○○機關資訊安全管理制度自行檢查表

○○年度

檢查日期：　年　月　日

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
1、**資訊安全政策** (1) 機關是否訂有資訊安全政策?(資訊安全政策指機關為達成資訊安全目標訂定之資訊安全管理作業規定、措施、標準、規範及行為準則等，並非指特定文件之名稱) (2) 機關之資訊安全政策文件是否由機關首長或授權人員核准，並正式發布且轉知所有員工與相關外部人員? (3) 資訊安全政策是否由機關管理階層每年至少審查一次?（經機關首長或其授權人員核准文件，如開會審查，會議紀錄亦應經機關首長核准）						
2、 **資訊安全組織與權責分工** (1) 機關是否確認資訊安全業務分工原則，配賦權責與相關單位及人員? (2) 是否指派副首長或高層主管人員擔任資訊安全長，負責資訊安全管理事項之協調及推動? (3) 是否成立跨部門之資訊安全小組，統籌資訊安全政策、計畫、資源調度等事項之協調研議? (4) 是否指定適當人員負責辦理資訊安全相關事宜?						
3、 **資訊資產管理** (1) 是否有資訊資產清冊，並隨時維護更新? (2) 各項資訊資產是否有明確的權責單位及保管者? (3) 資訊資產是否依其對組織的價值、法律要求、敏感性及重要性加以分類、標示？ (4) 資訊資產是否進行風險評鑑，並採行適當安全控制措施?						

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
4、 **人力資源安全** (1) 對人員之進用及調派，是否作適當之安全評估? (2) 機關是否針對人員進行適當的資訊安全認知教育與訓練? (3) 機關資訊安全人員教育訓練時數是否符合相關規定? (4) 人員是否瞭解單位資訊安全政策及應負之資安責任? (5) 對於可存取機密性、敏感性資訊或系統之人員以及配賦系統存取特別權限之人員是否有妥適分工與分散權責? (6) 員工調離職或委外作業人員於聘雇終止時，是否依規定繳回其使用或保管之資訊資產，並立即取消或調整其識別碼、通行碼、存取權限及安全責任? (7) 機關委外作業人力是否納入人力資源安全管理?是否簽署保密協議?						
5、 **實體與環境安全** ● **安全區域管理** (1) 是否針對管制區域之安全性（如機房、辦公區域或檔案室等），訂定適當之門禁管理及適當之控制措施加以保護，並指定專人負責管理？ (2) 相關人員（如維護廠商、系統管理人員、承辦人等）於管制區域執行作業時，是否留存相關工作記錄，並定期交由相關單位主管審核？ (3) 管制區域是否有適度的空調、消防、照明及備用電源等安全保護機制並定期檢視維修？ (4) 重要資訊處理設施是否與一般收發或裝卸區作實體隔離，以避免未經授權的存取? ● **設備安全** (5) 重要資訊設備是否予特別保護？設置地點是否檢查及評估來自環境如水、火、震動、電力供應、電磁幅射或人力破壞等可能對設備之危害?						

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
(6) 重要資訊設備電源之供應及備援電源是否作安全上考量? (7) 支援資訊服務之電源與電信佈纜是否作安全保護措施? (8) 設備是否定期維護保養，以確保其可用性及完整性? (9) 設備送機關外維修，對於儲存資訊是否訂有安全保護措施? (10) 在機關外使用資訊設備或存取資料是否訂有安全保護措施? (11) 可攜式的電腦設備是否訂有嚴謹的保護措施(如使用授權管理、設通行碼、檔案加密、專人看管)? (12) 設備報廢前是否將機密性、敏感性資料及授權軟體予以移除?						
6、 **通訊與作業管理** ● **作業程序與責任** (1) 機關負責管理之資訊系統，是否訂有操作程序並文件化（紙本或電子檔案），並持續更新維護? (2) 是否建立資訊處理設備與系統之變更管理程序? ● **第三方交付管理** (3) 資訊業務委外辦理時，是否與廠商簽訂適當的資訊安全與保密協定，賦與相關的安全管理責任，並納入契約條款? (4) 資訊業務委外辦理期間，是否定期對廠商所提供之服務、報告及記錄等進行監控與審查? (5) 委外服務如有變動時，是否評估資安措施之有效性?並作必要之調整。 ● **系統規劃與驗收** (6) 是否監視資訊系統各項資源的使用，並對未來容量需求預作規劃，以確保系統效能? (7) 是否建立資訊系統建置或升級版本的驗收標準，並於開發期間與驗收前實						

