資訊安全政策

就下列事項，實施資訊安全管理，並定期評估：

一、資訊安全政策訂定。

二、資訊安全權責分工。

三、人員管理及資訊安全教育訓練。

四、電腦系統安全管理。

五、網路安全管理。

六、系統存取控制管理。

七、系統發展及維護安全管理。

八、資訊資產安全管理。

九、實體及環境安全管理。

十、業務永續運作計畫管理。

十一、資訊安全稽核。

一、資訊安全政策訂定：

(一) 制定資訊安全政策，應包括下列事項：

1. 資訊安全之定義、資訊安全之目標及資訊安全之範圍等。

2. 資訊安全政策之解釋及說明，資訊安全之原則、標準以及員工應遵守之相關規定。

3. 推行資訊安全工作之組織、權責及分工。

4. 發生資訊安全事件之緊急通報程序、處理流程、相關規定及說明。

(二)資訊安全政策之訂定，應以書面、電子（E-MAIL）或其他方式通知員工及與機關連線作業之公私機關（構）、提供資訊服務之廠商共同遵行。

(三)資訊安全政策應至少每年評估一次，確保資訊安全實務作業之有效性。資訊安全政策評估，應由內部稽核單位辦理。

二、資訊安全權責分工：

(一) 指定高層主管人員，負責資訊安全管理事項之協調及推動，並得視需要，成立資訊安全管理之專責單位，統籌資訊安全政策、計畫、資源調度等事項之協調、研議。

(二) 資訊安全管理之分工原則如下：

1. 資訊安全相關政策、計畫、措施及技術規範之研議，以及安全技術之研究、建置及評估相關事項，由資訊室辦理。
2. 資料及資訊系統之安全等級研議、使用者權限需求等事項，由資訊室辦理。
3. 資訊機密維護及稽核使用管理事項，由稽核會同相關單位辦理。
4. 資訊資產安全及管理、緊急應變處理程序演練及測試，由資訊室辦理。
5. 資訊安全稽核作業，由稽核室辦理，並視實際狀況得不定期進行資訊安全稽核。

三、人員管理及資訊安全教育訓練：

(一) 對處理敏感性、機密性資料之人員及因工作需要須賦於系統管理權限之人員，應妥適分工，分散權責並建立評估及考核制度，及視需要建立人員相互支援制度。

(二) 對離（休、停）職人員，依據人員離（休、停）職之處理程序辦理，並於收到作業文件後立即取消使用各項系統資源所有權限。

(三) 依角色及職能為基礎，針對不同層級人員，視實際需要辦理資訊安全教育訓練及宣導，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

（四）各業務主管，須負責督導所屬員工之資訊作業安全，防範不法及不當行為。

四、電腦系統安全管理

(一)電腦系統作業程序及責任

1. 應依據電腦系統作業程序，以確保員工正確及安全的操作使用電腦，並作為系統發展、維護及測試作業的依據。

2. 電腦系統作業程序除載明執行每一項電腦作業的規定外，應包含電腦不正常停機及作業發生錯誤或遭遇非預期的電腦作業問題時之處理規定。

(二) 資訊安全事件之管理

應訂定資通安全事件(如資料檔案遭毀損或侵犯破壞、電腦不正常停機等)之處理作業程序，除遵循既訂的應變計畫外（如系統及服務之回復作業），尚應執行下列事項：

1.導致資訊安全事件原因之分析。

2.防止類似事件再發生之補救措施的規劃及執行。

3.電腦稽核軌跡及相關證據之蒐集。建立處理資訊安全事件之作業程序,並課予相關人員必要的責任,以便迅速有效處理資訊安全事件。

(三)日常作業之安全管理

1.重要的資料及軟體應定期執行備份作業外，並訂定災害回復計畫，定期實施災害回復演練。

2.資訊設施及系統的變更作業，應建立管控機制，對於電腦系統作業中斷及更正等異常事項，並應詳實記錄。

3.應建立軟體管理規定，使用具有智慧財產權的合法軟體，未經授權合法之軟體，並禁止使用。

4.電腦病毒之防範應採行必要的事前預防措施，防制電腦病毒入侵，並慎選功能完整的電腦病毒防制軟體，定期維護更新。

5.應建置監測系統，隨時監測電腦作業環境狀況(如溫度、溼度及電源供應之品質等)及相關因應措施。

(四)電腦媒體之安全管理

1.對可攜性移動的電腦媒體，應建立使用管理程序，以規範磁帶、磁碟、光碟及電腦輸出表等媒體之使用，及相關因應措施。

2.應建立機密性及敏感性資料媒體之處理程序,防止資料洩漏或不當使用。

3.應建立系統文件(包括系統流程、作業流程、資料結構、檔案格式及授權程序等)的安全保護措施，防止不當使用。

(五)資料及軟體交換之安全管理

1.進行資料或軟體資訊交換，應訂定正式的安全協定，並納入機密性及敏感性資料的安全保護事項及賦予有關人員的責任。

2.電腦媒體運送及傳輸過程，應有妥善的安全措施，以防止資料遭破壞、濫用或未經授權的取用。

3.電子資料交換為防止未經授權的資料存取及竄改,應採行特別的安全保護措施。

伍、網路安全管理

(一) 網路安全規劃作業

應建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取，並訂定網路安全政策。

(二)對於跨組織之電腦網路系統，應特別加強網路安全管理，並協定應遵循之網路安全規定。

(三)利用公眾網路傳送敏感性資訊，應採取特別的安全保護措施，以保護資料在公共網路傳輸的完整性及機密性,並保護連線作業系統之安全性。

(四)網路服務之管理

審慎賦予網路系統管理人員適當之權限,避免其接觸非業務範圍內之檔案，並應建立查核機制，預留稽核軌跡。

(五) 網路使用者之管理

被授權的網路使用者，只能在授權範圍內存取網路資源，不得將自己的登入身份識別與登入網路的密碼交付他人使用。禁止使用違反著作權、善良風俗或會妨害網路系統的正常運作之不法或不當的資訊。

