附件1

金門縣政府作業流程說明表

項目編號	G…
項目名稱	**資訊安全業務**
承辦單位	行政處資訊管理科
作業流程說明	一、資訊安全管理制度 (一)建立資訊安全管理制度。 (二)實作與運作資訊安全管理制度。 (三)監視與審查資訊安全管理制度。 (四)資訊安全管理制度文件化。 二、資訊安全管理系統 (一)資訊安全管理系統之適用範圍。 (二)資訊安全管理系統所需之文件及紀錄受到適當之保護與管制。 (三)資訊安全管理系統文件與紀錄發行前之適切性。 (四)定期檢視(至少一年一次)文件與紀錄的變更與最新修訂狀況。 (五)資訊安全管理系統內部稽核，以確保符合資訊安全規範、法規等的要求。 (六)稽核結果應確保所偵測出之不符合事項與原因均已消失，並確保所採行的措施並無不當延誤。

	(七)審查之審查輸入應依照資訊安全要求所訂之事項進行審查。 (八)藉由使用資訊安全政策、目標、稽核結果、監視事件之分析、矯正與預防措施以及審查，以持續改進資訊安全管理系統之有效性。 (九)建立內部及外部溝通聯繫相關措施。 三、風險評鑑與管理 (一)建立資訊資產及其擁有者。 (二)建立風險評鑑的方法論，且該方法論應確保產出可比較與可再產生的結果。 (三)建立資產可能遭遇之威脅。 (四)建立資產可能之脆弱點。 (五)建立風險擁有者。 (六)評鑑安全事件發生之可能性或機率。 (七)評鑑所有資產可能發生之風險值。 (八)確定風險接受之標準與可接受風險之等級。 (九)評鑑出所有可降低風險之控制措施。 (十)制定風險處理計畫並根據該計畫導入控制措施以降低風險。 (十一)應有書面的風險評鑑方法論、風險評鑑報告及風險處理計畫。 (十二)應評鑑出可忍受最大服務中斷時間(MTPD)、資料復原點(RPO)、系統回復時間(RTO)、資料復原(WRT)。 四、安全政策 (一)訂定資訊安全管理系統政策。 (二)資訊安全管理系統政策文件由單位資安長核准並正式發布且轉知所有員工與相關外部人員。 (三)資訊安全管理系統政策文件包括資訊安全之目標、範圍、實施內容、權責分工、員工責任、事件通報處理流程及違反安全政策的後果等。 (四)指定專人或專責單位進行資訊安全管理系統政策維護及檢討。 (五)定期(至少一年一次)或有重大變更時對資訊安全管理系統政策、目標之適切性及有效性，定期作必要之審查及調整。

	(六)資訊安全政策定期進行審查(至少一年一次)。 五、資訊安全組織 (一)指派適當權責之高階主管負責資訊安全管理系統之協調、推動及督導等事項。 (二)辦理資安政策、計畫、措施之研議，資料、資訊系統之使用管理及保護，資安認知、教育、訓練及資安稽核等資安工作事項。 (三)依一般使用者、系統管理者、系統擁有者等不同職務分別訂定其安全責任。 (四)重要資訊處理人員應簽署保密協議並定期審查。 (五)與相關單位如主管機關、資訊服務廠商、檢警單位、電力單位、電信單位及防救災單位建立聯絡管道。 (六)員工離職或第三方使用者於聘雇終止時，應依規定繳回其使用或保管之資訊資產並移除其存取權限。 八、實體與環境安全 (一)界定重要實體區域並施予安全保護。 (二)人員進入重要實體區域應實施安全控制措施。 (三)重要實體區域的進出權限應定期審查並更新(至少一年一次)。 (四)第三方支援服務人員進入重要實體區域應經過授權並監視其活動。 (五)電腦機房及重要地區，對於進出人員應作必要之限制及監督其活動。 (六)電腦機房操作人員應隨時注意環境監控系統，掌握機房溫度及溼度狀況。 (七)電腦機房操作人員應熟悉自動滅火系統操作方法及滅火器位置。 (八)各項安全設備應定期檢查(至少一年一次)，員工應施予適當的安全設備使用訓練。 (九)電源之供應及備援電源應作安全上考量。 (十)設備應定期維護保養(至少一年一次)，以確保其可用性及完整性。 (十一)設備送場外維修，對於儲存資訊應訂有安全保護措施。 (十二)設備報廢前應將機密性、敏感性資料及授權軟體予以