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
行適當之系統測試？						
● **防範惡意碼與行動碼**						
(8) 機關的資訊設備是否全面使用防毒軟體並即時更新病毒碼?						
(9) 資訊系統是否定期檢測安全弱點？並完成弱點修補？						
(10) 資訊系統行動碼的安裝是否作必要之授權處理或限制使用?						
● **備份與備援**						
(11) 重要的資料及系統軟體是否定期作備份處理?						
(12) 備份資料是否定期回復測試，以確保備份資料之有效性?						
● **網路安全管理**						
(13) 是否妥適管理網路，使其不受威脅，維持使用網路的系統與應用程式的安全，並確保資訊傳輸安全?（網路使用單位亦應妥善保護安置於機關之網路設備與佈線）						
(14) 網路管理機關是否訂定安全控制措施服務水準及管理要求，並訂定於相關契約中?						
(15) 網路管理機關是否依據所訂定之服務水準定期監視與審查委外廠商的執行狀況?						
(16) 網路管理機關是否使用網路防火牆並作符合組織需要之設定?						
(17) 利用網際網路及全球資訊網公布及流通資訊，是否評估資料安全等級？機密性、敏感性及未經當事人同意之個人隱私資料及文件，是否上網公布？						
(18) 機關網站存有個人資料及檔案者，是否建立妥適之安全保護措施？防止個人隱私資料遭不當或不法之竊取使用。						
(19) 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施?						
(20) 公務電腦是否安裝 P2P 軟體、資						

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
源分享軟體？ ● **媒體的處置** (21) 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟等)管理程序? (22) 媒體是否有安全之保存和報廢程序?機密性、敏感性資料之儲存或處理是否有安全處理程序及分級標示? (23) 系統文件是否有適當的存取保護措施? ● **資料交換** (24) 對於資訊及軟體交換是否訂有適當的交換政策、程序及控制措施? (25) 與外部單位間資訊與軟體的交換，是否訂有交換協議? (26) 重要電腦資料媒體(含報表)運送至機關外，是否有安全保護措施並留有完整監控記錄(含收送人、時間及內容)? (27) 採行電子交換之資料是否視資料安全等級採行識別碼通行碼管制、電子資料加密或電子簽章認證等保護措施? ● **系統監控** (28) 各項作業日誌是否定期稽查? (29) 是否建立各項監控系統之使用程序並定期審查監控? (30) 各項日誌是否有適當的保護措施?是否留有資訊系統管理者與操作者之作業日誌? (31) 資訊系統的故障是否存錄、分析、並採取適當措施? (32) 資訊系統的系統時間是否定期核對校正?以確保時間記錄正確。						
7、 **系統存取控制** (1) 是否訂有資訊存取控制政策及相關說明文件?是否訂定使用者存取權限註冊及註銷之作業程序?						

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
● **使用者存取管理** (2) 是否依業務需求及安全性考量，妥善賦予各級人員必要的系統存取權限?(系統管理最高權限不宜賦予全部人員，亦不宜完全賦予委外作業人員)。 (3) 機關負責管理之資訊系統是否建立使用者通行碼之管控制度?以正式的管理過程控制通行碼的配置? (4) 是否定期清查帳號權限，並移除久未使用之使用者權限?(一般使用者每年至少 1 次，特殊權限如伺服器的系統管理者每年至少 2 次)。 ● **使用者責任** (5) 機關負責管理之資訊系統是否建立系統使用者註冊管理制度?是否要求使用者定期更新(至少每六個月 1 次)使用者通行密碼? (6) 使用者通行密碼是否符合下列原則? 1. 密碼長度須 8~12 個字元。 2. 密碼複雜度設定至少需由英文、大小寫、數字或特殊符號的其中三個組成。 3. 避免使用與帳號相同的字元。 4. 避免使用個人公開的資料，如生日、電話號碼與身分證字號等。 5. 避免使用單位名稱、員工編號或其他相關事項。 (7) 對於無人看管之資訊設施是否有適當保護措施? (8) 個人電腦及終端機不使用時是否有關機或登出或設定螢幕通行碼或其他控制措施進行保護? (9) 員工離開座位時，是否維持桌面淨空(桌面不放置機密性文件、個人資料文件及可攜式媒體) ● **網路存取控制** (10) 網路管理機關是否妥適訂定網路存取控政策，有效防止網路服務遭未經授權的存取?						

