。

➢防制措施

❶強化網路使用管理措施

醫院應落實網路使用管理之內控機制，針對公務電腦及系統權限加強控管及稽核，勾稽系統資料以瞭解業管人員權限使用情形，禁止未經授權使用遠端連線存取公務電腦及系統資料情事。

❷加強資訊安全教育訓練

A 未經許可遠端登入 NIS 系統，資安意識不足，醫院應提供資訊安全相關教育訓練，提升內部基層及管理人員資訊安全認知，並加強相關防護知識，以避免相類事件再次發生。

❸做好資安事件通報應變

醫院員工如發現醫療資訊系統或網路狀態出現異常，或有不當登入及遠端連線等行為時，應立即通報單位主管及資訊單位處理，預防資安事件擴散，以維護資訊安全。

❹落實交接班及代理制度

A 透過家中電腦遠端連線處理病患相關事務，惟醫院均訂有醫療人員交接班流程，應遵照標準作業程序辦理，原照護醫療人員下班或休假時，亦應有代理人之機制，以確保病人安全。

➢參考法令

- 資通安全管理法。
- 個人資料保護法第 6 條。
- 衛生福利部醫療領域資通系統資安防護基準。
- 衛生福利部基層醫療院所資安防護參考指引。

溫馨提醒

遠距工作型態造成資安風險提高，居家網路環境的資安弱點亦可能帶來破口，勿因一時方便而忽視資訊安全規範；如因業務需要安裝並開啟遠端連線軟體之設定使用，應檢視是否有限制連線時間、IP 以及 Log 稽核紀錄保存等管理機制；倘無遠距使用需求時，應即中止連線服務（關閉遠端連線連接埠），以落實機關資安防護。

返回目錄頁

案例 2：一卡在手，病歷到手

➢案情概述

甲護理師自某部立醫院離職後，未依規定繳回門禁卡。某日甲利用門禁卡進入醫院管制區-呼吸照護病房護理站，恰巧當日值班護理師乙未即時登出醫療業務系統，使甲得以直接使用乙之帳號查詢其個人病歷資料並列印檢驗報告。

甲的行為經院方人員當場發現，立即收回其未繳還之門禁卡及所列印之檢驗報告，並要求甲即刻離開院區。

➢風險評估

❶門禁管制未落實

甲離職後未依醫院規定繳回門禁卡，院方亦未解除該門禁卡使用權限，致離職員工可自由進出管制區。醫院未落實呼吸照護病房之進出管制，除造成本案不當查詢外，亦徒增病人安全之風險。

❷帳號管理未臻嚴謹

甲擅自使用乙之帳號使用公務電腦，係因乙未即時登出資訊系統，給予甲存取醫療系統資料之機會，足見機關同仁對於公務電腦的管理及醫療資料的保護未臻嚴謹，易生資料外洩之風險。

❸同仁法治觀念不足

甲明知自己已不具該院護理師身分，仍任意進入醫院管制區域，無視門禁及人員管制措施，且心存僥倖以乙之權限查詢個人病歷資料，欠缺法治觀念。

➢防制措施

❶落實離職交接程序

離職員工應克盡交接離職手續，依規定繳回門禁識別證件、職章及申請停用內部系統帳號權限等。單位主管及相關單位亦應確認離職人員已完成交接，確保門禁與系統權限已解除，避免未經授權人員進出機關(構)及存取內部資訊。

❷強化管理使用權限

為落實帳號管控，應定期及不定期實施帳號清查作業，檢視現職人員帳號使用情形及離職、留職停薪人員是否仍具帳號權限；另同仁應養成使用完畢後，登出電腦系統的習慣，如長時間離開座位，應啟動螢幕保護並執行限制操作時間螢幕鎖定設定，避免讓有心人士有可乘之機。

❸加強員工法治教育

鑑於部分員工法律觀念不足，易生誤觸法令而身陷違法的風險，機關宜加強相關教育訓練，提醒同仁遵守帳號使用規範，不得借用或外借帳號密碼，個人健康資訊可透過正規管道(如院內健康管理系統或申請病歷複印)查詢，不得自行使用業務系統查詢，以免違反資安規範受行政責任追究，甚而觸犯刑責。

❹加強管制區人員進出控管措施

醫院管制區域應加強人員出入管控，如要求醫護與行政人員佩戴識別證、實施訪客登記制度及身分核實等，以避免離職員工或非必要人員任意進出管制區。

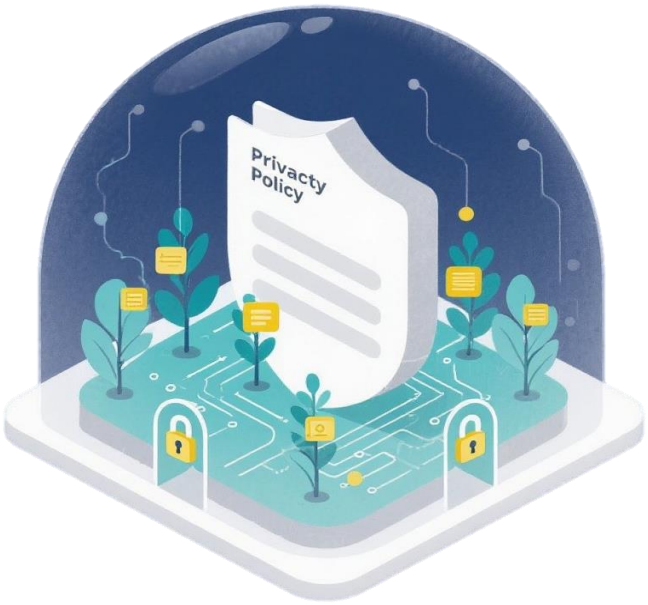
➢參考法令

- 刑法「妨害電腦使用罪章」。
- 資通安全管理法。
- 衛生福利部醫療領域資通系統資安防護基準。
- 衛生福利部基層醫療院所資安防護參考指引。

溫馨提醒

於公務機關（構）服務之人員離職時，應遵守《公務人員交代條例》等相關規定，妥慎辦理承辦業務及經管財物之移交工作，且離職人員之門禁卡及系統權限應及時收回註銷或停用，以避免公務資料外洩；另提醒同仁在沒有正當理由或未得設備所有人允許之情況下，擅自透過輸入帳號密碼、破解保護措施或利用系統漏洞的方式侵入他人電腦，係有可能因此觸犯刑事責任。

返回目錄頁



案例 3：病毒勒索，醫療束手

➢案情概述

某部立醫院資訊室於某日接獲員工反映醫療資訊系統(HIS)無法使用，且發現有多臺電腦主機遭駭客植入勒索病毒，院方旋即改以人工作業模式處理醫療業務，並至「國家資通安全通報應變網站」進行 2 級資安事件通報作業。

嗣本案除循「地區安全防護工作執行會報」平臺機制進行通報外，院方並於案發次日派員前往該地區法務部調查局調查站針對本資安事件涉嫌妨害電腦使用罪部分提出告訴。

➢風險評估

❶作業系統安全漏洞

勒索病毒又稱「勒索軟體」，係駭客透過強加密方式剝奪資料存取權限，藉以威脅要求贖金的惡意程式。勒索病毒常藉由醫院網路瀏覽器、作業系統、應用程式及防毒軟體未更新等資安防護漏洞，侵入醫療系統造成損害，甚擴散至其他連結的醫療單位，導致營運中斷或經營損失。

❷員工缺乏資安意識

醫院人員多專注於臨床工作，對於釣魚郵件、惡意附件等社交工程攻擊的警覺性較為不足，而勒索軟體常潛藏於釣魚郵件或非法軟體中，倘員工缺乏資安意識，安裝來歷不明的程式、隨意點選瀏覽網頁或連結、不當使用電子郵件、擅自更改系統環境設定或使用私人資訊設備等，均可能對於機關資訊安全造成漏洞，易導致公務電腦受到勒索病毒威脅。

➢防制措施

❶加強資安防護措施

①定期更新系統

應加強檢視網路瀏覽器及作業系統環境，保持系統為最新狀態，勿自行關閉系統自動更新修補程式功能，如設備使用之作業系統版本較為老舊且原廠不再提供版本更新服務，應改用還有官方支援的應用軟體，或增加資安防護設備，以確保整體資訊安全機制之運行。

②安裝防毒軟體

醫務/醫療作業使用之電腦、筆電或伺服器應安裝防毒軟體，並定期檢視防毒軟體之病毒碼是否已更新至最新版本；另應避免使用網路上提供之免費使用防毒軟體，以降低風險。

❷完備資料庫備份機制

本案醫院醫療系統雖遭受駭客攻擊，惟相關資料庫皆有備份機制，方能儘速完成系統資料重建回溯。故平時機關應定期執行重要資料之備份作業並加密處理，且建議備份資料異地存放，以減少意外災害造成的損失。

❸建立良好的使用習慣

機關同仁應有良好的電腦使用習慣，勿開啟來源不明的電子郵件，下載附件時，請使用防毒軟件掃描；點擊連結時，請檢查網址是否異常，不使用網路上非法授權之軟體、不隨意下載網路上的軟體程式、不私接 ADSL、無線網卡或手機熱點等網路通訊設備；另對於個人之帳號密碼，採取具複雜變化之防禦高強度密碼並定期更換，以維護機關資訊安全。

❹落實資安稽核及演練

透過資安稽核能及早發現漏洞，建立持續改進的循環，而定期演練資安事件及復原流程，則得以應對突發攻擊，確保病人資料安全與醫療不中斷。而本部前業將《資通安全法》納入醫院評鑑的基準項目，醫療院所須定期接受資安稽核，數位發展部亦於 114 年將資安稽核擴大至醫院，並引進 AI 智慧稽核與外部曝險檢測，為醫院進行深度資安體檢，找出潛在弱點並及早修復，讓駭客無從下手。

➢參考法令

- 刑法「妨害電腦使用罪章」。
- 資通安全管理法。
- 醫院面對勒索軟體攻擊的應變指南。
- 衛生福利部醫療領域資通系統資安防護基準。
- 衛生福利部基層醫療院所資安防護參考指引。

溫馨提醒

目前國內外醫療機構遭駭客嘗試攻破或以勒索病毒擴散造成系統當機等資安事件時有所聞，恐導致醫療資訊系統癱瘓、病歷資料外洩，嚴重影響醫療服務與病人安全；而國內醫療院所普遍存在資安管理不落實、內網防護薄弱、設備老舊及人力專業不足等問題，建議醫院高層要有資安治理的決心，全面盤點現有 IT、OT 設備及資安架構，加強端點與內部防護，並招募、培訓專業資安人員，嚴謹備份與復原計畫，且強化委外廠商管理，逐步提升醫療體系整體資安韌性。

返回目錄頁

案例 4：網路釣魚，小心上鉤

➢案情概述

某機關客服中心接獲民眾反映，收到以該機關名義寄發之不明郵件，研判應為釣魚郵件，可能夾帶惡意網址連結或木馬程式。該郵寄地址雖顯示為機關官方域名，惟透過線上惡意軟體分析網站查察，發現寄信來源出自愛爾蘭之主機，非由該機關郵件伺服器發出。

本案為 1 級資安事件，該機關依規定通報數位發展部資通安全署；另駭客冒用該機關名義部分，業由該機關向轄區派出所報案。

➢風險評估

❶以假亂真的網路釣魚

近年詐騙手法推陳出新，惡意郵件成為詐騙手段之一，惡意郵件常冒用政府機關名義，利用數字或英文字母相似的網域寄發郵件，混淆民眾視聽，藉以誘導開啟信件，進而竊取個人資料。

❷人性弱點為資安漏洞

此類釣魚郵件為社交工程常見手法，主要係利用人性的弱點，諸如好奇心、本能反應、無知、信任、貪婪、恐懼、惰性、掉以輕心等，透過電話、電子郵件、簡訊、LINE 等即時通訊軟體，誘騙其點擊惡意信件或行動簡訊，以竊取個資或植入惡意程式，造成機敏資料外洩或遭勒索病毒攻擊等風險。

❸防「釣」敏感度不足

資安事件多從一封釣魚郵件開始，駭客透過高度偽裝

的釣魚郵件，搭配社交工程手法對目標發動攻擊。一旦使用者戒心不足，被植入惡意程式或釣走帳號密碼，駭客攻擊便從入侵單一電腦，進而癱瘓機關資訊系統，影響業務正常執行。

➢防制措施

❶落實通報及應變作業

收到來源可疑之電子郵件時應謹慎應對，切勿直接開啟信件，應即時查證或向資訊單位通報協助處理；若有不慎或已察覺電腦異常，亦務必誠實通報，以即時控制損害，降低資安事件對於機關業務之衝擊影響。

❷加強社交工程模擬演練

機關平時應加強社交工程模擬演練，不定期以電子郵件或簡訊方式進行釣魚攻擊模擬，保持員工的高度警覺性，降低人為失誤風險；提醒同仁避免以公務信箱接收或傳遞私人訊息，並定期實施相關教育訓練，逐步建立員工的資安習慣，使資安意識融入機關文化。

❸妥善保護帳號密碼

妥善保護自身帳號密碼，避免成為釣魚幫兇，並減少使用重複的帳號密碼，當某一組帳號密碼外洩，可能所有使用同樣一組帳號密碼的都將被盜用；另機關應隨時掌握詐欺犯罪之趨勢及型態，並採多元方式加強防範宣導(例：即時於官網公告或發布新聞澄清)，以提醒民眾避免受騙。