	移除或實施安全性覆寫。 (十三)設備報廢後如確定不再使用時，應將儲存之資料及軟體移除後並做實體破壞。 (十四)資訊資產如須攜出場外使用，應均經事前授權，並作安全查核。 (十五)公文及儲存媒體在不使用或不在班時應妥為存放，機密性、敏感性資訊應妥為收存。 九、密碼管理 (一)要求使用者對其個人通行碼盡保護及保密責任。 (二)要求使用者初次登入電腦系統後必須立即更改預設之通行碼。 (三)通行碼輸入錯誤，應訂有5次以下之限制。 (四)依規定期限或使用次數限制，要求變更通行碼。 (五)規定避免使用與個人有關資料(如生日、身份證字號、單位簡稱、電話號碼等)當作通行碼。 (六)個人電腦及終端機不使用時應關機或登出或設定螢幕通行碼或其他控制措施進行保護。 十、通訊管理 (一)重要電腦資料媒體(含報表)之運送，應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)。 (二)採行電子交換之資料應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。 (三)對外開放之資訊，應訂有保護措施以確保資訊完整性。 (四)各項作業日誌應定期稽查(至少一年一次)及適當的保護措施。 (五)資安事件日誌之記錄內容應包括使用者識別碼、登入登出之日期時間、電腦的識別資料或其網址、事件描述及矯正措施等事項。 十一、作業管理(資訊及業務單位) (一)電腦設備設置前應進行容量規劃，並預留安全容量。 (二)全面使用防毒軟體，並即時更新病毒碼。 (三)定期對電腦系統及資料儲存媒體進行病毒掃描(至少一年一次)。 (四)重要的資料及軟體應定期作備份處理(至少一年一次)。

	(五)備份資料應異地存放，存放處所環境應合於等級之實體保護環境。 (六)網路防火牆應符合組織需要之設定。 (七)定期與適時檢測網路運作環境之安全漏洞(至少一年一次)。 (八)訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序。 (九)具機密性或敏感性資訊的媒體應有安全之保存和報廢程序。 (十)系統文件應有適當的存取保護措施。 十二、存取控制 (一)訂有資訊存取控制政策及相關說明文件。 (二)訂定使用者存取權限註冊及註銷之作業程序。 (三)定期審查並移除久未使用之使用者權限(至少一年一次)。 (四)系統管理或特殊作業需要，如需設定特殊權限時，應訂有嚴格管理控制措施。 (五)訂有重要資訊不得閒置於桌面及螢幕淨空政策。 (六)網路使用者(含外單位人員)應取得正式存取授權。 (七)依網路服務需要區隔出獨立的邏輯網域(如內部網路或外部網路)，每個網域皆有既定的防護措施並有通訊閘道管制過濾網域間資料的存取(如網路防火牆)。 (八)電子郵件、單雙向檔案傳輸、互動式存取與存取時段作必要之安全控制措施。 (九)設有檢測連線的來源位址與目的位址網路路由之控管措施。 (十)登入程序，應避免提供輔助訊息(含登入失敗訊息)。 (十一)限制登入失敗次數的上限(建議3次)並中斷連線。 (十二)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。 (十三)對於異常登入程序，應留有紀錄，並有專人定期檢視(至少一年一次)。 (十四)使用者應均有唯一的識別碼。 (十五)通行碼應避免以網路且明文方式告知申請者。 (十六)訂有使用者及應用系統對資訊存取之權限管制措施。

