

附件五：

資訊安全管理內部稽核表

公司名稱			
單位名稱			
單位主管		評估日期：	
評估人員		評估日期：	
聯絡窗口	電話：	傳真：	Email：

備註：內部稽核表之查核項目如有未建立或未落實等情況，請答「否」，並填寫「資訊安全管理矯正／預防措施一覽表」(附件八)及「資訊安全管理矯正／預防措施單」(附件九)，便於後續加強管理。

資訊安全管理內部稽核表(1)

頁次： 1/16

檢 查 項 目	是	否	不適 用
1. 資訊安全政策訂定			
1.1 是否訂有資訊安全政策？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2 資訊安全政策文件是否由管理階層核准，並正式發布且轉知所有員工？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3 是否訂有資訊安全政策的說明文件及資料(如作業程序、資訊安全控管文件、使用者應遵守的安全規則)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.4 資訊安全政策文件是否包括資訊安全定義、目標、涵蓋範圍、實施內容、執行組織、權責分工、員工責任、事件通報程序、處理流程等？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.5 資訊安全政策文件是否就一般使用人員與專責人員之權責分項說明？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.6 是否指定專人或專責部門進行資訊安全政策的維護及檢討？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.7 是否定期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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.8 資訊安全政策是否由管理階層每年至少審查一次？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.9 是否定期對單位人員及資訊設備進行安全評估，以確定其是否遵守資訊安全政策及相關規定？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.10 是否訂有違反資訊安全規定之處理程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(2)

頁次： 2/16

檢 查 項 目	是	否	不適 用
2. 資訊安全權責分工			
2.1 管理階層是否瞭解資訊安全目的予以支持並承諾？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2 是否指定高級主管人員或成立跨部門組織負責推動、協調及監督資訊安全管理事項？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3 是否指定專人或專責部門負責規劃、執行與控管資訊安全工作？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.4 是否指定部門辦理風險評估、安全分級、系統安全控管措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.5 是否訂定員工資訊安全作業程序與權責規範？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.6 是否訂定各項資訊設備的安全作業程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.7 是否訂定資訊安全狀況授權處理層級？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.8 是否對資訊計畫內容進行資訊安全政策符合性檢查？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.9 開放給外部機構之資料存取，是否辦理風險評估？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.10 開放給外部機構之資料存取，是否訂定控管程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.11 開放給外部機構之資料存取，於契約中是否訂定雙方權利義務及違約處分方式？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.12 簽訂資料存取之契約中是否包含資料保護、服務水準、智慧財產權、事故發生處理方式等條款？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.13 委外契約中有關安全需求內容是否包含法律需求(如電腦處理個人資料保護法)、界定雙方有關人員權責、使用何種實體與邏輯安全控管措施、對委外廠商稽核權、得依實際需要隨時修改安全控管措施及作業程序等？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.14 因業務需要開放給外部機構(含其他公司、上下游業者、顧問、維護廠商、委外承包商、臨僱人員)使用之資訊，其存取權限是否嚴加控管？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(3)

頁次: 3/16

檢 查 項 目	是	否	不適 用
3. 人員管理及資訊安全教育訓練			
3.1 員工應盡之安全責任是否納入其工作說明書或系統文件？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2 對人員之進用及調派，是否作適當之安全評估？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3 員工或第三方使用者是否簽署保密協議並均知保密事項？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.4 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否有妥適分工與分散權責？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5 管理階層是否有要求員工、承包商及第三方使用者，執行所制訂的政策及程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6 員工是否瞭解單位資訊安全政策及應負之資安責任？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.7 員工(含第三方使用者)是否依職務層級進行適當的資訊安全認知教育與訓練？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.8 是否訂有員工辦理或違反組織安全政策與程序獎懲規定？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.9 針對人員(含第三方使用者)之調動、離職或退休，是否立即取消或調整其識別碼、通行碼、存取權限及安全責任？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.10 員工離職或第三方使用者於聘雇終止時，是否依規定繳回其使用或保管之資訊資產並移除其存取權限？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.11 是否對員工品德、行為、家庭狀況等加以考核？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.12 是否隨時公告資訊安全相關訊息？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.13 下班後員工是否將經辦之機密性或敏感性資料，妥善收藏？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.14 是否對員工的私人資訊設備作必要之安全控管程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(4)