➢參考法令

- 資通安全管理法。
- 個人資料保護法。

溫馨提醒

近年來，對於公務機關或關鍵基礎設施進行網路攻擊之情形時有所聞，由於公務機關所承擔之公共任務，及關鍵基礎設施所維運或提供之服務，均對國家安全、民眾生活、經濟活動等有重大影響，一旦遭受惡意攻擊，恐造成難以回復之損害，爰機關同仁應時時刻刻提高警覺，建立零信任架構，落實機關資安防護作為，以確保國家安全。

返回目錄頁

案例 5：業務委外，嚴防被駭

➢案情概述

A 公司係甲機關委託印製及寄發繳款單之委外廠商，B 公司為 A 公司之母公司，某日 B 公司之資料庫遭駭客入侵，B 公司資安部門隨即啟動相關防禦機制及備援作業。

甲機關得知後，立即派員至 A 公司進行瞭解，確認此一資安事件尚未影響至 A 公司，無公務及個人資料外洩之情形，且 A 公司亦有依契約規範於完成印製後銷毀機關所交付之資料。

➢風險評估

❶供應網絡的資安威脅

機關將部分業務委外處理，委外廠商就受託業務而取得之公務或個人資料，倘因委外廠商資安防護措施不足，使駭客有機可乘，攻擊竊取機敏資料，甚至成為駭客入侵機關系統之跳板；另機關與外包廠商間，或外包廠商與其員工間資料傳遞時，若控管不當亦可能導致資料外洩。

❷委外人員的資安隱憂

委外作業人員可能使用機關內部系統處理個資、公文、財務等資料，存在接觸知悉民眾個人資料或公務機密之機會，若法治觀念薄弱、教育訓練不足或習慣不良，缺乏保密與責任意識，非授權存取、不安全資料傳輸、裝置或文件遺失，都可能成為資料外洩的源頭；又委外團隊成員更替頻繁，若無妥善管理，亦將成為資安漏洞。

➢防制措施

❶加強委外廠商管理

機關應將資安要求、資料處理規範、通報機制及違約責任等納入契約並落實履約管理，並加強存取權限與設備控管，僅提供廠商完成任務所需的最小資料與存取權限，避免過度授權；另於履約完成或契約終止後，督促廠商應即刪除或銷毀因執行服務所持有機關之相關資料，或依機關指示返還之。

❷強化人員資安意識

為降低委外作業人員之資安風險，機關應與委外服務人員簽署資安及保密協議，明確讓委外人員瞭解其法律責任，並定期辦理資安教育訓練，提升相關人員對資料保管、防護與傳輸機制的理解，以增強資料防護的安全性與人員資安意識；另建立資安通報機制，提供外包人員通報資安異常或可疑行為之管道，避免事態擴大。

➢參考法令

- 資通安全管理法。
- 個人資料保護法。

溫馨提醒

實務上曾發生外包業者弄丟存放民眾資料之 USB 儲存裝置事件，機關的資安範圍不限於「單一組織內部」，而是擴展到所有與該機關互動、有資料交換或系統介接的外部單位，特別是委外廠商與第三方服務提供者。因此，在強化資安管理時，務必將委外廠商視為整體防禦架構的一部分，納入政策、訓練與稽核範圍，不讓外包成為機關資訊安全的隱患。

返回目錄頁

案例 6：偷開處方，惹禍自傷

➢案情概述

甲為某部立醫院護理師，明知其未具醫師資格，不得擅自執行醫療業務，竟多次未經醫師乙授權同意，使用其醫師權限，為多位病患開立醫囑及處方箋；嗣後亦多次使用乙之帳號密碼，為自己開立醫囑及處方箋，領取藥品私用。

甲的行為係犯《醫師法》第 28 條非法執行醫療業務、《刑法》第 220 條第 2 項、第 210 條、第 216 條之行使偽造準私文書罪等罪，經法院審理後，各判處 6 月、5 月有期徒刑，應執行 9 月，緩刑 2 年。
（參考資料：臺灣桃園地方法院 111 年度審醫簡字第 1 號刑事簡易判決）

➢風險評估

❶法紀觀念薄弱

甲因病患及自身之領藥需求，擅自執行醫療業務，認為以醫師帳號密碼登入醫療管理系統無人會察覺，因而私自開立醫囑及處方箋，使自己陷入刑事犯罪而不自覺。

❷逾越本身權限

開立醫囑及處方箋為醫師權限，除有《護理人員法》第 24 條第 3 項情形，專科護理師始得於醫師監督下執行醫療業務，而本案甲非專科護理師，竟逾越本身權限開立醫囑及處方箋。

❸疏忽帳密保管

乙醫師表示因請甲協助處理資訊系統故障排除，方告

知帳號密碼，惟並未授權甲使用。實務上，部分醫師基於醫療服務需要，會告知跟診護理師醫療管理系統之帳號密碼，惟事後又未即時更改帳密，致醫師權限遭濫用而衍生偽造醫囑及處方箋之風險。

➢防制措施

❶落實業務權責分工

開立醫囑及處方箋是醫師的權責，護理人員除有《護理人員法》第 24 條第 3 項所規定的情形，才能在醫師的監督之下執行醫療業務。因此，各自必須在法律授權的範圍內執行本身的權責。

❷妥善管理帳號密碼

醫護人員應遵守系統帳號密碼使用規範，不得借用或外借帳號密碼，如遇偶發事件告知他人帳號密碼，應於事件結束後儘速更換；另倘發現系統有不當登入、未授權存取病歷等異常行為，應立即通報處理。

❸強化同仁資安意識

機關宜適時對於新進或在職醫護人員辦理法紀及資安教育訓練，強化員工守法意識。同時應養成正確使用電腦的習慣，避免讓有心人士有可乘之機；另可適時進行不定期稽核，確認有無未經醫師授權而冒開醫令等異常情事。

❹請醫師開立處方箋

醫事人員平日忙於工作，如身體不適而有拿藥需求時，應依一般看診流程，先掛號然後請醫師開立處方箋，切勿私自利用醫師帳密登入系統自行開立醫囑及處方箋，以免誤觸法令。

➢參考法令

- 醫師法第 28 條。
- 刑法第 210 條、第 216 條及第 220 條第 2 項。

溫馨提醒

因醫療資訊系統涉及大量個人健康資訊、病歷資料等機敏資訊，任何一個帳密外洩都可能造成全面性資安事件，損害病人安全與醫療機構信譽，故帳號密碼的管理在醫療機構中尤為重要，醫護人員應確實遵守醫療系統使用規範，落實帳號密碼管理措施，以減少個資洩漏風險。

返回目錄頁

參、不當查詢態樣

案例 7：走過留痕跡，亂查留案底

➢案情概述

A 係某機關同仁，為依法令服務於國家所屬機關而具有法定職務權限之公務員。惟其除於任職期間以公務電腦及其職務上所配發之公務帳號、密碼，登入內含民眾個人資料之應用系統，基於私人目的查詢多位機關員工及民眾，並儲存於個人公務電腦，共計數千筆個人資料外，並於 113 年間違法查詢取得其子之入出境資料，且以電子郵件傳送予當事人。

A 利用職務權限違法查詢及蒐集民眾個人資料之行為，經檢察官偵查終結，以違反《個人資料保護法》第 19 條第 1 項、第 41 條、第 44 條之公務員假借職務上機會非法蒐集、處理、利用個人資料罪嫌予以起訴，並經機關考績委員會決議分別核予大過 2 次、記過 2 次之處分。

➢風險評估

❶濫用職務權限

A 於執行法定職務時始具有查詢相關應用系統資料之權限，惟 A 卻濫用職務權限，不當查詢及蒐集與公務無關之個人資料，足生損害於被查詢者及危害機關對於個人資料之管理，更損及民眾對公務員公正行使職務之信賴，影響機關廉潔形象。

❷人員久任一職

A 長期濫用職權查詢與公務無關之個人資料，或係因其久任一職，熟悉相關系統之使用及勾稽制度，易有「人熟、事熟、系統也熟」之風險，滋生舞弊空間。

❸欠缺法紀觀念

因承辦業務所需，賦予 A 查詢個人資料權限，然 A 卻濫用系統權限，查詢個資為己所用，違反《個人資料保護法》及機關資訊管理相關規範，輕忽公私界線，法紀觀念薄弱。

➢防制措施

❶強化系統管控機制

機關內部應有系統使用規範，明訂非因公查詢之態樣及後續處置作為，以及列管個人可攜式存取設備等；另應用系統本身應存有使用者、查詢鍵值、查詢時間等資訊，以利存取權限控管及查詢紀錄管理。

❷加強執行內控查核

除以系統監控並篩選異常情形外，對於同仁查詢及使用資訊系統實施定期或不定期查核，審視使用者帳號之查詢次數、查詢原因及查詢日期等，如查有違失，應落實檢討並研訂內部規管措施，以發揮警惕作用，並避免發生相類情事。

❸定期檢討辦理輪調

機關宜適時進行職務調整或輪調，以避免員工因久任職務，衍生可能濫權、圖利本人或第三人等不法情事，建議得按業務屬性之風險高低程度，制定輪調年限標準，亦得就平時表現及品德操守不定期調整職務。

❹提升個資保護意識

機關可透過內部會議或教育訓練時機，辦理相關法令宣導，以洩密違規案例，分享個案事件發生原因及可能涉及之法律責任等，深化同仁公務機密維護及個人資料保護

之觀念，以避免同仁因不諳法令，而誤觸法網。

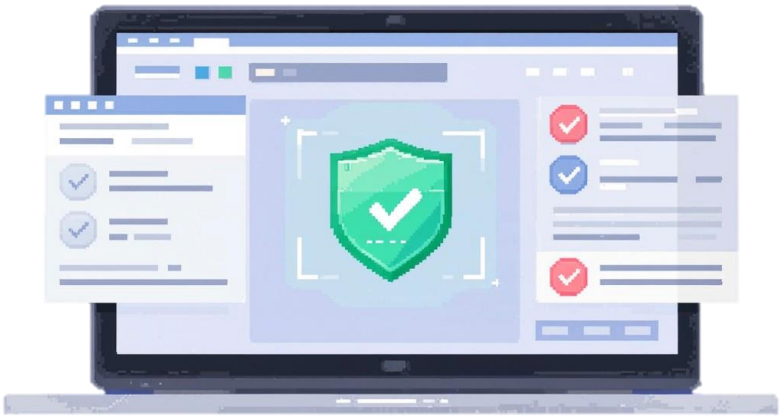
➢參考法令

- 刑法第 132 條第 1 項。
- 個人資料保護法第 19 條、第 41 條及第 44 條。

溫馨提醒

如何善用電腦資訊作業系統資料，以提升行政效能，同時保護民眾個人資料不致外洩，實有賴每一位服務於公部門之人員共同努力；機關應持續推動資安宣導與教育訓練，使同仁明確認知對於公務機密及個人資料的保護不僅是法律義務，更是維繫政府公信力與保障人民基本權利的重要基礎。

返回目錄頁



案例 8：幫忙查一下，傷人又害己

➢案情概述

甲為某機關醫事人員，基於私人因素，拜託擁有系統權限之同事乙，協助查詢民眾丙之醫療資料，乙查詢後將其所知悉之病歷資料回覆甲，甲又告知其友人丁，嗣後丙輾轉得知自己個資外洩，遂向機關提出檢舉。

甲、乙的行為係犯《刑法》第 132 條第 1 項洩漏國防以外秘密罪、《個人資料保護法》第 6 條、第 41 條及第 44 條之公務員假借職務上機會蒐集、利用個人資料罪，經檢察官偵查終結，予以緩起訴處分，並應分別繳交新臺幣(下同)8 萬元、3 萬元不等之緩起訴處分金，另經考績委員會核予 2 人各申誡 1 次處分。

➢風險評估

❶法紀觀念薄弱

病歷資料涉及病患個人隱私，病患隱私權是人格權的一部分，《醫療法》、《護理人員法》、《刑法》妨害秘密及瀆職罪章、《個人資料保護法》等，都有與醫療隱私保護相關之規範，從事相關業務應特別注意，避免一時不察而不慎觸法。本案乙幫忙甲查詢民眾丙不願予他人知悉的病情及醫療內容，且甲得知後又將此事告知丁，足見相關法律觀念均待加強。

❷受人請託查詢

實務上常見基於人情請託或同事情誼，透過各種理由，委請不知情同仁代為查詢資料，藉此方式違法取得、利用

他人資料，衍生違法洩密，損及民眾權益，更破壞政府公信力。

❸事後查核不足

同仁因公務需要使用系統權限及作業功能，系統均保有相關紀錄，以利事後查核；惟倘相關作業規範及查核監督機制不足，又未落實系統端及使用者端之資安稽核作業，恐導致使用者心存僥倖，因此降低對於業務持有之公務機密與個資保護之敏感度。

➢防制措施

❶加強法紀教育宣導

持續辦理專案或例行性宣導，以利同仁明確瞭解執行公務應保密資料之範圍、處理及利用，並重視資訊系統使用規範之教育訓練，使同仁知悉查詢及運用相關資訊，應限於公務目的始可為之，以防止資訊不當使用或外洩情事。

❷強化資料查調稽核

機關應加強執行核心業務系統之資安稽核，檢視系統防火牆、帳號密碼管理使用情形，並針對重點項目進行稽核。透過清查統計異常查詢資料，確實執行抽檢作業，將查詢次數或資料異常者進行列管，以杜絕使用者僥倖心態。

❸落實帳號權限管理

實務上不乏利用不知情之同事代查，故應落實帳號權限管理機制，對於涉嫌不當查詢之員工予以調離現職、取消系統查詢權限等措施，並刪除離(調)人員之查詢權限，加強後續工作追蹤管考。