	十三、委外廠商管理 (一)資訊業務委外辦理時，應與廠商簽訂適當的資訊安全協定並文件化，內容是否包含資訊與通訊技術供應鏈，賦與相關的安全管理責任，並納入契約條款。 (二)資訊業務委外辦理期間，應定期對廠商所提供之服務、報告及記錄等進行監控與審查，並定期進行稽核。 (三)委外服務如有異動時，應評估資安措施之有效性，並作必要之調整。 十四、資訊系統獲取、開發及維護 (一)應用系統在規劃需求時應將安全要求納入分析及規格。 (二)測試作業應避免以真實資料進行。 (三)原始程式庫之存取行為，應留有稽核日誌。 (四)作業系統變更後，應對應用系統作技術性審查。 (五)委外開發之系統上線前應偵測有無惡意程式。 (六)委外開發合約中應對著作權之歸屬訂有規範。 (七)訂約時應簽訂安全履行條款與相關罰則。 (八)應定期執行各項系統漏洞修補程式(至少每年一次)。 十五、資訊安全事故管理 (一)建立資安事件(含安全漏洞、系統弱點、病毒、非法入侵及系統異常)之通報及處理程序。 (二)建立資安事故管理責任及應變程序。 (三)建立資安事故管理機制，如記錄事故形式、處置方法、處理成本及矯正預防措施。 (四)機關員工及外部使用者應知悉資安事件通報及處理程序並依規定辦理。 十六、營運持續管理 (一)擬訂關鍵性業務營運衝擊分析表(BIA)。 (二)鑑別可能造成營運中斷事件之衝擊及機率，並進行風險評鑑。 (三)擬訂營運持續計畫(含啟動條件、參與人員、緊急程序、備援程序、重置程序、維護時間表、教育訓練、職責說明、所需資源、往來單位之應變規劃及合約適當性等)。 (四)營運持續計畫應定期完整測試、演練並予維護(至少一年一次)。 (五)營運持續計畫應配合業務及人員之變更而更新。