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
(11) 是否對委外作業廠商以遠端連線方式進行系統維護者，辦理申請並限制連線作業時間，並對維護人員進行身分驗證?每次遠端連線維護作業，是否皆有維護紀錄?(紀錄前揭資料及維護內容) ● **作業系統存取控制** (12) 機關負責管理之資訊系統是否採取下列控制措施?有效防止作業系統經未經授權的存取。 1. 登入程序，是否避免提供輔助訊息(含登入失敗訊息)? 2. 是否限制登入失敗次數超過上限時需強制延遲一段時間或重新取得授權後才可再登入? 3. 對於異常登入程序，是否留有紀錄，並有專人定期檢視? 4. 使用者是否均有唯一的帳號? 5. 是否限制網路會談結束或在一定期間未操作電腦設備時,即予中斷連線或關閉設備? 6. 對風險高的應用系統是否設定連線時間限制? ● **應用系統與資訊存取控制** (13) 機關負責管理之資訊系統是否訂定存取控制政策，限制使用者與維護人員對資訊與應用系統功能之存取權限。? ● **行動電腦與遠距工作** (14) 是否訂定行動式電腦設備之管理政策? (15) 遠距工作是否得到管理階層授權和施以必要之保護措施?						
8、 **資訊系統獲取、開發及維護** **（適用於自行或委外開發、維護資訊系統之機關）** (1) 應用系統在規劃需求時，是否將安全要求納入分析及規格?						

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
(2) 委外作業廠商建置及維護重要之軟硬體設施，是否在機關相關人員監督及陪同下為之?						
● **應用系統的正確處理**						
(3) 機關為防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用，以確保應用系統的正確處理，是否針對負責管理的資訊系統採取下列控制措施? 1. 輸入資料是否作檢查，以確認其正確且適切性? 2. 應用程式內部處理是否加入檢查措施? 3. 應用系統是否依機關對資訊完整性的要求，妥善保護訊息的完整性? 4. 輸出資料是否具檢查確認功能?						
● **系統檔案安全**						
(4) 是否妥善管控作業系統軟體安裝與更新作業?作業系統升級前是否作版本安全性評估?						
(5) 測試作業是否避免以真實資料進行?如以真實資料測試，是否對委外作業廠商限制其可接觸之系統與資料範圍?						
(6) 程式源碼之存取控制，是否訂有控制措施?						
● **開發與維護過程的安全**						
(7) 是否建立應用系統之變更管理程序?						
(8) 系統變更後是否立即更新系統文件?						
(9) 系統變更後其相關控管措施與程序是否檢查仍然有效?						
(10) 作業系統變更後，是否對應用系統作技術性審查與測試?						
(11) 委外作業合約是否訂定資訊安全履行條款與相關罰則?是否依合約履行。						
(12) 委外作業合約中是否對著作權之歸屬訂有規範?						
● 系統漏洞修補						

檢查重點	自行檢查情形					檢查情形說明
	符合	部分符合	未符合	不適用	其他	
(13) 是否定期執行各項系統漏洞修補程式? (14) 進行系統修補前是否先作系統影響評估與測試，再採取必要措施?						
9、 **業務永續運作管理** ● 是否訂定業務永續運作計畫?(含緊急應變、復原作業程序、相關人員之權責等) (1) 是否建立資訊安全事件緊急處理機制? (2) 業務永續運作計畫是否定期測試、演練並予維護?						
10、 **資訊安全稽核** (1) 是否定期辦理資訊安全內部稽核?(每年至少 1 次) (2) 是否訂有資訊安全內部稽核計畫? (含稽核目標、範圍、時間、程序、人員) (3) 稽核時的存取行為是否作監控與並留有記錄? (4) 稽核後是否產生稽核報告並追踪改善情形(包括稽核發現的摘要、缺失說明及改進建議等)? (5) 資訊系統是否定期進行安全技術性查核? (如主機弱點檢測、網站弱點檢測或原始碼檢測等，包含資訊中心統籌辦理之測試) (七)針對安全技術性查核發現之弱點是否修補完成?若經評估無法修補，是否經機關首長或其授權人員核准暫不修補?						
11、 **軟體管理** (1) 是否建立電腦軟體使用管理制度? (2) 電腦是否安裝未經機關授權安裝之軟體? （P2P 軟體、資源分享軟體、未經申請程序安裝之 MSN、翻牆軟體等）						
結論/需採行之改善措施：						

<table>
<tr><td rowspan="2">檢查重點</td><td colspan="5">自行檢查情形</td><td>檢查情形說明</td></tr>
<tr><td>符合</td><td>部分符合</td><td>未符合</td><td>不適用</td><td>其他</td><td></td></tr>
<tr><td colspan="7">經檢查結果，。</td></tr>
</table>

填表人：　　單位主管：　　機關首長：