頁次： 4/16

檢 查 項 目	是	否	不適 用
4. 系統安全管理			
4.1 是否訂有資訊處理設備之操作程序及管理責任？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2 是否建立系統變更之管理程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.3 是否訂定電腦當機及服務中斷後之緊急處理程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.4 對於安全要求高的資訊業務，是否分散其資訊安全管理及執行之責任？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.5 業務系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否授權由不同的人員執行？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.6 系統開發及正式作業是否區隔在不同的系統環境處理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.7 是否與委外廠商簽訂適當的資訊安全協定，賦予相關的安全管理責任，並納入契約條款？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.8 資訊業務委外辦理期間，是否定期對廠商所提供之服務、報告及紀錄等進行監控與審查，並定期進行稽核？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.9 委外服務如有異動時，是否評估資安措施之有效性？並作必要之調整。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.10 電腦設備設置前是否進行容量規劃並預留安全容量？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.11 是否建立新系統或系統升級之驗收程序(含驗收標準及應有之測試)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.12 是否使用網路防火牆(Fire Wall)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.13 是否全面使用防毒軟體並即時更新病毒碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.14 是否定期對電腦系統及資料儲存媒體進行病毒掃描？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.15 是否訂定電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.16 行動碼的安裝是否作必要之授權處理或限制使用？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(4)

頁次： 5/16

檢 查 項 目	是	否	不適 用
4.17 重要的資料及軟體是否定期作備份處理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.18 備份資料是否異地存放？存放處所環境是否合於等級之實體保護環境？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.19 備份資料是否定期回復測試，以確保備份資料之有效性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.20 復原程序是否定期檢查與測試？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.21 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？			
4.22 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？			
4.23 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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.24 系統文件是否有適當的存取保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.25 對於資訊及軟體之交換是否訂有適當的交換政策、程序及控制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.26 對於採用語音、傳真及視訊通訊等設施進行資訊交換，是否訂有保護控制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.27 與外部單位間資訊與軟體的交換，是否訂有交換協議？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.28 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)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.29 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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.30 對於線上交易或申辦的資訊，是否訂有控制措施？以確保資訊之機密性及完整性。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.31 對外開放之資訊，是否訂有保護措施以確保資訊完整性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.32 各項作業日誌是否定期稽查？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.33 是否建立各項監控系統之使用程序並定期審查監控？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(4)

頁次： 6/16

檢 查 項 目	是	否	不適 用
4.34各項日誌是否有適當的保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.35是否留有詳細的管理者與操作員之作業日誌？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.36 資安事件日誌之紀錄內容是否包括使用者識別碼、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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.37所有系統鐘訊是否定期核對校正？以確保時間紀錄正確。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.38是否訂有資訊安全事故建立通報程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.39資訊安全事件處理的過程是否均留有完整記錄？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.40是否遵守軟體授權規定，禁止使用未取得授權的軟體？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(5)

頁次： 7/16

檢 查 項 目	是	否	不適用
5. 網路安全管理			
5.1 是否將網路運作及電腦運作之使用權責予以區隔？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2 是否訂定使用網路遠端設備之使用權責及程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3 對於機敏性資訊之傳輸過程是否採取資料加密等保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.4 是否訂定為確保網路服務連線品質及可用性之保護措施，以提供最佳服務？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.5 是否使用網路安全防禦設備？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.6 是否定期檢討網路安全控管事項之執行？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.7 是否定期檢測網路運作環境之安全漏洞？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.8 有關網路安全之事項是否隨時公告？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.9 是否訂定網路服務提供者及使用者之服務及使用範圍、相關權責及程序，並納入服務協議中？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(6)

頁次： 8/16

檢 查 項 目	是	否	不適 用
6. 系統存取控制管理			
6.1 是否訂有資訊存取控制政策及相關說明文件？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.2 資訊存取控制政策是否符合個人資料保護等相關法令與契約規定？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.3 是否訂定使用者存取權限註冊及註銷之作業程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4 是否定期審查並移除久未使用之使用者權限？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5 基於系統管理或特殊作業需要，如需設定特殊權限時，是否訂有嚴格管理控制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.6 是否要求使用者對其個人通行碼應盡保護及保密責任？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.7 是否強制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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.8 對於忘記通行碼之處理，是否要求須作身份確認程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.9 預設之通行碼是否以安全之程序轉交於使用者，使用者取得通行碼確認無誤後需回應系統管理者？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.10 軟體安裝完畢後是否立即更新廠商所預設之通行碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.11 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.12 通行碼長度是否規定須超過6個字元(建議以9位或以上)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.13 通行碼是否規定需有大小寫字母及數字組成？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.14 通行碼輸入錯誤，是否訂有三次以下之限制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.15 是否依規定期限或使用次數限制，要求變更通行碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.16 是否將輸入的通行碼顯示在螢幕上？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.17 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）當做通行碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(6)