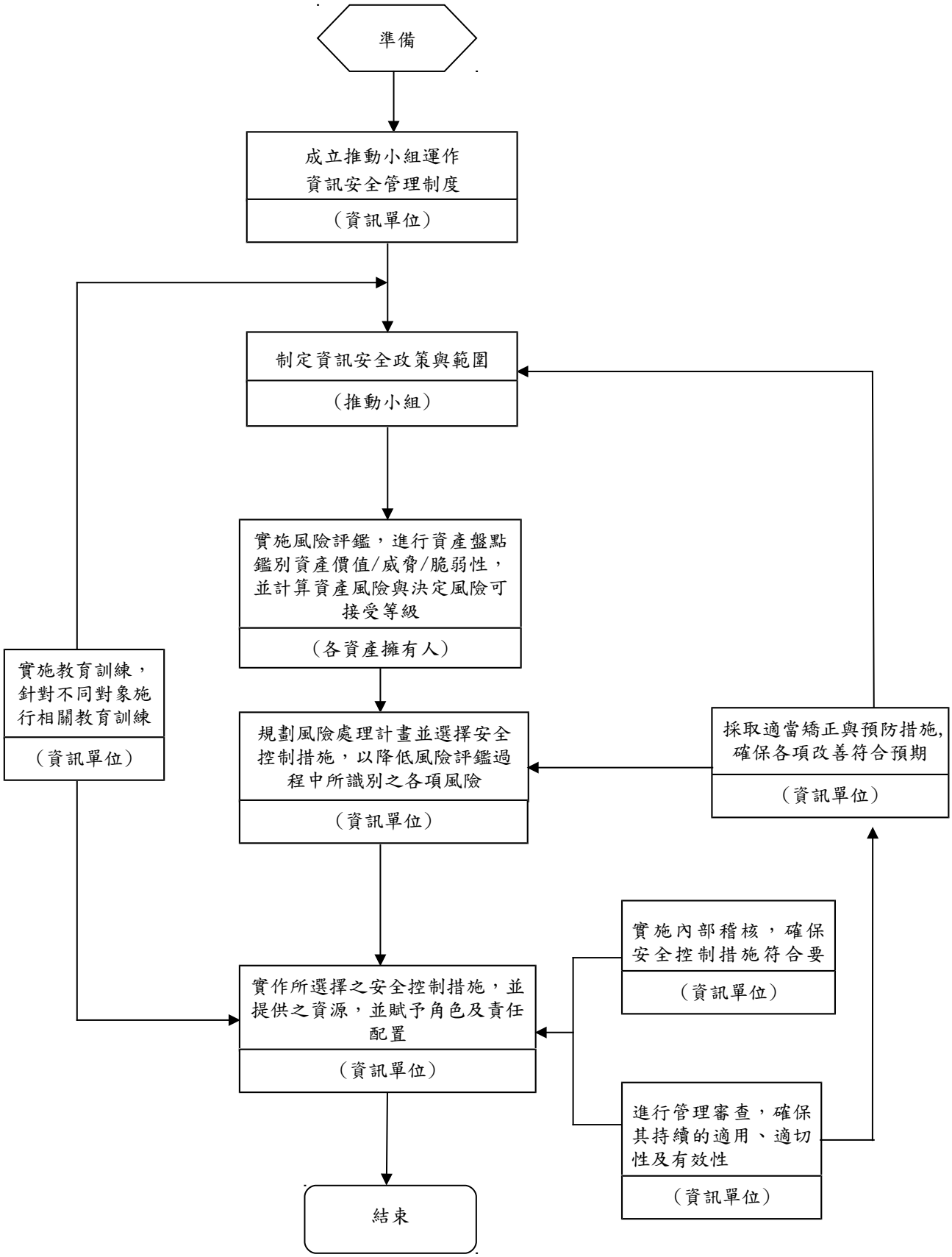
	(六)營運持續計畫定期審查和更新(至少一年一次)。 十七、遵循性 (一)軟體取得(含自行開發、委外開發、購置或租用)應依智慧財產權規定或合約要求確實辦理。 (二)重要紀錄(如資料庫紀錄、系統日誌、操作日誌、稽核日誌)應依安全等級加以保護儲存(如檔案加密或數位簽章)。 (三)涉有個人隱私及個人資料之保護應有妥適之保護機制。 (四)應有監視設備或其他可偵測未經授權使用的設備，以防止資訊設施被不當使用。 (五)資訊系統應定期進行安全技術符合性的檢查(如滲透測試或系統弱點檢測)(至少一年一次)。 (六)定期辦理資訊安全內部稽核(至少一年一次)。 (七)內部稽核範圍應包含資訊系統、資訊資產負責人、使用者和管理階層。 (八)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)。 (九)稽核時的存取行為應作監控與並留有記錄。 (十)稽核後應產生稽核報告並追蹤改善情形。
控制重點	一、成立資訊安全組織，以運作資訊安全管理制度。 二、訂定資訊安全政策，並由單位資安長核准與正式發布，且轉知所有同仁。 三、實施風險評鑑，並針對評鑑結果規劃適當的風險處理計畫。 四、依風險評鑑結果，針對以下之安全控制領域，實作各項安全控制措施： (一)安全政策。 (二)資訊安全組織。 (三)人力資源安全。 (四)資產管理。 (五)存取控制。 (六)密碼管理。 (七)實體與環境安全。 (八)作業管理。 (九)通訊管理。 (十)系統獲取、開發及維護。