➢參考法令

- 刑法第 132 條第 1 項。
- 個人資料保護法第 6 條、第 41 條及第 44 條。

溫馨提醒

因為好心協助他人查詢個人資料等機敏資訊，即使非主動發起，也可能因此構成違規或違法；另各級主管應主動關懷同仁平時人際關係、生活習慣及財務狀況，提醒同仁切勿輕忽公私界線，以達到機先預防之目的。

返回目錄頁

肆、資料外洩態樣

案例 9：PO 文一秒鐘，個資永流通

➢案情概述

A 係某機關技術人員，為向朋友炫耀工作內容，遂將某業務系統螢幕畫面(內含民眾姓名)予以拍照截圖，並分享至個人社群媒體。

嗣經友人提醒，A 隨即刪除貼文資料，機關知悉後移送考績委員會追究行政責任，並加強考核。

➢風險評估

❶未遵守辦公紀律

公務員不宜於上班時間或以公家電腦上網連結臉書等社交網站，從事與執行職務無關之網路行為。本案 A 未經機關允許，任意於社群媒體發布因職務而取得之照片，並於辦公時間從事與公務無關之行為，未遵守辦公紀律。

❷未落實保密義務

現今資訊傳遞的速度超乎想像，公務員若因一時疏忽而洩漏公務機密，往往造成不可預測的嚴重後果。本案 A 因疏於注意，為一己之私，而將執行公務所知悉之資料拍照上傳至社群媒體，雖然即時刪除，其行為仍有違失及涉刑責之虞，保密警覺之觀念仍待加強。

➢防制措施

❶公務機密教育訓練

保密係公務員應盡義務之一，機關應針對同仁進行公務機密教育訓練及宣導，以利同仁明確瞭解公務機密之範

疇及法律責任；另身為公務員必須養成良好的保密習慣，在日常生活言行及處理公務機密事務方面，隨時提高警覺，才能有效避免洩密違規情事之發生。

❷落實人員關懷考核

單位主管應關懷瞭解屬員工作狀況及平日交往，注意屬員品德操守，掌握其工作狀況，嚴格要求辦公時間勿處理個人私務。

➢參考法令

- 公務員服務法第 1 條、第 5 條第 1 項。
- 個人資料保護法第 6 條。

溫馨提醒

公務員能否落實保密義務，攸關國家利益之維護、政策推動之順遂及民眾權益之保障，因此，每一位公務機關內之成員，都應該將維護公務機密視為最重要的工作之一，嚴守文書、通訊、資訊、會議等各項機密作為，避免因一時大意而造成不良之嚴重後果。

返回目錄頁

案例 10：舉報變受害，正義反遭殃

➢案情概述

甲為某縣市政府衛生局食品藥物管理科技正，與某藥局負責人乙頗有私交，經常聚餐飲酒。某日民眾丙向甲檢舉乙販售未經醫師開立之處方箋藥物，甲得知後竟向乙通風報信稽查資訊，致該檢舉案件查無具體違法事證，不了了之；又乙不甘被人檢舉，向甲打探檢舉人丙之身分信息，甲竟予以透漏。

甲的行為係犯《刑法》第 132 條第 1 項洩漏國防以外秘密等罪，經法院審理後，被判處有期徒刑 1 年 8 月。
（參考資料：臺灣高等法院臺南分院 108 年度上訴字第 1029 號刑事判決）

➢風險評估

❶洩漏檢舉內容

檢舉內容、檢舉人身分及行政稽查任務之執行等事項，與國家事務及公共利益攸關，屬中華民國國防以外應秘密之消息，不得任意洩漏予他人。本案甲基於朋友私交，竟洩漏稽查資訊及檢舉人身分予乙知悉，恐對檢舉人之生命及財產安全造成危害。

❷逾越公私分際

公務員執行職務應依法行政，本案中甲接獲丙之檢舉，本應妥慎處理，惟甲不僅未能依法行政，反逾越公私分際，基於情誼而洩漏稽查資訊，導致該檢舉案查無具體違法事證，嚴重怠忽職守，傷害機關公正廉潔形象。

➢防制措施

❶落實保護檢舉人措施

《行政院及所屬各機關處理人民陳情案件要點》第 18 點規定「人民陳情案件有保密之必要者，受理機關應予保密。」; 另《公益揭弊者保護法》自 114 年 7 月 22 日施行，機關受理檢舉或揭弊案件時，應依相關法令落實保密檢舉案件內容及檢舉人保護措施，避免因身分資料洩漏，對檢舉人生命及財產安全造成危害。

❷強化處理陳情案件知能

實務上，時有同仁不慎洩漏檢舉人資料，如於製作公文書時將檢舉人並列於正副本，或於公文附件未適當隱蔽檢舉人姓名、電話或其他足資辨認出檢舉人身分特徵資料。機關應適時辦理檢舉或陳情案件處理之教育訓練，協助員工精進處理相類案件之保密觀念、工作態度及技巧，藉以避免民怨及訟累。

❸定期檢討實施職務輪調

依據行政院《強化行政院及所屬機關（構）公立學校公務員定期遷調參考原則》等規定，各機關對辦理廉政風險業務之職務，應依業務特性訂定職期，每年定期檢討辦理職期屆滿人員之遷調，並落實考核機制，以避免人員久任並與業務往來業者或廠商建立相當交情，進而產生袒護心理，提高濫用職權之風險。

❹辦理廉政倫理規範等法令宣導

公務員廉政倫理規範之目的，係維護政府清廉形象，確保公務員在執行職務時，不受利益衝突或不正當誘惑，

以建立廉潔風氣。規範內容包括限制公務員收受與其職務有利害關係者的餽贈、飲宴應酬、請託關說等，並規範公務員應誠實、公開、公正執行職務。本案公務員甲與業者乙過從甚密，致逾越往來分際而罹於刑責，機關應加強宣導相關廉政法令，使同仁認知彼此身分有別，避免與業者飲宴或公務程序外的活動，以免滋生不必要之困擾。

➢參考法令

- 刑法第 132 條第 1 項。
- 行政程序法第 170 條。
- 行政院及所屬各機關處理人民陳情案件要點第 18 點。
- 強化行政院及所屬機關（構）公立學校公務人員定期遷調參考原則第 3 點。
- 公務員廉政倫理規範第 3 點。

溫馨提醒

為追求廉能政府公益社會，法務部多年來致力於推動揭弊者保護法制，立法院並已於去（113）年 12 月 27 日三讀通過《公益揭弊者保護法》，建立國內首部揭弊保護專法，提供揭弊者安心吹哨的環境，足見「保護檢舉人」之重要；故應提醒同仁不論是揭弊或一般陳情檢舉案件，均應落實檢舉（陳情）人身分保密措施。

返回目錄頁

伍、附錄

一、相關法規

(一)資通安全管理法

(二)個人資料保護法

(三)衛生福利部醫療領域資通系統資安防護基準

(四)衛生福利部基層醫療院所資安防護參考指引(參、區域醫院或地區醫院篇)

(五)醫院面對勒索軟體攻擊的應變指南

(六)公益揭弊者保護法

(七)公務員廉政倫理規範

(八)強化行政院及所屬機關(構)公立學校公務人員定期遷調參考原則

二、摘錄法規

(一)中華民國刑法

(二)醫師法

(三)公務員服務法

(四)行政程序法

(五)行政院及所屬各機關處理人民陳情案件要點

一、相關法規

(一)資通安全管理法

修正日期：114 年 9 月 24 日

第 一 章 總則

第 1 條

為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。

第 2 條

本法之主管機關為數位發展部。

資通安全業務之執行，由數位發展部指定資安專責機關辦理。

第 3 條

本法用詞，定義如下：

一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、資通安全：指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，或其他情形影響其機密性、完整性或可用性。

四、資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全或保護措施失效之狀態發生，影響資通系統機能運作。

五、公務機關：指依法行使公權力之中央、地方機關(構)或公法人。但不包括軍事機關及情報機關。

六、特定非公務機關：指關鍵基礎設施提供者、公營事業、特定財團法人或受政府控制之事業、團體或機構。

七、關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經行政院定期檢視並公告之領域。

八、關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，

經中央目的事業主管機關指定，並報行政院核定者。

九、特定財團法人：指符合財團法人法第二條第二項、第三項或第六十三條第一項、第四項規定之財團法人，並屬該法第二條第八項所定全國性財團法人者。

十、受政府控制之事業、團體或機構：指銓敘部依公務人員退休資遣撫卹法第七十七條第一項第二款第三目及第四目公告之事業、團體或機構，具資通安全重要性，經中央目的事業主管機關指定，並經主管機關核定者；其受地方政府控制者，應經地方主管機關同意後，主管機關始得核定。

十一、危害國家資通安全產品：指經主管機關認定，對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統、服務或產品。

第 4 條

為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：

一、資通安全專業人才之培育。

二、資通安全科技之研發、整合、應用、產學合作及國際交流合作。

三、資通安全產業之發展。

四、資通安全軟硬體技術規範、相關服務及審驗機制之發展。

五、協助民間處理、因應及防範重大資通安全事件。

前項相關事項之推動，由主管機關擬訂國家資通安全發展方案，報請行政院核定後實施。

第 5 條

為落實國家資通安全政策，各政府機關、中央及地方間，應致力配合推動執行國家資通安全措施，共同建構國家資通安全環境。

為辦理國家資通安全政策、應變機制與重大計畫之諮詢審議，協調各政府機關、中央及地方間之資通安全相關事務，行政院應定期召開國家資通安全會報，由行政院院長或副院長擔任召集人，得邀請專家學者及民間團體代表出席，必要時得召開臨時會議，其幕僚作業由主管機關辦理。

前項國家資通安全會報決議事項，相關政府部門應予執行，由主管機關定期追蹤管考，並得辦理績效評核。

第二項國家資通安全會報之組成、任務、議事程序及其他相關事項之辦法，由行政院定之。

第 6 條

主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應每年公布國家資通安全情勢報告、資通安全維護計畫實施情形稽核概況報告及國家資通安全發展方案。

前項情勢報告、實施情形稽核概況報告及國家資通安全發展方案，應由主管機關送立法院備查。

第 7 條

公務機關及特定非公務機關，應按其業務重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，報由主管機關核定或備查其資通安全責任等級。

公務機關及特定非公務機關應符合資通安全責任等級之要求，並自管理、技術、認知及訓練等面向，辦理資通安全防護措施。

前二項資通安全責任等級之區分基準、核定或備查程序、變更申請、資通安全防護措施辦理項目、內容、專職人員之資格條件與配置及其他相關事項之辦法，由主管機關定之。

第 8 條

主管機關得定期或不定期稽核公務機關及特定非公務機關之資通安全維護計畫實施情形。

前項稽核後，發現受稽核機關資通安全維護計畫實施情形有缺失或待改善者，受稽核機關應提出改善報告，公務機關送交依第十四條規定收受其實施情形之機關、特定非公務機關送交中央目的事業主管機關審查後，由該審查機關送交主管機關。

前項收受改善報告之機關認有必要時，得要求受稽核機關進行說明或調整。

前三項資通安全維護計畫實施情形之稽核頻率、內容與方法、改善報告之提出及其他相關事項之辦法，由主管機關定之。

第一項稽核由主管機關擬訂年度計畫，報請行政院核定後辦理，年度計畫及年度成果報告應送交國家資通安全會報備查。

第 9 條

主管機關應建立資通安全情資分享機制。

前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。

第 10 條

公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應選任適當之受託者，要求受託者建立有效之資通安全管理機制，並監督該機制之實施。

前項受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過公正第三方驗證。

公務機關或特定非公務機關辦理第一項委外業務，應與受託者簽訂書面契約，載明雙方之權利義務及違約責任。

公務機關及特定非公務機關，應配合主管機關之規劃辦理資通安全演練作業，並視需要導入第三方協力機制；演練內容及其他相關事項，由主管機關定之。

第 二 章 公務機關資通安全管理

第 11 條

公務機關不得下載、安裝或使用危害國家資通安全產品；其自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時，亦同。但因業務需求且無其他替代方案者，經該機關資通安全長及依第十四條規定收受其實施情形之機關資通安全長核可，函報主管機關核定後，得以專案方式使用，並列冊管理。

公務機關發配供業務使用之資通訊設備，不得下載、安裝或使用危害國家資通安全產品，並應遵守相關法令規範。但因業務需求且無其他替代方案者，準用前項但書規定辦理。

前二項有關危害國家資通安全產品之審查程序、風險評估、情資分享、使用限制及其他相關事項之辦法，由主管機關會商有關機關擬訂，報請行政院核定之。

第 12 條

公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。

第 13 條

公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

第 14 條

公務機關應每年向上級機關或監督機關提出資通安全維護計畫實施情形；無上級機關或監督機關者，其資通安全維護計畫實施情形

應依下列各款規定辦理：

一、總統府、國家安全會議及五院，向主管機關提出。

二、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會，向主管機關提出。

三、直轄市山地原住民區公所、直轄市山地原住民區民代表會，向直轄市政府提出；鄉（鎮、市）公所、鄉（鎮、市）民代表會，向縣政府提出。

第 15 條

公務機關應稽核其所屬、所監督之公務機關、所轄鄉（鎮、市）公所、直轄市山地原住民區公所及鄉（鎮、市）民代表會、直轄市山地原住民區民代表會之資通安全維護計畫實施情形。

第 16 條

受稽核機關之資通安全維護計畫實施情形有缺失或待改善者，應向稽核機關提出改善報告，並由稽核機關連同稽核結果依指定之方式送交主管機關。

稽核機關或主管機關認有必要時，得要求受稽核機關進行說明或調整。

前三條及第一項資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、結果之交付、改善報告之提出及其他相關事項之辦法，由主管機關定之。