頁次： 9/16

檢 查 項 目	是	否	不適 用
6.18 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.19 對於無人看管之資訊設施是否有適當保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.20 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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.21 是否訂有重要資訊不得閒置於桌面及螢幕淨空政策？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.22 網路使用者(含外單位人員)是否取得正式存取授權？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.23 是否訂定網路服務存取安全政策？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.24 對於外部連線使用者是否進行身份鑑別機制，如密碼技術、硬體符記或詰問/應答(Challenge/Response)協定等安全技術？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.25 無線網路之存取及應用，是否訂有鑑別控制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.26 對於遠端使用者的存取控制，是否有適當的鑑別機制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.27 是否使用自動識別設備，以鑑別來自特定地點或設備之連線？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.28 如需採用遠端診斷作業方式，是否有訂定診斷埠的存取作業規範(如用金鑰管理及人員身份查驗或稽核等機制)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.29 是否依據網路服務需要區隔出獨立的邏輯網域(如組織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)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.30 是否針對電子郵件、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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.31 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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.32 登入程序，是否避免提供輔助訊息(含登入失敗訊息)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.33 是否限制登入失敗次數的上限(建議三次)並中斷連線？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.34 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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(6)

頁次：10/16

檢 查 項 目	是	否	不適 用
6.35對於異常登入程序，是否留有紀錄，並有專人定期檢視？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.36是否於登入作業完成後顯示前一次登入的日期與時間，或提供登入失敗的詳細資料？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.37使用者是否均有唯一的識別碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.38重要系統使用者除採一般識別碼外，是否採用適切的身份鑑別技術？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.39通行碼是否避免以網路且明文方式告知申請者？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.40使用系統公用程式是否作授權管制及身份鑑別程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.41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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.42對風險高的應用系統是否限制其連線作業需求？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.43對風險高的應用系統是否設定連線時間限制？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.44是否訂有使用者對應用系統資訊存取之權限管制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.45機密及敏感性資料的處理是否採用專屬(隔離)的電腦作業環境	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.46是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.47遠距工作是否得到管理階層授權和施以必要之保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.48主機、伺服器、個人電腦、終端機等電腦設備於不使用、人員離座時是否即刻進行保護措施如關機、登出、設定螢幕密碼或是以其他控制措施進行保護？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(7)

頁次：11/16

檢 查 項 目	是	否	不適 用
7. 系統發展與維護安全管理			
7.1 應用系統在規劃需求時是否將安全要求納入分析及規格？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.2 輸入資料是否作檢查，以確認其正確且適切性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.3 應用程式內部處理是否加入檢查措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.4 應用系統是否使用密碼技術，以鑑別與保護訊息的完整性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.5 輸出資料是否具檢查確認功能？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.6 對高度機敏性的資料在傳輸或儲存中是否使用加密技術？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.7 密碼金鑰管理是否有作業標準或管理程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.8 作業系統軟體更新是否需經管理階層授權之人員處理？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.9 作業系統升級前是否作變更營運要求及版本安全性評估？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.10 測試作業是否避免以真實資料進行？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.11 原始程式庫之存取控制，是否訂有控制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.12 原始程式庫之存取行為，是否留有稽核日誌？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.13 是否建立應用系統之變更管制程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.14 系統變更後是否立即更新系統文件？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.15 作業系統變更後，是否對應用系統作技術性審查？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.16 系統變更後，是否主動公告異動範圍、時間、可能的影響？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.17 系統變更後檢查其相關控管措施與程序是否仍然有效？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.18 委外開發之系統上線前是否偵測有無惡意程式？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.19 系統安裝後是否管制程式碼？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.20 委外開發合約中是否規範著作權之歸屬？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.21 訂約時是否簽訂安全履行條款與相關罰則？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.22 是否定期執行各項系統漏洞修補程式？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.23 進行系統修補前是否先作系統影響評估與測試，如風險評估後，再採取必要措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.24 應用程式可執行碼更新作業是否限定由授權的管理人員才可執行？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(8)