	(十一)委外廠商。 (十二)資訊安全事故管理。 (十三)營運持續管理。 (十四)遵循性。 五、定期實施內部稽核，以確保各項安全控制措施符合要求(至少一年一次)。 六、定期審查資訊安全管理制度，以確保其持續的適用、適切性及有效性(至少一年一次)。 七、資訊安全管理制度中所需之文件與紀錄，並受到適當的保護。
法令依據	一、行政院88年9月15日台88經字第34735號函訂頒之「行政院及所屬各機關資訊安全管理要點」。 二、行政院研究發展考核委員會88年11月16日（88）會訊字第05787號函頒之「行政院及所屬各機關資訊安全管理規範」。 三、行政院96年2月15日核定修正之「建立我國通資訊基礎建設安全機制計畫」。 四、行政院資通安全會報102年12月25日核定之「國家資通訊安全發展方案(102-105)」。 五、行政院國家資通安全會報99年7月核定之「資訊系統分類分級與鑑別機制參考手冊」。 六、101年5月26日發布「個人資料保護法」，本府將依所規範之權利義務，盡善良管理人之注意義務。相關資料之保存、利用等事項，依個人資料保護法規定為之。
使用表單	「資訊安全管理制度」內部控制制度作業層級自行評估表。

附件 2

（機關名稱）（單位名稱）作業流程圖

（機關名稱 ） 資訊安全業務



附件3

（機關名稱）內部控制制度自行評估表

_____年度

自行評估單位：_____

作業類別（項目）：（單位預算機關名稱）資訊安全　評估日期：__年__月__日

評估重點	自行評估情形		評估情形說明
	符合	未符合	
一、資訊安全管理制度 (一)是否已建立資訊安全管理制度？ (二)是否定期審查資訊安全管理制度？ (三)資訊安全管理制度文件化？			
二、資訊安全管理系統 (一)是否明確建立資訊安全管理系統之適用範圍？ (二)資訊安全管理系統所需之文件及紀錄是否受到適當之保護與管制？ (三)是否定期檢視(至少一年一次)文件與紀錄的變更與最新修訂狀況？ (四)資訊安全管理系統內部稽核，是否符合資訊安全規範、法規等的要求？ (五)是否針對不符合事項與原因均採行的措施並無不當延誤。 (六)審查輸入是否依照資訊安全要求所訂之事項進行審查？ (七)是否依照資訊安全政策、目標、稽核結果、監視事件之分析、矯正與預防措施以及審查，持續改進資訊安全管理系統之有效性？ (八)是否建立內部及外部溝通聯繫相關措施？			
三、風險評鑑與管理			

(一)是否建立資訊資產及其擁有者？ (二)是否建立風險評鑑的方法論，且該方法論應確保產出可比較與可再產生的結果？ (三)是否建立資產可能遭遇之威脅？ (四)是否建立資產可能之脆弱點？ (五)是否有建立風險擁有者？ (六)是否評鑑安全事件發生之可能性或機率？ (七)是否評鑑所有資產可能發生之風險值？ (八)是否確定風險接受之標準與可接受風險之等級？ (九)是否評鑑出所有可降低風險之控制措施？ (十)是否制定風險處理計畫並根據該計畫導入控制措施以降低風險？ (十一)是否有書面的風險評鑑方法論、風險評鑑報告及風險處理計畫？ (十二)是否評鑑出可忍受最大服務中斷時間(MTPD)、資料復原點(RPO)、系統回復時間(RTO)、資料復原(WRT)？			
四、安全政策 (一)是否訂定資訊安全管理系統政策？ (二)資訊安全管理系統政策文件是否由單位資安長核准並正式發布且轉知所有員工與相關外部人員？ (三)資訊安全管理系統政策文件是否包括資訊安全之目標、範圍、實施內容、權責分工、員工責任、事件通報處理流程及違反安全政策的後果等？ (四)是否指定專人或專責單位進行資訊安全管理系統政策維護及檢討？ (五)是否定期(至少一年一次)或有重大變更時對資訊安全管理系統政策、			