第 17 條

公務機關為因應資通安全事件，應訂定通報及應變機制。

公務機關知悉資通安全事件時，應向第十四條規定收受其實施情形之機關及主管機關通報。

公務機關應向前項受通報機關提出資通安全事件調查、處理及改善報告。

前三項通報與應變機制之必要事項、通報內容、報告之提出、演練作業及其他相關事項之辦法，由主管機關定之。

第二項受通報機關知悉重大資通安全事件時，得提供公務機關相關協助；於適當時機並得公告與事件相關之必要內容及因應措施。

第 18 條

公務機關應符合其資通安全責任等級之要求，設置資通安全專職人員，辦理資通安全業務及應變處理；所屬人員辦理資通安全業務績效優良者，應予獎勵。

主管機關應妥善規劃推動專職人員之職能訓練，增進其資通安全專業知能；遇有重大資通安全事件，主管機關得調度各級機關資通安全人員支援之。

前二項人員獎勵、職能訓練、調度支援、績效評核及其他相關事項之辦法，由主管機關定之。

第 19 條

公務機關於必要時，得對所屬資通安全專職人員之適任性進行查核。

主管機關得於資通安全人員任用考試榜示後，對錄取人員之適任性進行查核。

拒絕查核或前二項查核結果經用人機關認定未通過者，不得辦理涉及國家機密、軍事機密及國防秘密之資通安全業務。

前項人員職務得由用人機關基於內部管理及業務運作需要，依法進行調整。

第一項及第二項查核紀錄，由用人機關依相關規定保密處理，並妥為保管，不得移作他用；違反者，視情節予以議處。

有關查核權責機關、應受查核人員、查核程序、內容及其他相關事項之辦法，由主管機關會商有關機關定之。

第 三 章 特定非公務機關資通安全管理

第 20 條

中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，送由主管機關報請行政院核定，並以書面通知受核定者。

關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，設置資通安全專職人員，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。

中央目的事業主管機關應綜合考量所管關鍵基礎設施提供者業務之重要性與機敏性、資通系統之規模、性質、資通安全事件發生之頻率、程度及其他與資通安全相關之因素，定期稽核其資通安全維護計畫之實施情形。

關鍵基礎設施提供者之資通安全維護計畫實施情形有缺失或待

改善者，應向中央目的事業主管機關提出改善報告。

中央目的事業主管機關應依指定之方式將稽核結果及改善報告送交主管機關。

第 21 條

關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，設置資通安全專職人員，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

中央目的事業主管機關得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。

中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。

中央目的事業主管機關應依指定之方式將稽核結果及改善報告送交主管機關。

第 22 條

前二條資通安全維護計畫之必要事項、實施情形之提出、稽核之頻率、內容與方法、結果之交付、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報由主管機關核定。

第 23 條

特定非公務機關應置資通安全長，由特定非公務機關之代表人、管理人、其他有代表權人或其指派之適當人員擔任，負責推動及監督機關內資通安全相關事務。

第 24 條

特定非公務機關為因應資通安全事件，應訂定通報及應變機制。

特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。

特定非公務機關應向中央目的事業主管機關提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。

前三項通報與應變機制之必要事項、通報內容、報告之提出、送交、演練作業及其他應遵行事項之辦法，由主管機關定之。

中央目的事業主管機關或主管機關知悉重大資通安全事件時，應提供必要之協助；於適當時機並得公告與事件相關之必要內容及因應

措施。

第 25 條

中央目的事業主管機關為調查特定非公務機關發生之重大資通安全事件，得依下列程序辦理：

一、通知當事人或關係人到場陳述意見。

二、通知當事人及關係人提出獨立第三方機構出具之鑑識或調查報告。

三、派員、委任或委託其他機關（構）前往當事人及關係人之處所實施必要之檢查。

前項所定關係人，以該項特定非公務機關委託辦理資通系統之建置、維運或資通服務提供之受託者，且與重大資通安全事件相關者為限。

當事人或關係人對於中央目的事業主管機關依第一項所為之調查，不得規避、妨礙或拒絕。

執行調查之人員應出示有關執行職務之證明文件；其未出示者，受調查者得拒絕之。

第一項第三款受委任或委託之機關（構）對於辦理受任或受託事務所獲悉特定非公務機關之秘密，不得洩漏。

第 26 條

特定非公務機關對於所屬人員辦理資通安全業務績效優良者，應予獎勵。

第 27 條

中央目的事業主管機關對特定非公務機關下載、安裝或使用危害國家資通安全產品，得予以限制或禁止；特定非公務機關自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時，亦同。但因業務需求且無其他替代方案者，經該特定非公務機關資通安全長核可，函報中央目的事業主管機關核定後，得以專案方式使用，並列冊管理。

前項對特定非公務機關限制或禁止使用危害國家資通安全產品之管控措施，由中央目的事業主管機關訂定，報主管機關備查。

第 四 章 罰則

第 28 條

公務機關所屬人員未依本法規定辦理者，應按其情節輕重，依相關規定予以懲戒或懲處。

前項懲處事項之辦法，由主管機關定之。

特定非公務機關所屬人員未依本法規定辦理，情節重大者，由特定非公務機關依規定予以懲處。

第 29 條

特定非公務機關未依第二十四條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上一千萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。

第 30 條

特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上五百萬元以下罰鍰：

一、未依第二十條第二項或第二十一條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第二十二條所定辦法中有關資通安全維護計畫必要事項之規定。

二、未依第二十條第三項或第二十一條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第二十二條所定辦法中有關資通安全維護計畫實施情形提出之規定。

三、未依第八條第二項、第二十條第五項或第二十一條第三項規定，提出改善報告送交中央目的事業主管機關，或違反第二十二條所定辦法中有關改善報告提出之規定。

四、未依第二十四條第一項規定，訂定資通安全事件之通報及應變機制，或違反第二十四條第四項所定辦法中有關通報及應變機制必要事項之規定。

五、未依第二十四條第三項規定，向中央目的事業主管機關提出或向主管機關送交資通安全事件之調查、處理及改善報告，或違反第二十四條第四項所定辦法中有關報告提出、送交之規定。

六、違反第二十四條第四項所定辦法中有關通報內容、演練作業之規定。

第 31 條

違反第二十五條第三項規定，規避、妨礙或拒絕調查者，由中央目的事業主管機關處新臺幣十萬元以上一百萬元以下罰鍰。

第 五 章 附則

第 32 條

主管機關得委託其他公務機關、法人或團體，辦理資通安全整體

防護、演練、稽核、國際交流合作及其他資通安全相關事務。

前項受委託之公務機關、法人或團體，不得洩露辦理相關事務過程中所知悉之秘密。

特定非公務機關之業務涉及數個中央目的事業主管機關之權責，主管機關得協調指定其中一個或數個中央目的事業主管機關，單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。

第 33 條

本法所定資通安全事件，涉及個人資料外洩時，公務機關及特定非公務機關應另依個人資料保護法及其相關法令規定辦理。

第 34 條

本法施行細則，由主管機關定之。

第 35 條

本法施行日期，由行政院定之。

(二)個人資料保護法

修正日期：112 年 5 月 31 日

第一章 總則

第 1 條

為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促 進個人資料之合理利用，特制定本法。

第1-1條

本法之主管機關為個人資料保護委員會。

自個人資料保護委員會成立之日起，本法所列屬中央目的事業主管機關、直轄市、縣（市）政府及第五十三條、第五十五條所列機關之權責事項，由該會管轄。

第 2 條

本法用詞，定義如下：

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、蒐集：指以任何方式取得個人資料。

四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、公務機關：指依法行使公權力之中央或地方機關或行政法人。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。

第 3 條

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一、查詢或請求閱覽。
二、請求製給複製本。
三、請求補充或更正。
四、請求停止蒐集、處理或利用。
五、請求刪除。

第 4 條

受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。

第 5 條

個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

第 6 條

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一、法律明文規定。
二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

第 7 條

第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。

第十六條第七款、第二十條第一項第六款所稱同意，指當事人經

蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。

公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。

蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

第 8 條

公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公務機關或非公務機關名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依第三條規定得行使之權利及方式。

六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

有下列情形之一者，得免為前項之告知：

一、依法律規定得免告知。

二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

三、告知將妨害公務機關執行法定職務。

四、告知將妨害公共利益。

五、當事人明知應告知之內容。

六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

第 9 條

公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。

有下列情形之一者，得免為前項之告知：

一、有前條第二項所列各款情形之一。

二、當事人自行公開或其他已合法公開之個人資料。

三、不能向當事人或其法定代理人為告知。

四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

第一項之告知，得於首次對當事人為利用時併同為之。

第 10 條

公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

二、妨害公務機關執行法定職務。

三、妨害該蒐集機關或第三人之重大利益。

第 11 條

公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。

個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。

個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第 12 條

公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

第 13 條

公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

第 14 條

查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。

第 二 章 公務機關對個人資料之蒐集、處理及利用

第 15 條

公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、執行法定職務必要範圍內。

二、經當事人同意。

三、對當事人權益無侵害。

第 16 條

公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：

一、法律明文規定。

二、為維護國家安全或增進公共利益所必要。

三、為免除當事人之生命、身體、自由或財產上之危險。

四、為防止他人權益之重大危害。

五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

六、有利於當事人權益。

七、經當事人同意。

第 17 條

公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：

一、個人資料檔案名稱。

二、保有機關名稱及聯絡方式。

三、個人資料檔案保有之依據及特定目的。

四、個人資料之類別。

第 18 條

公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第 三 章 非公務機關對個人資料之蒐集、處理及利用

第 19 條

非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、法律明文規定。

二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五、經當事人同意。

六、為增進公共利益所必要。

七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

八、對當事人權益無侵害。

蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

第 20 條

非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

一、法律明文規定。

二、為增進公共利益所必要。

三、為免除當事人之生命、身體、自由或財產上之危險。

四、為防止他人權益之重大危害。

五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

六、經當事人同意。

七、有利於當事人權益。

非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

第 21 條

非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：

一、涉及國家重大利益。

二、國際條約或協定有特別規定。

三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。

四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。

第 22 條

中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。

中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

中央目的事業主管機關或直轄市、縣(市)政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之。

對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。

參與檢查之人員，因檢查而知悉他人資料者，負保密義務。

第 23 條

對於前條第二項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。

扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。

第 24 條

非公務機關、物之所有人、持有人、保管人或利害關係人對前二條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣（市）政府聲明異議。

前項聲明異議，中央目的事業主管機關或直轄市、縣（市）政府

認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。

對於中央目的事業主管機關或直轄市、縣（市）政府前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行為逕行提起行政訴訟。

第 25 條

非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分：

一、禁止蒐集、處理或利用個人資料。

二、命令刪除經處理之個人資料檔案。

三、沒入或命銷燬違法蒐集之個人資料。

四、公布非公務機關之違法情形，及其姓名或名稱與負責人。

中央目的事業主管機關或直轄市、縣（市）政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法為之。

第 26 條

中央目的事業主管機關或直轄市、縣（市）政府依第二十二條規定檢查後，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。

第 27 條

非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

第 四 章 損害賠償及團體訴訟

第 28 條

公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。

對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。

同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。

第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

第 29 條

非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。

依前項規定請求賠償者，適用前條第二項至第六項規定。

第 30 條

損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。

第 31 條

損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。

第 32 條

依本章規定提起訴訟之財團法人或公益社團法人，應符合下列要件：

一、財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。

二、保護個人資料事項於其章程所定目的範圍內。

三、許可設立三年以上。

第 33 條

依本法規定對於公務機關提起損害賠償訴訟者，專屬該機關所在地之地方法院管轄。對於非公務機關提起者，專屬其主事務所、主營業所或住所地之地方法院管轄。

前項非公務機關為自然人，而其在中華民國現無住所或住所不明

者，以其在中華民國之居所，視為其住所；無居所或居所不明者，以其在中華民國最後之住所，視為其住所；無最後住所者，專屬中央政府所在地之地方法院管轄。

第一項非公務機關為自然人以外之法人或其他團體，而其在中華民國現無主事務所、主營業所或主事務所、主營業所不明者，專屬中央政府所在地之地方法院管轄。

第 34 條

對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。

前項訴訟，法院得依聲請或依職權公告曉示其他因同一原因事實受有損害之當事人，得於一定期間內向前項起訴之財團法人或公益社團法人授與訴訟實施權，由該財團法人或公益社團法人於第一審言詞辯論終結前，擴張應受判決事項之聲明。