頁次：12/16

檢 查 項 目	是	否	不適 用
8 資訊資產分類及控管			
8.1 是否建置資產清冊且隨時維護更新？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2 各項資訊資產是否有明確的擁有者、管理者及使用者(含資訊、軟體、實體)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3 是否定義資訊與資產（含電子郵件、網路使用及行動設備等）之使用規則？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.4 資訊是否分類(區分機密性、敏感性及一般性)？是否建立資訊安全等級之分類標準？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.5 是否依據採用的各類資訊分類法，制定標示與處置管理程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.6 對於安全等級要求高的各類資訊，是否標示清楚？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(9)

頁次：13/16

檢 查 項 目	是	否	不適 用
9. 實體及環境安全管理			
9.1 是否界定重要實體區域並施予安全保護？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.2 人員進入重要實體區域是否實施安全控制措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.3 重要實體區域的進出權限是否定期審查並更新？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4 第三方支援服務人員進入重要實體區域是否經過授權並監視其活動？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6 安全區域是否與易燃物或危險物品保持安全距離？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8 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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9 辦公處所是否實施必要之保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.10 備援設備及備份媒體存放位置是否與重要實體區域保持安全距離？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.11 重要資訊處理設施是否與一般收發或裝卸區作實體隔離？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.12 重要資訊處理設施是否予特別保護並評估其有效性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.13 重要資訊設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.14 是否制訂資訊安全緊急應變處理程序？有否定期演練及測試？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.15 電源之供應及備援電源是否作安全上考量？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.16 通訊線路及電纜線是否作安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.17 電源線與通訊纜線是否分隔，以防止互相干擾。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(9)

頁次：14/16

檢 查 項 目	是	否	不適 用
9.18設備是否定期維護保養，以確保其可用性及完整性？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.19設備送場外維修，對於儲存資訊是否訂有安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.20在外使用資訊設備或存取資料是否訂有安全保護措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.21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)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.22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或實施安全性覆寫？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.23設備報廢後如確定不再使用時，是否將儲存之資料及軟體移除後並做實體破壞？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.24若屬機密性、敏感性之手稿或影印公文廢紙及已過保存期限之公文，棄置之前是否予以銷毀？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.25資訊資產如須攜出場外使用，是否均經事前授權，並作安全查核？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.26各項安全設備是否定期檢查？員工有否施予適當的安全設備使用訓練？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.27電腦機房內是否嚴禁存放易燃物及未經核准之電器或其他物品？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(10)

頁次：15/16

檢 查 項 目	是	否	不適用
10. 業務永續運作計畫管理			
10.1 是否已擬訂關鍵性業務及其衝擊影響分析？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2 是否對可能造成營運中斷之機率及衝擊進行風險評鑑？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3 是否擬訂營運持續計畫(含資訊安全的持續計畫，內容包括：起動條件、參與人員、緊急程序、後撤程序、回復程序、維護時程、教育訓練、職責說明、所須資源、往來機構之應變規劃及適當性合約等)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4 營運持續計畫是否定期審查、測試、演練、維護、更新？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5 營運持續計畫是否配合業務、組織及人員之變更而更新？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6 是否建立資安事件(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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.7 系統或服務之安全弱點，是否通報至所有員工、承包商及第三方使用者？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.8 是否建立資安事故管理責任及應變程序？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.9 是否建立資安事故管理機制，如記錄事故型式、處置方法、處理成本及矯正預防措施？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.10 內部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？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.11 是否已建立及使用各項指標，以協助偵測安全事件，並預防安全事故？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.12 資安事件中相關證據資料是否有適當保護措施？以作為問題分析及法律必要依。	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.13 永續經營管理是否隨法令更新？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.14 緊急應變計畫是否納入內部教育訓練？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.15 緊急應變程序是否設有對外發言的處理機制？是否結合相關單位及地方警消單位？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

資訊安全管理內部稽核表(11)

頁次：16/16

檢 查 項 目	是	否	不適用
11 資訊安全系統稽核			
11.1 是否定期辦理資訊安全內部稽核？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2 內部稽核範圍是否涵括資訊系統、供應商、資訊資產負責人、使用者和管理階層？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3 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)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.4 稽核時的存取行為是否作監控與並留有紀錄？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5 稽核結果是否文件化？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.6 稽核後是否產生稽核報告並追蹤改善情形(包括稽核發現的摘要、稽核區域、缺失說明及改進建議等)？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.7 稽核人員是否經過訓練，並作事前工作分配？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.8 是否指派專人負責有關個人資料保護法規之蒐集、公告、實施作為？	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>