目標之適切性及有效性，定期作必要之審查及調整？ (六)資訊安全政策是否定期進行審查(至少一年一次)？			
五、資訊安全組織 (一)是否指派適當權責之高階主管負責資訊安全管理系統之協調、推動及督導等事項？ (二)是否辦理資安政策、計畫、措施之研議，資料、資訊系統之使用管理及保護，資安認知、教育、訓練及資安稽核等資安工作事項？ (三)是否有依一般使用者、系統管理者、系統擁有者等不同職務分別訂定其安全責任？ (四)重要資訊處理人員是否有簽署保密協議並定期審查？ (五)是否有與相關單位如主管機關、資訊服務廠商、檢警單位、電力單位、電信單位及防救災單位建立聯絡管道？ (六)員工離職或第三方使用者於聘雇終止時，是否有依規定繳回其使用或保管之資訊資產並移除其存取權限？			
八、實體與環境安全 (一)是否有界定重要實體區域並施予安全保護？ (二)人員進入重要實體區域是否有實施安全控制措施？ (三)重要實體區域的進出權限是否有定期審查並更新(至少一年一次)。 (四)第三方支援服務人員進入重要實體區域是否有經過授權並監視其活動？ (五)電腦機房及重要地區，對於進出人			

員是否有作必要之限制及監督其活動。 (六)電腦機房操作人員是否有隨時注意環境監控系統，掌握機房溫度及溼度狀況？ (七)電腦機房操作人員是否熟悉自動滅火系統操作方法及滅火器位置？ (八)各項安全設備是否有定期檢查(至少一年一次)，員工是否有適當的安全設備使用訓練？ (九)電源之供應及備援電源是否有作安全上考量？ (十)設備是否有定期維護保養(至少一年一次)，以確保其可用性及完整性？ (十一)設備送場外維修，是否訂有儲存資訊應訂有安全保護措施？ (十二)設備報廢前是否有將機密性、敏感性資料及授權軟體予以移除或實施安全性覆寫？ (十三)設備報廢後如確定不再使用時，是否有將儲存之資料及軟體移除後並做實體破壞？ (十四)資訊資產如須攜出場外使用，是否有事前授權，並作安全查核？ (十五)公文及儲存媒體在不使用或不在班時是否有妥善存放？機密性、敏感性資訊是否有妥善收存？			
九、密碼管理 (一)是否要求使用者對其個人通行碼盡保護及保密責任？ (二)是否要求使用者初次登入電腦系統後必須立即更改預設之通行碼？ (三)通行碼輸入錯誤，是否訂有5次以下之限制。 (四)是否規定期限或使用次數限制，要			

求變更通行碼？ (五)是否規定避免使用與個人有關資料(如生日、身份證字號、單位簡稱、電話號碼等)當作通行碼？ (六)個人電腦及終端機不使用時是否關機或登出或設定螢幕通行碼或其他控制措施進行保護？			
十、通訊管理 (一)重要電腦資料媒體(含報表)之運送，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)？ (二)電子交換之資料是否有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？ (三)對外開放之資訊，是否訂有保護措施以確保資訊完整性？ (四)各項作業日誌是否定期稽查(至少一年一次)，各項日誌是否有適當的保護措施？ (五)資安事件日誌之記錄內容是否有包括使用者識別碼、登入登出之日期時間、電腦的識別資料或其網址、事件描述及矯正措施等事項？			
十一、作業管理 (一)電腦設備設置前是否有進行容量規劃並預留安全容量？ (二)是否有使用防毒軟體，並即時更新病毒碼？ (三)是否有定期對電腦系統及資料儲存媒體進行病毒掃描(至少一年一次)。 (四)重要的資料及軟體是否有定期作備份處理(至少一年一次)。 (五)備份資料是否有異地存放，存放			

處所環境是否有合於等級之實體保護環境？ (六)網路防火牆是否有符合組織需要之設定。 (七)是否有定期與適時檢測網路運作環境之安全漏洞(至少一年一次)？ (八)是否有訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？ (九)具機密性或敏感性資訊的媒體是否有安全之保存和報廢程序？ (十)系統文件是否有適當的存取保護措施？			
十二、存取控制 (一)是否有資訊存取控制政策及相關說明文件？ (二)是否有使用者存取權限註冊及註銷之作業程序？ (三)是否有定期審查並移除久未使用之使用者權限(至少一年一次)？。 (四)系統管理或特殊作業需要，如需設定特殊權限時，是否有嚴格管理控制措施？ (五)是否訂定重要資訊不得閒置於桌面及螢幕淨空政策？ (六)網路使用者(含外單位人員)是否有取得正式存取授權？ (七)是否依網路服務需要區隔出獨立的邏輯網域(如內部網路或外部網路)，每個網域皆有既定的防護措施並有通訊閘道管制過濾網域間資料的存取(如網路防火牆)？ (八)電子郵件、單雙向檔案傳輸、互動式存取與存取時段是否訂有安全控制措施？			