其他因同一原因事實受有損害之當事人未依前項規定授與訴訟實施權者，亦得於法院公告曉示之一定期間內起訴，由法院併案審理。

其他因同一原因事實受有損害之當事人，亦得聲請法院為前項之公告。

前二項公告，應揭示於法院公告處、資訊網路及其他適當處所；法院認為必要時，並得命登載於公報或新聞紙，或用其他方法公告之，其費用由國庫墊付。

依第一項規定提起訴訟之財團法人或公益社團法人，其標的價額超過新臺幣六十萬元者，超過部分暫免徵裁判費。

第 35 條

當事人依前條第一項規定撤回訴訟實施權之授與者，該部分訴訟程序當然停止，該當事人應即聲明承受訴訟，法院亦得依職權命該當事人承受訴訟。

財團法人或公益社團法人依前條規定起訴後，因部分當事人撤回訴訟實施權之授與，致其餘部分不足二十人者，仍得就其餘部分繼續進行訴訟。

第 36 條

各當事人於第三十四條第一項及第二項之損害賠償請求權，其時效應分別計算。

第 37 條

財團法人或公益社團法人就當事人授與訴訟實施權之事件，有為一切訴訟行為之權。但當事人得限制其為捨棄、撤回或和解。

前項當事人中一人所為之限制，其效力不及於其他當事人。

第一項之限制，應於第三十四條第一項之文書內表明，或以書狀提出於法院。

第 38 條

當事人對於第三十四條訴訟之判決不服者，得於財團法人或公益社團法人上訴期間屆滿前，撤回訴訟實施權之授與，依法提起上訴。

財團法人或公益社團法人於收受判決書正本後，應即將其結果通知當事人，並應於七日內將是否提起上訴之意旨以書面通知當事人。

第 39 條

財團法人或公益社團法人應將第三十四條訴訟結果所得之賠償，扣除訴訟必要費用後，分別交付授與訴訟實施權之當事人。

提起第三十四條第一項訴訟之財團法人或公益社團法人，均不得請求報酬。

第 40 條

依本章規定提起訴訟之財團法人或公益社團法人，應委任律師代理訴訟。

第 五 章 罰則

第 41 條

意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。

第 42 條

意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。

第 43 條

中華民國人民在中華民國領域外對中華民國人民犯前二條之罪者，亦適用之。

第 44 條

公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

第 45 條

本章之罪，須告訴乃論。但犯第四十一條之罪者，或對公務機關犯第四十二條之罪者，不在此限。

第 46 條

犯本章之罪，其他法律有較重處罰規定者，從其規定。

第 47 條

非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：

一、違反第六條第一項規定。

二、違反第十九條規定。

三、違反第二十條第一項規定。

四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。

第 48 條

非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：

一、違反第八條或第九條規定。

二、違反第十條、第十一條、第十二條或第十三條規定。

三、違反第二十條第二項或第三項規定。

非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰。

非公務機關違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，其情節重大者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣十五萬元以上一千五百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處罰。

第 49 條

非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰。

第 50 條

非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

第 六 章 附則

第 51 條

有下列情形之一者，不適用本法規定：

一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。

第 52 條

第二十二條至第二十六條規定由中央目的事業主管機關或直轄市、縣（市）政府執行之權限，得委任所屬機關、委託其他機關或公益團體辦理；其成員因執行委任或委託事務所知悉之資訊，負保密義務。

前項之公益團體，不得依第三十四條第一項規定接受當事人授與訴訟實施權，以自己之名義提起損害賠償訴訟。

第 53 條

法務部應會同中央目的事業主管機關訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用。

第 54 條

本法中華民國九十九年五月二十六日修正公布之條文施行前，非由當事人提供之個人資料，於本法一百零四年十二月十五日修正之條文施行後為處理或利用者，應於處理或利用前，依第九條規定向當事人告知。

前項之告知，得於本法中華民國一百零四年十二月十五日修正之條文施行後首次利用時併同為之。

未依前二項規定告知而利用者，以違反第九條規定論處。

第 55 條

本法施行細則，由法務部定之。

第 56 條

本法施行日期，由行政院定之。

本法中華民國九十九年五月二十六日修正公布之現行條文第十九條至第二十二條、第四十三條之刪除及一百十二年五月十六日修正之第四十八條，自公布日施行。

(三)衛生福利部醫療領域資通系統資安防護基準

一、依據

衛生福利部(以下簡稱本部)為資通安全管理法醫療領域特定非公務機關之中央目的事業主管機關，就該特定領域類型資通系統有另為規定防護基準之必要，爰依資通安全責任等級分級辦法第11條第2項後段規定，訂定本防護基準，供醫院資通系統實施各項資安防護控制措施之依循。

二、適用範圍

本防護基準適用範圍為依資通安全管理法受本部轄管之醫療領域之特定非公務機關。

醫療儀器資通系統與其他支援設施資通系統應依循機關之資安維護計畫，涉及相關組織及委外管理等要項，須依循機關之資安管理框架。

三、用詞定義：

(一)資安列管醫療儀器：指放置院區內場域，有對外連線網際網路（Internet）或連結院內系統網路(Intranet)，或具網路位址(IP)追蹤性，或交換資料間接上傳醫療相關資訊系統(如:PACS、HIS)等之臨床使用醫療終端儀器及控制系統。

(二)醫療資訊系統(Healthcare Information System,HIS)：指傳統醫療資訊業務管轄之臨床資訊應用系統，包含資料庫及後端處理臨床表單之系統。

(三)醫療影像儲傳系統(Picture archiving and communication system,PACS)：包含 OT 之影像擷取組像及上傳元件端與 IT 之醫療影像傳輸儲存及調閱系統端二部份；元件端，為具醫療數位影像傳輸協定(DICOM Module)醫療儀器的集合，系統端，含醫師醫囑項目與照攝影像及報告資訊。

(四)醫療儀器資通系統：泛指資安列管醫療儀器之控制系統分群、終端儀器分群之邊界主機，參考「醫療儀器資安分群分類模型」範圍。

(五)醫療物聯網裝置（The Internet of Medical Things,IoMT）：泛指藉由物聯網(The Internet of Things,IoT) 技術進行資料蒐集或傳輸之設備。

(六)邊界主機：指管理獨立網域內網(Local LAN)運作之儀器群組主機，並隔離介接院內系統網路(Intranet)之具網路區隔功能閘道器或伺服主機(如:雙網卡 Edge Gateway 或 Device Server)。

(七)儀器獨立網域內網(Local LAN)：指儀器群組(為：「群組型儀器」或「系統型儀器」)依儀器原廠建議或工控區(OT Zone)資安防護目的，所規劃及佈建的獨立網域內網，以確保穩定性、安全性需求；或稱「設備內網」、「內內網」。

(八)儀器獨立網段：指院內系統網路(Intranet)網域，分割隔離網段後，規劃獨立於行政電腦網段外，專屬予醫療儀器運行使用之網段。

(九)OT防火牆:對比於資通區(IT Zone)介接網際網路(Internet)的「醫院外部防火牆」名詞，指醫院內部「資安列管類醫療儀器」分區佈建後，介接院內系統網路(Intranet)的醫療儀器跨區防火牆。

四、醫療儀器資安分群分類

(一)機關盤點具連網功能的醫療儀器資產，應涵蓋「資安列管醫療儀器」之範圍。

(二)「資安列管醫療儀器」依「元件」與「系統」資料流之從屬關係特性，作為「分群」依循，為「終端儀器」與「控制系統」二群；依資料流來源至目的 IP 之跨區軌跡，作為「分類」依循，二群分五類；透過「醫療儀器資安分群分類模型」模型化分群分類，防護標的實施普、中、高分級的控制措施項目。

(三)終端儀器群：指臨床上使用之醫療儀器，經連結院內系統網路(Intranet)傳輸資料之儀器設備或醫療儀器，包含三類:「終端單機」、「群組型儀器」及「系統型儀器」。

1.終端單機：指臨床使用直接連結院內系統網路(Intranet)傳輸資料至資通區(IT Zone)中繼邊界 Gateway 之單機型醫療儀器。如：超音波影像儀為單機型醫療儀器，傳輸資料連結 PACS 系統之工作清單 Gateway、DICOM 影像 Gateway。

2.群組型儀器：指多台功能相同之醫療儀器組成獨立網域內網(Local LAN)，透過隔離措施間接進行單機院內系統網

路(Intranet)連線之「內網邊界主機」。如：ICU 生理監視器群組的中央站、內網化連網洗腎機群組的邊界主機(Edge Loader Gateway)。

3. 系統型儀器：指由不同功能模組單機在獨立網域內網(Local LAN)組合而成一套醫療儀器，透過隔離措施間接進行單機院內系統網路(Intranet)連線之內網邊界主機；或指使用於臨床獨立網域內網(Local LAN)，多台功能不相同模組單機組合而成一套醫療儀器的「邊界主機」，經隔離間接連結院內系統網路(Intranet)。如：MRI、CT、PET 連結 PACS 系統的介面控制台 console。

(四)控制系統群：指規格上可連線管理2台(含)以上「終端儀器」群之終端單機或邊界主機，連結院內系統網路(Intranet)傳輸資料之臨床儀器控制系統，包含「醫儀控制系統」與「醫儀應用系統」二類。

1. 醫儀控制系統：全稱為「醫療儀器資訊控制系統」，指控制「終端儀器」非人類連線的管理系統(Device Server)；只管理「儀器ID」及「檢驗檢查資料」；不落地儲存與醫療相關資訊系統交換的「可識別資料」、不管理資料查詢的「醫事人員帳密權控」；功能上不涉及識別個人資訊的控制軟體系統。如：ICU 生理監護系統伺服器主機、洗腎機拋轉系統設備伺服器的控制軟體系統。

2. 醫儀應用系統：全稱為「醫療儀器資訊應用系統」，指「終端儀器」的控制應用管理系統(AP Server)；包含交換且儲存 HIS 病人個資資訊、提供臨床人員查詢報告等服務，有管理醫事人員帳密權控等可識別資訊的儀器控制及連結臨床應用套裝軟體系統。如：產房資訊系統、檢驗備管系統伺服器的應用軟體系統。

五、機關資通系統適用規定

(一)機關自行或委外開發之資通系統，應依「資通安全責任等級分級辦法」第11條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，並依附表十所定資通系統防護基準執行控制措施。

(二)醫療儀器應符合「醫療器材管理法」及相關子法與「醫療器材品質管理系統準則」之衛生福利部許可證相關安規驗證規

定;另「資安列管醫療儀器」終端儀器群邊界主機與控制系統群為醫療儀器資通系統防護基準之防護標的，應依本防護基準附表一執行控制措施。

(三)其他支援設施之特定類型資通系統，執行「資通安全責任等級分級辦法」第11條附表十所定控制措施，因技術限制、系統設計、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，得參考其他領域公告之相關資通或工控系統之控制措施。

六、醫療儀器資料流管理

(一)「資安列管醫療儀器」分群分類之醫療儀器，依資安風險區劃 ZCR方法，評估分區「防護需求等級(SL)」、規劃「網路安全區塊(Zone)」分區、建立跨區資料傳輸「安全管道(Conduit)」；ZCR 網路規劃參考公用之醫療儀器資料流網路模板(Template)。

(二)資安風險區劃(Zone, conduit and risk assessment, ZCR)：「資安列管醫療儀器」分群分類之醫療資料流，依評估資安需求等級SL(Security Level)規劃建立「網路安全區塊(Zone)」分區；跨區管道(Conduit)佈建資料流通道之過濾阻擋「控制項」防護機制，達到：受攻擊面縮小(Attack Surface Reduction)、縱深防禦(Defense in Depth)等防護效果之資安風險管理實作流程。

(三)資安防護需求等級(Security Level,SL)：針對「控制系統」依據資通系統防護需求分級原則，評估機密性(C)、完整性(I)、可用性(A)、法遵性(L)各構面之分級取最高等級者，評估「資產價值」，評定普、中、高之「資安防護需求等級」，簡稱SL(Security Level)；SL 由低至高分級為 SL(0)~SL(4)對應資安防護需求普、中、高等級。

1.SL(0)：指「信任連線」。

2.SL(1)~ SL(2)：資安防護需求等級普級。

3.SL(3)為：資安防護需求等級中級。

4.SL(4)為：資安防護需求等級高級。

(四)信任連線：指經風險評鑑後，風險可承受範圍內的短距離機器連線資料傳輸；對應防護需求等級為 SL(O)；安全(Safety)議題另受醫療法規「醫療器材管理法」規範。

(五)網路安全區塊(Zone)：指「資安列管醫療儀器」之建置，網路規劃上的資料流資安防護需求分區，可分「網際網路(Internet)」、「院內系統網路(Intranet)」、「工控區(OT Zone)」、「信任連線」區塊(包含:儀器獨立網域內網(Local LAN)、RS232連線、藍芽、RF、IR...等低風險短距連線)。每一區塊，透過資安風險評估資安防護需求等級(SL)，每一資安風險區塊(Zone)內之資安列管儀器列為相同 SL；「子區塊」之 SL≦「母區塊」。

(六)管道(Conduit)：泛指跨「網路安全區塊(Zone)」之間，經套用對應跨區等級「控制項」防護機制(如：資料流經隔離、清洗、阻擋)後，之安全資料傳輸通道。

七、醫療儀器資通系統資安風險評估與檢討改善

(一)本防護基準「醫療儀器資料流網路模版」，提供機關確認「終端儀器群」與「控制系統群」之醫療資訊資料流、清查連網方式、連網儀器及所介接系統，依分區完成資安風險評估，並執行對應控制措施。

(二)資產風險改善

在套用「控制措施」後，依據可能發生的外部事件影響風險構面，每年針對「資安列管儀器」，經選擇適用規範之「風險識別」、「風險分析」與「衝擊分析」等風險評估工具與方法論，逐年檢討「資安風險等級(Cyber Risk Level,CRL)」之低、中、高等級，改善資安風險。

1.高：不可接受(Unacceptable)。

2.中：可能接受的(Potentially Acceptable)。

3.低：可接受的(Acceptable)。

八、實作指引

為協助機關落實本防護基準，逐年完備機關之醫療儀器資安防護控制措施，由本部另行公告「醫療儀器資通系統資安防護作業實作指引」，供醫院導入實務運作參考。

(四)衛生福利部基層醫療院所資安防護參考指引 (參、區域醫院或地區醫院篇)

訂定日期：109 年 8 月 17 日

有資訊專屬人員但沒有專屬資安人力資源配置的區域醫院或地區醫院屬之。通常在沒有專屬資安人員配置及有限的資訊預算下，資安預算通常與資通訊需求合併運用，故資安相關需求大多直接委外由資訊廠商統合處理。對於非「資通安全管理法」規範對象之區域醫院或地區醫院內的資訊安全措施，建議可以如下指引自我檢核與改善執行：

