附件六：

資訊安全管理自我檢視表

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。

資訊安全管理自我檢視表

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？	☐	☐	☐
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？	☐	☐	☐
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)？	☐	☐	☐
1.4 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？	☐	☐	☐
1.5 資訊安全政策是否由管理階層每年至少審查一次？	☐	☐	☐
1.6 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？	☐	☐	☐
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？	☐	☐	☐
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？	☐	☐	☐
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？	☐	☐	☐
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？	☐	☐	☐
2.5 是否訂定員工資訊安全作業程序與權責規範？	☐	☐	☐
2.6 是否訂定各項資訊設備的安全作業程序？	☐	☐	☐
2.7 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？	☐	☐	☐
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？	☐	☐	☐
3.2 對人員之進用及調派，是否作適當之安全評估？	☐	☐	☐
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？	☐	☐	☐

資訊安全管理自我檢視表

檢　查　項　目	是	否	不適用
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？	☐	☐	☐
3.5 員工是否瞭解單位資訊安全政策及應負之資安責任？	☐	☐	☐
3.6 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？	☐	☐	☐
3.7 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？	☐	☐	☐
3.8 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？	☐	☐	☐
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？	☐	☐	☐
4.2 是否訂定電腦當機及服務中斷後之緊急處理程序？	☐	☐	☐
4.3 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？	☐	☐	☐
4.4 電腦設備設置前是否進行容量規劃並預留安全容量？	☐	☐	☐
4.5 是否使用網路防火牆(Fire Wall)？	☐	☐	☐
4.6 是否全面使用防毒軟體並即時更新病毒碼？	☐	☐	☐
4.7 是否定期對電腦系統及資料儲存媒體進行病毒掃描？	☐	☐	☐
4.8 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)？	☐	☐	☐
4.9 重要的資料及軟體是否定期作備份處理？	☐	☐	☐
4.10 備份資料是否定期回復測試，以確保備份資料之有效性？	☐	☐	☐
4.11 是否訂有資訊安全事故建立通報程序？	☐	☐	☐

資訊安全管理自我檢視表

檢　查　項　目	是	否	不適用
4.12資訊安全事件處理的過程是否均留有完整記錄？	☐	☐	☐
4.13是否遵守軟體授權規定，禁止使用未取得授權的軟體？	☐	☐	☐
5. 網路安全管理			
5.1 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？	☐	☐	☐
5.2 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？	☐	☐	☐
5.3 是否使用網路安全防禦設備？	☐	☐	☐
5.4 是否定期檢討網路安全控管事項之執行？	☐	☐	☐
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？	☐	☐	☐
6.2 是否訂定使用者存取權限註冊及註銷之作業程序？	☐	☐	☐
6.3 是否要求使用者對其個人通行碼應盡保護及保密責任？	☐	☐	☐
6.4 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？	☐	☐	☐
6.5 對於忘記通行碼之處理，是否要求須作身份確認程序？	☐	☐	☐
6.6 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？	☐	☐	☐
6.7 通行碼長度是否規定須超過6個字元(建議以9位或以上)?	☐	☐	☐
6.8 通行碼是否規定需有大小寫字母及數字組成？	☐	☐	☐
6.9 通行碼輸入錯誤，是否訂有三次以下之限制？	☐	☐	☐
6.10是否依規定期限或使用次數限制，要求變更通行碼？	☐	☐	☐

資訊安全管理自我檢視表

檢　查　項　目	是	否	不適用
6.11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？	☐	☐	☐
6.12網路使用者(含外單位人員)是否取得正式存取授權？	☐	☐	☐
6.13是否訂定網路服務存取安全政策？	☐	☐	☐
6.14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？	☐	☐	☐
6.15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？	☐	☐	☐
6.16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	☐	☐	☐
6.17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？	☐	☐	☐
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？	☐	☐	☐
7.2 對高度機敏性的資料在傳輸或儲存中是否使用加密技術？	☐	☐	☐
7.3 訂約時是否簽訂安全履行條款與相關罰則？	☐	☐	☐
7.4 是否定期執行各項系統漏洞修補程式？	☐	☐	☐
8 資訊資產分類及控管			
8.1 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？	☐	☐	☐
8.2 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？	☐	☐	☐
8.3 對於安全等級要求高的各類資訊，是否標示清楚？	☐	☐	☐
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？	☐	☐	☐
9.2 人員進入重要實體區域是否實施安全控制措施？	☐	☐	☐

資訊安全管理自我檢視表

檢　查　項　目	是	否	不適用
9.3 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？	☐	☐	☐
9.4 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？	☐	☐	☐
9.5 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？	☐	☐	☐
9.6 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？	☐	☐	☐
9.7 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？	☐	☐	☐
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？	☐	☐	☐
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？	☐	☐	☐
10.3 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？	☐	☐	☐
10.4 是否建立資安事故管理責任及應變程序？	☐	☐	☐
10.5 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？	☐	☐	☐
10.6 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?	☐	☐	☐
10.7 緊急應變計畫是否納入內部教育訓練？	☐	☐	☐