(九)是否設有檢測連線的來源位址與目的位址網路路由之控管措施？ (十)登入程序，是否有避免提供輔助訊息(含登入失敗訊息)？ (十一)是否有限制登入失敗次數的上限(建議3次)並中斷連線？ (十二)是否有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？ (十三)對於異常登入程序，是否有紀錄，並專人定期檢視(至少一年一次)？ (十四)使用者是否有唯一的識別碼？ (十五)通行碼是否避免以網路且明文方式告知申請者？ (十六)是否訂有使用者及應用系統對資訊存取之權限管制措施？			
十三、委外廠商管理 (一)資訊業務委外辦理時，是否與廠商簽訂適當的資訊安全協定並文件化，內容是否包含資訊與通訊技術供應鏈，賦與相關的安全管理責任，並納入契約條款？ (二)資訊業務委外辦理期間，是否應定期對廠商所提供之服務、報告及記錄等進行監控與審查，是否有定期進行稽核？ (三)委外服務如有異動時，是否有評估資安措施之有效性，並作必要之調整？			
十四、資訊系統獲取、開發及維護 (一)應用系統在規劃需求時是否有將安全要求納入分析及規格？ (二)測試作業是否有避免以真實資料進行？ (三)原始程式庫之存取行為，是否留有			

稽核日誌？ (四)作業系統變更後，是否有對應用系統作技術性審查？ (五)委外開發之系統上線前是否有偵測有無惡意程式？ (六)委外開發合約中是否對著作權之歸屬訂有規範？ (七)訂約時是否有簽訂安全履行條款與相關罰則？ (八)是否有定期執行各項系統漏洞修補程式(至少每年一次)？			
十五、資訊安全事故管理 (一)是否建立資安事件之通報及處理程序？ (二)是否建立資安事故管理責任及應變程序？ (三)是否建立資安事故管理機制，如記錄事故形式、處置方法、處理成本及矯正預防措施？ (四)機關員工及外部使用者是否知悉資安事件通報及處理程序並依規定辦理？			
十六、營運持續管理 (一)是否擬訂關鍵性業務營運衝擊分析表(BIA)？ (二)是否鑑別可能造成營運中斷事件之衝擊及機率，並進行風險評鑑？ (三)是否擬訂營運持續計畫？ (四)營運持續計畫是否定期完整測試、演練並予維護(至少一年一次)？ (五)營運持續計畫是否配合業務及人員之變更而更新？ (六)營運持續計畫是否定期審查和更新(至少一年一次)？			
十七、遵循性 (一)軟體取得是否依智慧財產權規定或			

合約要求確實辦理？ (二)重要紀錄是否依安全等級加以保護儲存？ (三)涉有個人隱私及個人資料之保護是否有妥適之保護機制？ (四)是否有監視設備或其他可偵測未經授權使用的設備，以防止資訊設施被不當使用？ (五)資訊系統是否定期進行安全技術符合性的檢查(至少一年一次)？ (六)是否定期辦理資訊安全內部稽核(至少一年一次)？ (七)內部稽核範圍是否包括資訊系統、資訊資產負責人、使用者和管理階層？ (八)是否訂有資訊安全內部稽核計畫？ (九)稽核時的存取行為是否有監控與並留有記錄？ (十)稽核後是否有產生稽核報告並追蹤改善情形？			
結論／需採行之改善措施：			
填表人：　　單位主管：　　機關首長：			

註：1.機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，就作業流程重點納入評估。

2.自行評估情形除勾選外，未符合者必須於說明欄內詳細記載評估情形。