一、醫療/醫務專屬使用設備

建議醫療/醫務使用之設備需與其他用途之設備區隔，並應定期盤點、造冊列管以維持最新狀態。

二、電腦須安裝防毒軟體並隨時更新作業系統

許多的惡意攻擊程式是透過作業系統的漏洞滲透執行。所以過舊的電腦及作業系統須儘速汰換，並應安裝合法的防毒軟體，或至少更新至Windows 10 並開啟內建之 Windows defender 進行防護。

三、強化內部基層及管理人員資安意識

1.資安教育訓練:

(1)每年應安排資安教育訓練，建議時數如下:

①主管及一般人員：3 小時

②資訊人員：每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練。

(2)每年定期辦理資安教育訓練，請一般同仁與主管務必參加，以提昇資訊安全認知及相關技能。

2.建議於電腦的明顯處提醒 USB 限用機制，也可以友善提醒資安宣導標語。例如以下：

資安守則最重要；權限控管要確實。

密碼外洩風險高；定期更改才安全。

機密資料慎處理；個人資料要保密。

不明軟體勿下載；駭客入侵機會少。

網路安全要規範；資安檢核要精實。

四、加強委外廠商管理

1.委外廠商須充份了解資訊安全對醫療院所之重要性，建議於委外廠商簽訂合約時，合約內容應新增/包含資安條款要求。

2.委外廠商使用 USB 存取診所裝置時，須由最新版之防毒軟體進行掃描，並將掃描結果及時間目的進行登載。

五、落實網路隔離

1.獨立使用連結健保署 VPN 之電腦，與任何連結形式之網際網路區隔，如：有線網路連結、無線網路連結及透過手機上網連結。

2.避免透過遠端連線之方式來維護醫院連結中央醫療體系專用VPN的電腦。

3.供民眾使用或內部員工使用之 Wifi 應與內部作業電腦網段進行隔離。

六、強化 IoT 設備管理

要求維護廠商將相關 IoT 設備(如：監視器、門禁、事務機、醫療設備...等)之韌體更新至最新版本。

七、落實設備預設帳號密碼並使用較強的密碼規則

1.至少 8 個字元以上；

2.混合字母大小寫、數字及特殊符號，任選三種。

3.避免和使用者帳號相同；避免使用有意義之單字。

4.避免使用相同密碼於不同網站。

5.定期變更密碼。

八、設備報廢/再利用之管制

設備及媒體報廢或改為其他用途時，應檢查其內容是否包含敏感資訊，確認其內容已被適當的處理後(格式化、刪除內容或實體銷毀) ，方可移交至相關人員作後續處理。

所有銷毀/報廢的電子設備應留存紀錄(設備名稱/型號、銷毀日期、處理人員、照片..等)，以備日後查詢。

九、進階資安防護建置建議

為了強化醫院之資訊安全，可導入資安雲端訂閱型服務以介接健保署VPN 及民用網路並強化防護；對於經費預算及服務內容亦可保有較大的選擇彈性。

(五)醫院面對勒索軟體攻擊的應變指南

訂定日期：114 年 5 月 7 日

勒索軟體攻擊對醫院構成重大威脅，可能干擾病人照護、洩露敏感數據，甚至危及生命。本指南提供分階段的應對方法——立即應對、遏制與診斷、恢復與重建，並附上詳細技術指引，以辨識勒索軟體、追溯其來源並減輕影響。

本文件適用各級醫療機構，惟執行步驟依機構內規定調適，請依「勒索軟體應變分工及執行程序自我檢核表」建立執行程序，並適時檢視修正。

第一階段：立即應對（最初 1-2 小時）

初始應對對於「限制勒索軟體擴散」和「證據保全」至關重要，並依照規定完成通報。

1.1 隔離受感染系統

- 行動：立即將受感染設備從所有網路（Wi-Fi、LAN、藍牙）中斷開。
  - ○ 拔掉網路線並禁用無線連接。
  - ○ 避免完全關閉系統，以保留易揮發性資料(如記憶體)以供取證分析。
- 額外步驟：
  - ○ 禁用遠端存取工具（例如遠端桌面協議 [RDP]、VPN），防止進一步入侵。
  - ○ 若感染範圍不明確，隔離受影響的子網路。
  - ○ 通知全院，勿開啟關機狀態的電腦，避免擴散感染
  - ○ 使用非內部網路通信方式（市話、手機、LINE、Signal 等）進行協調。避免使用內部可能已被監控的電子郵件或內部系統。
  - ○ 若醫療相關系統受影響，考量啟動單機版或人工紙本作業

1.2 啟動事件應變團隊

- 行動：立即通知醫院的資安部門主管、資安專責(職)人員與資安

長。

○遵循醫院事件應變計畫及組建應變小組。

● 關鍵角色：

○醫院領導層(院長)：管理運營連續性和重大決策

○總指揮官(資安長)：協調跨單位資源、外部支援

○第一線指揮官(資訊/安主管)：負責損害控管、復原作業之指揮

○資安專(職)人員：通報聯繫作業，並應注意通報時效

○應變復原組(醫院資訊、醫工等及各設備、系統供應商)：執行復原與重建

○事件調查組(醫院資安 SOC 服務廠商)：事件調查及鑑識

○公關(醫院發言人)

1.3 證據保全

● 行動：除非絕對必要，切勿重啟系統、刪除或清除檔案(如清理回收資料夾)。

○若遇到以下情形必須關機，則採用直接拔除電源方式。

■主機死當狀態、藍屏(Blue Screen of Death)無法操作

■作業系統異常影響操作功能

■系統繁忙資源耗盡無法操作

○拍攝勒索訊息、錯誤訊息或其他可疑活動的螢幕截圖。

○ 記錄檔案時間戳記和檔案詳情（例如加密文件的路徑、修改時間與建立時間、檔案擁有者等）。

● 工具：使用手機或外部相機記錄，以免系統受損致證據佚失。

1.4 通報主管機關

● 行動：於知悉事件一個小時內完成資安事件通報。

○公務醫院請至 N-CERT 通報，https://www.ncert.nat.gov.tw/

○非公務醫院請至H-ISAC 通報，https://hisac.nat.gov.tw/【電話：03-4072132 (24 小時客服及緊急應變專線) |電子郵件：hisac-cs@mohw.gov.tw】若需外部支援可於通報單註明，並洽客服專線。

○駭侵事件之犯罪調查，應向所在地之(縣)市調查(站)處報案。

報案電話請參閱調查局所屬單位地圖 - 法務部調查局

- 額外步驟：
  - ○如個資外洩或損壞(個資安維事件)，請依「個人資料保護法」及「醫院個人資料檔案安全維護計畫實施辦法」辦理
    - ■ 事故時起七十二小時內，填寫「個人資料侵害事故通報紀錄表」以書面通報地方衛生局、副知衛生福利部
    - ■ 配合地方衛生局個資安維事件之行政調查作業
    - ■ 於發生個人資料被竊取、洩漏、竄改、毀損、滅失或其他侵害事故時迅速處理，以保護當事人之權益，包含「查明事故發生原因及損害狀況，以適當方式通知當事人或其法定代理人」
    - ■ 個人資料保護法、醫院個人資料檔案安全維護計畫實施辦法，可至「全國法規資料庫(https://law.moj.gov.tw/)」查詢

1.5 保護備份

- 行動：確認與驗證備份完整性。
  - ○檢查備份文件是否已被加密或竄改。
  - ○將備份主機離線或是副本儲存在隔離媒體(例如外部硬碟、磁帶) 。

第二階段：遏制與診斷 (最初 24 小時)

此階段專注於「識別勒索軟體」、「追溯其進入點」並保護關鍵資產。(由資安SOC 服務廠商協助執行)

2.1 識別惡意軟體類型

- 行動：分析勒索軟體痕跡以確定其類型和來源。
  - ○勒索訊息：檢查檔案 (如 README.txt 或 DECRYPT_INSTRUCTIONS.html) 中的時間戳記、檔案名稱或 IP 位址。
  - ○加密文件副檔名 : 尋找特徵(例如 .locky、.crypt、.WNCRY)。
  - ○C2：中繼站與攻擊者來源 IP。
  - ○惡意程式雜湊：提供惡意程式雜湊值 (MD5、SHA-1、SHA-256)

- 將雜湊值與威脅情報平台（例如 VirusTotal、ID Ransomware、 NoMoreRansom）比對。

※ 注意：不可將完整檔案上傳，避免造成資料外洩

○ 動態分析：可在沙盒環境（例如 Cuckoo Sandbox、Any.Run）中執行勒索軟體，觀察其行為。

● 目標：識別勒索軟體類型（例如 WannaCry、Ryuk、LockBit）並尋找已知的解密工具。

2.2 蒐集入侵指標（IOCs）

● 行動：蒐集 IOCs 資料，並於 24 小時內提供H-ISAC 客服信箱 (hisac-cs@mohw.gov.tw)

○ 受害主機作業系統及用途
○ 惡意程式植入時間
○ 文件雜湊：勒索軟體文件的 MD5、SHA-1、SHA-256。
○ 惡意 IP/域名：中繼站、攻擊來源及下載到惡意程式的網站。
○ 網路流量：從分析網路封包後發現的異常行為。
○ 檔案名稱/副檔名：.locked、.crypt 或隨機字串。
○ 機碼變更：開機啟動（例如 HKLM\Software\Microsoft\Windows\CurrentVersion\Run）。
○ 異常程序：非預期的 powershell.exe 或cmd.exe 活動。
○ 攻擊路徑：找出入侵的手法 (如利用弱點、工具、VPN 入口…等資訊)

● 額外步驟：若有取得惡意程式樣本，請將檔案加密壓縮寄送至 H-ISAC 客服信箱，壓縮密碼請設定為 virus。

● 目的：提供 IoC，以協助集體防禦

第三階段：恢復與重建（接下來 72 小時+）

此階段恢復運營，同時修補漏洞並強化防禦。

3.1 評估損壞與系統優先級

● 行動：識別關鍵核心（例如 HIS、PACS、EMR、LIS、NIS 等）。

○ 根據對病人照護的影響優先恢復。
○ 評估是否可進行備份復原(Online)，若不宜，則以單機作業或

紙本作業。

- 驗證：使用 「端點防護工具」持續監控，以確認系統處於安全狀態。

3.2 清理與恢復系統

- 行動：從驗證過的乾淨備份重建受影響系統。
  ○ 重灌受感染設備(從可信來源重新安裝作業系統/軟體)。
  ○ 全院修補所有漏洞並更新軟體/硬體。
- 驗證：使用 EDR 工具持續監控，以確認系統處於安全狀態。
  ※ 參考國家資通安全研究院 EDR 連通測試通過清單：
  https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/EDR/Related_ Documents_and-Forms/
  https://download.nics.nat.gov.tw/api/v4/file-service/UploadFile/edr/EDR%E9%80%A3%E9%80%9A%E6%B8%AC%E8%A9%A6%E9%80%9A%E9%81%8E%E6%B8%85%E5%96%AE_1140115.pdf
  【請自行維護最新版本下載點】

3.3 透明溝通

- 內部：告知員工事件情況、恢復時間表和臨時程序。
- 外部：若病人資料受影響，應依「個人資料保護法」第 12 條規定 通知當事人。
- 經驗教訓：根據調查結果更新安全政策。

3.4 文件記錄與分享

- 完成通報主管機關之續報： 1、2 級事件要於 72 小時，3、4 級事件於 36 小時完成續報。
- 完成通報主管機關之結報：後續於 1 個月內完成結案，送交調查、處理及改善報告。
- 召開調查檢討會議。

事前預防措施

勒索軟體的攻擊路徑包含取得合法帳號、利用系統漏洞或植入惡意程式後，建立後門並試圖橫向擴散至其他系統或取得高權限帳號，

再開始發動攻擊，唯有在每個環節導入防護措施，才能有效阻擋。

1. **帳號密碼控管：**加強密碼原則(例如至少 12 碼、包含英數大小寫及特殊符號)，並定期檢查高權限帳號是否有異常活動。
2. **落實資訊資產設備盤點：**應及時汰換或加強管制停止支援(EOS)及存在風險之設備。
3. **及時修補漏洞：**定期執行滲透測試及弱點掃描，漏洞修補完成後，仍應檢視修補期間是否已被零時差攻擊。
4. **提升同仁資安意識：**定期辦理資安教育訓練，並實施社交工程訓練，避免同仁誤觸惡意程式。
5. **制定通報應變程序並定期演練**。
6. **監控異常告警**：監控異常存取大量資料與未授權變更(如關閉防毒軟體)等行為，並啟用日誌記錄、異常告警、備份與刪除保護。
7. **建立網路架構圖及網段隔離：**記錄網路設備、IP 配置、通訊協定等資訊，並落實網段隔離避免橫向擴散。
8. **最小權限原則：**分配給使用者最低限度權限，禁止使用者自行安裝程式與使用 PowerShell，如需要額外權限應另行申請，且高權限帳號應有多重身分驗證保護。
9. **端點保護工具：**於端點設備安裝EDR 及防毒軟體，阻止惡意程式並發出告警，並落實可攜式媒體控管，未授權裝置不得連接內部網路
10. **系統備份及備援：**

(1) 重要資料至少備份 3 份，使用 2 種不同形式媒體，其中 1 份備份要存放異地，並定期進行測試還原演練。

(2) 離線加密備份也很重要，因為大多數勒索軟體攻擊者會嘗試尋找並刪除可存取的備份或將勒索病毒放入備份中。

11. **如不慎遭到成功入侵，請儘速依本文辦理應變處置。**

(六)公益揭弊者保護法

施行日期：114 年 7 月 22 日

第 1 條

為維護公共利益，有效發現、防止、追究重大不法行為，並保障公部門、國營事業及受政府控制之事業、團體或機構揭弊者之權益，特制定本法。

揭弊者之揭弊程序及保護，依本法之規定。但其他法律之規定更有利於揭弊者之保護者，從其規定。

第 2 條

本法之主管機關為法務部。

法務部為辦理本法所定之揭弊者保護事項，應組成揭弊者保護委員會。

本法所定事項，涉及各目的事業主管機關職掌者，由各該目的事業主管機關辦理。目的事業主管機關有爭議者，由揭弊者保護委員會確定之。

揭弊者保護委員會置委員七人，以法務部部長為主任委員，並為當然委員；其餘委員由主管機關就具下列資格者遴聘之，任期三年：

一、曾任法官、檢察官、律師及其他依法具有專門執業及技術執業資格人員五年以上者。

二、曾任或現任教育部認可之大專院校教授五年以上，聲譽卓著者。

三、對揭弊者保護、人權保障有專門研究或貢獻，或具相關公民團體實務經驗，聲譽卓著者。

揭弊者保護委員會之組織規程、遴聘方式、處理程序及其他應遵行事項之辦法，由主管機關定之。

第 3 條

本法所稱弊案，係指公務員或政府機關（構）、受政府控制之事業、團體或機構之人員，涉有下列犯罪或違法行為或涉及公共利益且情節重大者：

一、犯刑法瀆職罪章之行為。

二、違反貪污治罪條例之行為。

三、包庇他人犯罪之行為。但以法律有明文規定刑事處罰者為限。

四、違反公職人員利益衝突迴避法得處以罰鍰之行為。

五、違反政府採購法之行為。
六、法官法第三十條第二項第七款或第八十九條第四項第七款之應付評鑑行為。
七、違反下列各目涉有危害公共利益且情節重大之行為：
（一）犯刑法公共危險罪章、詐欺背信及重利罪、第二百三十一條之一、第二百九十六條、第二百九十六條之一之行為。
（二）違反洗錢防制法、組織犯罪防制條例、槍砲彈藥刀械管制條例、懲治走私條例、毒品危害防制條例、人口販運防制法、兒童及少年性剝削防制條例之行為。
（三）犯刑法妨害投票罪章或違反公職人員選舉罷免法、總統副總統選舉罷免法、公民投票法、反滲透法之行為。
（四）違反營業秘密法之行為。
（五）違反銀行法、保險法、證券交易法、期貨交易法、信託業法、金融控股公司法、票券金融管理法、證券投資信託及顧問法、公平交易法或其他有關經濟、財政法規之行為。
（六）違反水土保持法、山坡地保育利用條例、空氣污染防制法、水污染防治法、海洋污染防治法、廢棄物清理法、毒性及關注化學物質管理法、土壤及地下水污染整治法、環境用藥管理法之罪或其他有關環境保護法規之行為。
（七）違反藥事法、醫療器材管理法、食品安全衛生管理法、傳染病防治法或其他有關衛生福利法規之行為。
（八）違反勞動基準法、勞動檢查法、職業安全衛生法、就業服務法或其他有關勞動法規之行為。
（九）違反性騷擾防治法、性別平等工作法、性別平等教育法之行為。
（十）違反身心障礙者權益保障法、老人福利法、兒童及少年福利與權益保障法之行為。
八、其他涉及重大公共利益之犯罪、處以罰鍰或應付懲戒之行為。
前項第八款弊案範圍，由主管機關會商相關機關定之，並定期檢討、調整或增減。

第 4 條

本法所稱受理揭弊機關如下：
一、公部門之政府機關（構）主管、首長或其指定單位、人員。
二、國營事業、受政府控制之事業、團體或機構之主管、負責人或其

指定單位、人員。

三、檢察機關。

四、司法警察機關。

五、目的事業主管機關。

六、監察院。

七、政風機構。

揭弊內容涉及國家機密保護法之國家機密者，應向下列機關揭弊，始受本法保護：

一、涉及機密等級事項，應向前項第一款、第三款或第六款之受理揭弊機關為之。

二、涉及絕對機密及極機密等級事項，應向最高檢察署或高等檢察署及其檢察分署為之。

受理揭弊機關對揭弊內容，應依相關法令予以保密之。

受理揭弊機關經判定揭弊內容非其主管事項時，應將案件移送各權責機關，並通知揭弊者。揭弊案件經移送各權責機關者，仍依本法規定保護之。

第 5 條

本法所稱揭弊者如下：

一、公部門揭弊者：指公務員或接受政府機關（構）僱用、定作、委任、派遣、承攬、特約或其他契約關係而提供勞務獲致報酬之相對人及其員工，有事實合理相信政府機關（構）或其員工、其他公務員涉有第三條所列之弊案，具名向前條第一項受理揭弊機關提出檢舉者。

二、國營事業、受政府控制之事業、團體或機構揭弊者：指接受國營事業、受政府控制之事業、團體或機構之派任、僱用、定作、委任、派遣、承攬、特約或其他契約關係而提供勞務獲致報酬之相對人及其員工，有事實合理相信任職或提供勞務對象之事業、團體或機構或其員工，涉有第三條第五款、第七款或第八款之弊案，具名向前條第一項之受理揭弊機關提出檢舉者。

前項第一款所稱公務員，係指政務官及各級民意代表以外，依法令從事於公務之人員。

本法所稱政府機關（構），係指中央與各級地方政府機關、行政法人、公立學校、公立醫療院所、公營事業、政府捐助之財團法人。

本法所稱國營事業，係指國營事業管理法第三條所規定之事業。

本法所稱受政府控制之事業、團體或機構，係指銓敘部公告之政府暨其所屬營業基金、非營業基金轉投資金額累計占該事業資本額百分之二十以上之轉投資或再轉投資事業、受政府直接或間接控制其人事、財務或業務之轉投資或再轉投資事業、團體或機構。

前項事業、團體或機構之揭弊，限於弊案原因發生時屬於公告所列之事業、團體或機構。

第 6 條

揭弊者向受理揭弊機關揭弊後，未於二十日內獲受理調查之通知，經促請辦理後於十日內仍未獲回應，得再具名向下列人員或法人揭弊，自其向原受理揭弊機關揭弊時起，依本法規定保護之：

一、中央或地方民意代表。

二、具公司登記之媒體業者。

三、具法人登記之公益團體。

揭弊者向受理揭弊機關揭弊後，六個月內未獲調查結果之通知，經促請辦理後於十日內仍未獲回應，得再具名向前項人員或法人揭弊，自其向原受理揭弊機關揭弊時起，受本法之保護。

揭弊者未依第四條規定揭弊，而先向第一項人員或法人揭弊，第一項人員或法人受理後，應於十日內轉由受理揭弊機關辦理，經調查後發現揭弊屬實者，自其向第一項人員或法人揭弊時起，受本法之保護。

揭弊者經原受理揭弊機關受理調查為查無實據之結案通知後，再向前項人員或法人揭弊者，以該案另經起訴、緩起訴、職權不起訴、聲請簡易判決處刑、裁定准予自訴、懲戒、懲處、懲罰、彈劾、糾正、糾舉或行政罰鍰者為限，依本法規定保護之。

第 7 條

受理揭弊機關對揭弊事由應為調查，並得要求揭弊者、涉嫌事業單位或機關（構）等關係人提供相關事證配合調查，涉案關係人非有正當理由不得拒絕。

受理揭弊機關基於證據保全，於法院判決前，得向法院聲請扣押，準用刑事訴訟法第一百三十三條之規定。

第 8 條

政府機關（構）、法人或團體、個人，不得因揭弊者有下列行為，而對其採行不利之措施：

一、揭發第三條所列弊案。

二、配合弊案之調查或擔任證人。
三、拒絕參與弊案之決定或實施。
四、因前三款之作為而遭受不利措施後，依法提起救濟。
前項所稱不利措施，指下列情形之一：
一、解職、撤職、免職、停職、解約、降調，或不利之考績、懲處、懲罰及評定。
二、減薪（俸）、罰款（薪）、剝奪或減少獎金、退休（職、伍）金。
三、與陞遷有關之教育或訓練機會、福利、特殊權利之剝奪。
四、工作地點、職務內容或其他工作條件、管理措施之不利變更。
五、非依法令規定揭露揭弊者之身分。
因第一項各款行為而受不利措施者，得為下列請求：
一、回復其受不利措施前之職位及職務；其原職位已補缺或經裁撤者，回復至相當之職位及職務。
二、回復其原有年資、特殊權利、獎金、退休（職、伍）金、福利、工作條件及管理措施。
三、受不利措施期間俸（薪）給或工資之補發，及財產上損害之賠償。
四、受有身體、健康、名譽、自由、信用、隱私，或其他人格法益之侵害者，雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求為回復名譽之適當處分。
前項第三款所定財產上損害之賠償，包括俸（薪）給或工資以外其他期待利益之合理估算金額，及遭受不利措施後，依法提起救濟所合理支出之費用及律師酬金。
第二項所定不利措施之爭議，應先由受不利措施之人證明下列情事：
一、有第一項各款之行為。
二、有遭受第二項之不利措施。
三、第一款行為之發生時間在第二款不利措施之前。
受不利措施之人為前項證明後，推定為有違反本條第一項規定。但任職之政府機關（構）、法人、團體或其主管、雇主證明縱無該等行為，其於當時仍有正當理由採相同之人事措施者，不在此限。
訂有禁止揭弊者為第一項各款行為之約定，或限制揭弊者依第三項、第四項為請求之權利者，其約定無效。

第 9 條

具公務員身分之人因受第八條第二項第一款至第四款不利措施

者，應依其原有身分關係適用之法律程序提起行政救濟，所生同條第三項第三款及第四款之賠償請求權，自政府機關（構）依第二項主張作成回復原狀、行政救濟為有理由之決定確定之日起；因第八條第二項第五款不利措施所生之賠償請求權，自知悉事實發生之日起，六個月間不行使而消滅；自損害發生時起，逾二年者亦同。

公務員於申訴、再申訴、復審、訴願、評鑑、懲戒、行政訴訟或其他人事行政行為救濟程序中，主張其有第八條第一項各款行為者，而遭移送或受有不利措施者，應先於其他事證而為調查，並依調查結果而為成立或不成立之認定。

具公務員身分之受不利措施者主張其因有第八條第一項各款之行為而遭移送懲戒，經懲戒法院審理後，認定其依前項之主張成立並為不受懲戒之判決確定者，亦得請求第八條第三項第三款及第四款之賠償，並準用第一項時效之規定。

第一項及前項請求權之行使，不妨礙依民法、國家賠償法或其他法律所得行使之權利。

第 10 條

未具公務員身分之受不利措施者因雇主違反第八條第一項規定者，得自知悉其情形之日起三十日內，不經預告終止勞動契約。

前項人員得請求雇主給付其適用勞動基準法、勞工退休金條例或其他法規所規定之資遣費、退休金及相當於六個月工資補償金；其請求權自勞動契約終止時起，六個月間不行使而消滅。

未具公務員身分而受不利措施者所生第八條第三項之請求權，自知悉事實發生之日起，六個月間不行使而消滅；自損害發生時起，逾二年者亦同。

於行使前二項請求權之救濟程序中，未具公務員身分之受不利措施者主張其有第八條第一項各款行為者，應先於其他事證而為調查，並依調查結果而為成立或不成立之認定。

第二項及第三項請求權之行使，適用第八條第五項、第六項之規定，且不妨礙依民法或其他法律所得行使之權利。

依第八條第三項第一款復職顯有事實上之困難時，雇主得給付受不利措施者適用勞動基準法、勞工退休金條例或其他法規所規定之資遣費、退休金及相當於十二個月工資補償金，合意終止勞動契約。

第二項及前項之補償金，依受不利措施者為第八條第一項各款行為之前一月工資計算。

未具公務員身分之受不利措施者為政府機關（構）、法人或團體編制內支領俸（薪）給而訂有委任契約者，得準用第二項、第四項至前項規定請求補償金。但契約之約定有利於該受不利措施者，從其約定。

第 11 條

違反第八條第一項規定者，依下列情形予以處罰：

一、有公務員身分者，按其情節輕重，公務員懲戒法、公務人員考績法或其相關法規予以懲戒或懲處。

二、未具公務員身分之自然人、國營事業、受政府控制之事業、團體或機構，由各目的事業主管機關處新臺幣五萬元以上五百萬元以下罰鍰，但其他法律有較重之處罰規定者，從其規定。

前項第二款情形，各目的事業主管機關得限期命其改善，屆期不改善者，按次處罰之。

第 12 條

揭弊者依本法程序向第四條所列受理揭弊機關所陳述之內容涉及國家機密、營業秘密或其他依法應保密之事項者，不負洩密之民事、刑事、行政及職業倫理之懲戒責任；其為揭弊向律師徵詢法律意見而涉及前開依法應保密之事項者，亦同。

第 13 條

揭弊者係揭弊內容所涉犯罪之正犯或共犯，且符合證人保護法第三條及第十四條第一項之要件者，得依同法第十四條第一項予以減輕或免除其刑，不受該法第二條所列罪名之限制。

前項經法院判決免除其刑確定之揭弊者再任公職案件，得不受公務人員任用法第二十八條第一項第四款之限制。

第 14 條

揭弊者符合證人保護法第三條之要件者，其本人或其密切關係人，得依該法施以人身安全之保護措施，不受該法第二條所列罪名之限制。

意圖妨害或報復受本法保護之揭弊者揭發弊端、配合調查或擔任證人，而向揭弊者或其密切關係人實施犯罪行為者，依其所犯之罪，加重其刑至二分之一。

本法所稱揭弊者之密切關係人，指揭弊者之配偶、直系血親、三親等內旁系血親、二親等內姻親或家長、家屬、與其訂有婚約者或其他身分上或生活上有密切利害關係之人。

第 15 條

受理揭弊之機關及其承辦調查、稽查人員、執法人員或其他依法執行該相當職務、業務之人，對於揭弊者身分應予保密，非經揭弊者本人同意，不得無故洩漏於被揭弊對象或他人。

公務員無故洩漏揭弊者之身分者，處六月以上五年以下有期徒刑，得併科新臺幣三十萬元以下罰金。

因過失犯前項之罪者，處一年以下有期徒刑、拘役或科或併科新臺幣十萬元以下罰金。

非公務員無故洩漏揭弊者之身分者，處一年以下有期徒刑、拘役或科或併科新臺幣十萬元以下罰金。

第 16 條

揭弊者之個人資料，除法律另有規定或已無身分保密之必要者外，揭弊者得請求以代號製作筆錄或文書，遮隱其姓名、性別、出生年月日、住居所、身分證明文件編號或其他得以直接或間接方式識別該個人之資料，其簽名有保密之必要者，以按指印或簽寫代號代之；並應製作代號及真實姓名對照表，以密封套密封附卷。

前項筆錄或文書，除法律另有規定外，不得供閱覽或提供偵查、審判機關以外之其他機關（構）、法人或團體、個人。

揭弊者於偵查或審理中為詢(訊)問時，得依其要求蒙面、變聲、變像、視訊傳送或其他適當隔離方式為之。於其依法接受對質或詰問時，亦同。

前三項之保密措施，揭弊者得放棄之。

第 17 條

揭弊者之揭弊內容有下列情形之一者，仍得依本法受有保護：

一、所揭露之內容無法證實。但明顯虛偽不實或揭弊行為經受誣告、偽證罪緩起訴或判決有罪確定者，不在此限。

二、所揭露之內容業經他人檢舉或受理揭弊機關已知悉。但案件已公開或揭弊者明知已有他人檢舉，不在此限。

第 18 條

因揭弊者之揭弊而查獲不法事實者，應給與獎金。但因行使公權力而得知不法事實之政府機關（構）及其所屬人員、配偶或三親等以內之親屬，不在此限。

揭弊者任職之政府機關（構）、法人、團體或雇主對於揭弊者依法令所得領取之檢舉獎金，不得主張扣抵。

第一項獎金發給之標準及其他相關事項，由主管機關會同各目的事業主管機關定之。但其數額不得低於違反法令者因揭弊所受罰鍰、罰金、沒收之財物或財產上利益、追徵價額、財產抵償之總額百分之十。

第 19 條

為保障揭弊者之權益，揭弊者保護委員會辦理下列業務：

一、協助揭弊者依本法主張除去不利措施及請求損害賠償等權益。

二、提供揭弊者必要的法律諮詢與法律扶助。

三、協助揭弊者或其密切關係人依本法請求人身安全之保護措施及安置措施。

四、提供揭弊者緊急之生理、心理醫療與生活重建之協助。

五、揭弊者保護之宣導、倡議及研究。

六、其他符合揭弊者保護之事項。

主管機關應調派專任人員或聘用專業人員，承主任委員之命，協助辦理揭弊者保護委員會之業務。

第 20 條

本法施行細則，由行政院會同司法院、考試院定之。

第 21 條

本法自公布後六個月施行。

(七)公務員廉政倫理規範

修正日期：99 年 7 月 30 日

一、行政院（以下簡稱本院）為使所屬公務員執行職務，廉潔自持、公正無私及依法行政，並提升政府之清廉形象，特訂定本規範。

二、本規範用詞，定義如下：

（一）公務員：指適用公務員服務法之人員。

（二）與其職務有利害關係：指個人、法人、團體或其他單位與本機關（構）或其所屬機關（構）間，具有下列情形之一者：

1、業務往來、指揮監督或費用補(獎）助等關係。

2、正在尋求、進行或已訂立承攬、買賣或其他契約關係。

3、其他因本機關（構）業務之決定、執行或不執行，將遭受有利或不利之影響。

（三）正常社交禮俗標準：指一般人社交往來，市價不超過新臺幣三千元者。但同一年度來自同一來源受贈財物以新臺幣一萬元為限。

（四）公務禮儀：指基於公務需要，在國內（外）訪問、接待外賓、推動業務及溝通協調時，依禮貌、慣例或習俗所為之活動。

（五）請託關說：指其內容涉及本機關（構）或所屬機關（構）業務具體事項之決定、執行或不執行，且因該事項之決定、執行或不執行致有違法或不當而影響特定權利義務之虞。

三、公務員應依法公正執行職務，以公共利益為依歸，不得假借職務上之權力、方法、機會圖本人或第三人不正之利益。

四、公務員不得要求、期約或收受與其職務有利害關係者餽贈財物。但有下列情形之一，且係偶發而無影響特定權利義務之虞時，得受贈之：

（一）屬公務禮儀。

（二）長官之獎勵、救助或慰問。

（三）受贈之財物市價在新臺幣五百元以下；或對本機關（構）內多數人為餽贈，其市價總額在新臺幣一千元以下。

（四）因訂婚、結婚、生育、喬遷、就職、陞遷異動、退休、辭職、離職及本人、配偶或直系親屬之傷病、死亡受贈之財物，其

市價不超過正常社交禮俗標準。

五、公務員遇有受贈財物情事，應依下列程序處理：

（一）與其職務有利害關係者所為之餽贈，除前點但書規定之情形外，應予拒絕或退還，並簽報其長官及知會政風機構；無法退還時，應於受贈之日起三日內，交政風機構處理。

（二）除親屬或經常交往朋友外，與其無職務上利害關係者所為之餽贈，市價超過正常社交禮俗標準時，應於受贈之日起三日內，簽報其長官，必要時並知會政風機構。

各機關（構）之政風機構應視受贈財物之性質及價值，提出付費收受、歸公、轉贈慈善機構或其他適當建議，簽報機關首長核定後執行。

六、下列情形推定為公務員之受贈財物：

（一）以公務員配偶、直系血親、同財共居家屬之名義收受者。

（二）藉由第三人收受後轉交公務員本人或前款之人者。

七、公務員不得參加與其職務有利害關係者之飲宴應酬。但有下列情形之一者，不在此限：

（一）因公務禮儀確有必要參加。

（二）因民俗節慶公開舉辦之活動且邀請一般人參加。

（三）屬長官對屬員之獎勵、慰勞。

（四）因訂婚、結婚、生育、喬遷、就職、陞遷異動、退休、辭職、離職等所舉辦之活動，而未超過正常社交禮俗標準。

公務員受邀之飲宴應酬，雖與其無職務上利害關係，而與其身分、職務顯不相宜者，仍應避免。

八、公務員除因公務需要經報請長官同意，或有其他正當理由者外，不得涉足不妥當之場所。

公務員不得與其職務有利害關係之相關人員為不當接觸。

九、公務員於視察、調查、出差或參加會議等活動時，不得在茶點及執行公務確有必要之簡便食宿、交通以外接受相關機關（構）飲宴或其他應酬活動。

十、公務員遇有第七點第一項第一款或第二款情形，應簽報長官核准並知會政風機構後始得參加。

十一、公務員遇有請託關說時，應於三日內簽報其長官並知會政風機構。

十二、各機關（構）之政風機構受理受贈財物、飲宴應酬、請託關說

或其他涉及廉政倫理事件之知會或通知後，應即登錄建檔。

十三、公務員除依法令規定外，不得兼任其他公職或業務。

十四、公務員出席演講、座談、研習及評審（選）等活動，支領鐘點費每小時不得超過新臺幣五千元。

公務員參加前項活動，另有支領稿費者，每千字不得超過新臺幣二千元。

公務員參加第一項活動，如屬與其職務有利害關係者籌辦或邀請，應先簽報其長官核准及知會政風機構登錄後始得前往。

十五、本規範所定應知會政風機構並簽報其長官之規定，於機關（構）首長，應逕行通知政風機構。

十六、公務員應儘量避免金錢借貸、邀集或參與合會、擔任財物或身分之保證人。如確有必要者，應知會政風機構。

機關（構）首長及單位主管應加強對屬員之品德操守考核，發現有財務異常、生活違常者，應立即反應及處理。

十七、各機關（構）之政風機構應指派專人，負責本規範之解釋、個案說明及提供其他廉政倫理諮詢服務。受理諮詢業務，如有疑義得送請上一級政風機構處理。

前項所稱上一級政風機構，指受理諮詢機關（構）直屬之上一級機關政風機構，其無上級機關者，由該機關（構）執行本規範所規定上級機關之職權。

前項所稱無上級機關者，指本院所屬各一級機關。

十八、本規範所定應由政風機構處理之事項，於未設政風機構者，由兼辦政風業務人員或其首長指定之人員處理。

十九、公務員違反本規範經查證屬實者，依相關規定懲處；其涉及刑事責任者，移送司法機關辦理。

二十、各機關(構)得視需要，對本規範所定之各項標準及其他廉政倫理事項，訂定更嚴格之規範。

二十一、本院以外其他中央及地方機關（構），得準用本規範之規定。

(八)行政院及所屬機關（構）公立學校公務人員定期遷調參考原則

公發布日：111 年 11 月 18 日

一、 為強化行政院及所屬機關（構）、公立學校（以下簡稱各機關）公務人員久任廉政風險職務之監督制衡機制，促進廉正誠信之文化，特訂定本參考原則。

二、 各機關首長應親自或指定幕僚長以上人員召集政風單位會同人事及其他各單位，定期盤點及檢討廉政風險業務，並簽報機關首長核定。

前項機關未設置政風單位者，由機關首長指定特定單位或人員辦理。

機關首長應指定特定人員，就廉政風險業務不定期實施業務檢查。

三、 各機關對辦理廉政風險業務之職務，應依業務特性訂定職期，每年定期檢討辦理職期屆滿人員之遷調，並落實考核機制；如職期屆滿無適當職務可資遷調，得以調整業務內容或工作轄區方式辦理。檢討辦理情形應報主管機關備查。

前項所稱主管機關，指行政院及所屬二級機關、獨立機關。

四、 各機關辦理遷調，應依公務人員任用法、公務人員陞遷法及相關法令規定，並以遷調本機關及所屬機關職務列等及職務相當之職務為原則。

五、 因實際業務需要或人員有不適任、違反品操風紀、人地不宜等情形經查證屬實者，機關首長及單位主管得隨時調整人員職務，不受職期之限制。

六、 公務人員擔任具廉政風險之職務，其他法令另有職務遷調規定者，從其規定。

七、 教育人員及交通事業人員擔任具廉政風險之職務，其遷調得比照本參考原則辦理。

各機關聘用人員、約僱人員、臨時人員及工友辦理之業務，如有涉及廉政風險，得比照本參考原則及相關法令規定，檢討調整業務內容或工作轄區。

八、 公營事業、行政法人及地方政府得參照本參考原則，自行訂定廉政風險職務之遷調規定。

二、摘錄法規

(一)中華民國刑法

第 132 條

公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。

因過失犯前項之罪者，處一年以下有期徒刑、拘役或九千元以下罰金。

非公務員因職務或業務知悉或持有第一項之文書、圖畫、消息或物品，而洩漏或交付之者，處一年以下有期徒刑、拘役或九千元以下罰金。

第 210 條

偽造、變造私文書，足以生損害於公眾或他人者，處五年以下有期徒刑。

第 216 條

行使第二百一十條至第二百一十五條之文書者，依偽造、變造文書或登載不實事項或使登載不實事項之規定處斷。

第 220 條

在紙上或物品上之文字、符號、圖畫、照像，依習慣或特約，足以為表示其用意之證明者，關於本章及本章以外各罪，以文書論。

錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。

第三十六章 妨害電腦使用罪

第 358 條

無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 359 條

無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 360 條

無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致

生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 361 條

對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

第 362 條

製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 363 條

第三百五十八條至第三百六十條之罪，須告訴乃論。

(二)醫師法

第 28 條

未取得合法醫師資格，執行醫療業務，除有下列情形之一者外，處六個月以上五年以下有期徒刑，得併科新臺幣三十萬元以上一百五十萬元以下罰金：

一、在中央主管機關認可之醫療機構，於醫師指導下實習之醫學院、校學生或畢業生。

二、在醫療機構於醫師指示下之護理人員、助產人員或其他醫事人員。

三、合於第十一條第一項但書規定。

四、臨時施行急救。

五、領有中央主管機關核發效期內之短期行醫證，且符合第四十一條之六第二項所定辦法中有關執業登錄、地點及執行醫療業務應遵行之規定。

六、外國醫事人員於教學醫院接受臨床醫療訓練或從事短期臨床醫療教學，且符合第四十一條之七第四項所定辦法中有關許可之地點、期間及執行醫療業務應遵行之規定。

(三)公務員服務法

第 1 條

公務員應恪守誓言，忠心努力，依法律、命令所定執行其職務。

第 5 條

公務員有絕對保守政府機關（構）機密之義務，對於機密事件，無論是否主管事務，均不得洩漏；離職後，亦同。

公務員未經機關（構）同意，不得以代表機關（構）名義或使用職稱，發表與其職務或服務機關（構）業務職掌有關之言論。

前項同意之條件、程序及其他應遵循事項之辦法，由考試院會同行政院定之。

(四)行政程序法

第 170 條

行政機關對人民之陳情，應訂定作業規定，指派人員迅速、確實處理之。

人民之陳情有保密必要者，受理機關處理時，應不予公開。

(五)行政院及所屬各機關處理人民陳情案件要點

第18點

人民陳情案件有保密之必要者，受理機關應予保密。

指導單位：  **衛生福利部政風處**

執行單位：  **衛生福利部疾病管制署政風室**