(六) 主機安全防護

1.存放機密性及敏感性資料之大型主機或伺服器主機(如Domain Name Server 等)，除作業系統既有的安全設定外，應規劃安全等級較高之密碼辨識系統，以強化身份辨識之安全機制，防制非法使用者登入主機進行盜取、破壞等情事；必要時，使用電子簽章及電子信封等各種安全控管技術，以提升網路作業之安全性。

2.存放個人資料保護法中規範須保護資料之主機系統，如需連結於公眾網路,應經審慎評估並經由資訊主管同意後實施。

(七) 防火牆之安全管理

公司內部與外界公眾網路連接的網點，應加裝防火牆。防火牆系統及管控機制應依資料安全等級、網路設備更動等情況

定期檢討，以因應各種新型態網路攻擊。

（八）軟體輸入控制

經由網際網路下載軟體或資料檔案，得視業務特性及需要，由使用單位經核准事前測試及掃瞄，在確認安全無虞及不違反智慧財產權前提下，方得下載執行。

（九）網路資訊之管理：

1.對外開放的資訊系統中不得存放機密性及敏感性資料或文件，並對可能導致系統作業癱瘓等情事，預作有效的防範，以免影響機關的服務品質。

2.存放員工申請或註冊的私人資料檔案，應研究以安全方式處理，以防止資料被非法使用。

（十）電子郵件之安全管理

1.應依資訊安全政策及規定，明訂電子郵件的使用規定。

2.應建立電子郵件的安全管理機制，以降低電子郵件可能帶來的業務上及安全上的風險。

（十一）機密性資料或文件，不得以電子郵件傳送；機密性資料以外之敏感性資料如有電子傳送之必要，應經加密或電子簽章等安全處理後傳送。

（十二）網路設備備援與系統備援

1.網路系統中各主要主機伺服器(包括防火牆主機)應評量其對業務之急迫性設立備援主機，以備主要作業主機無法正常運作時之用。

2.網路系統中之防火牆與各主機應定期（或異動時）做系統備份，包括完整系統備份，系統架構設定備份以及稽核資料備份。

（十三）網路安全稽核

1.網路安全稽核事項

(1) 對網路系統管理人員或資訊安全主管人員的操作，均應建立詳細

的紀錄。

(2) 視業務需要，對於通過防火牆之特定網路服務，就其來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。特定網路服務由各單位自訂之。

2. 警示系統：依資訊安全規定，視需要建立警示系統，讓網路系統管理人員在特定的網路安全事件發生時，及時獲得警示性的訊號，俾利採取有效的防範措施，減少網路安全事件的發生。

3. 網路入侵之追查：網路入侵者之行為若觸犯法律規定，構成犯罪事實，應立即通報檢警憲調單位處理。

六、系統存取控制管理

(一) 系統存取控制規定

1. 應訂定資訊系統存取控制規定，並以書面、電子或其他方式告知員工遵守。

2. 業務系統應將其存取控制需求，明確告知系統服務提供者，以利其執行及維持有效的存取控制機制。

3. 業務應用系統擁有者，應訂定系統存取控制規定，並明定使用單位及使用人員的系統存取權利。

(二) 系統存取之管理

1. 應建立系統使用者註冊管理制度，並加強使用者通行碼之管理，通行碼應定期更新，最長不得超過三個月為原則。

2. 系統存取權限之配賦，應以執行業務及職務所必需者為限，當使用者調整職務及離(休)職時，應於收到作業文件後立即註銷其系統存取權限。

3. 終端使用者之識別碼及通行碼，均應限制使用，並嚴禁轉知他人，若已為他人知悉者，應即報告主管適時更新；凡因故被冒用致造成

不良後果，應負洩密之責。

4. 對各項作業及管理系統應賦予系統存取權限，並建立使用人員名冊，以加強安全管控；該存取權限之評估，以每六個月評估一次為原則。

5. 對被賦予系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

（三）網路存取之安全控制

1. 身分鑑別

開放公司以外的使用者從公眾網路與公司內部連線作業，應建立遠端使用者身分鑑別機制及網路節點之身分鑑別機制，以降低未經授權存取系統的風險。

2. 網路連線作業之控制

為確保系統安全，跨內部的網路系統可限制使用者之連線作業能力。

3. 強制性的通道

網路使用者端末機連接電腦系統之線路，應建立強制性的通道（如使用專線等），以防止未被授權的使用者從不同的管道進入電腦系統。

4. 網路之分隔

網路系統規模過於龐大者，可考量將不同使用者及電腦系統分開成不同之領域，各領域並應以特定的安全設施（如防火牆及網路閘門）加以保護，以降低可能之安全風險。

5. 應盡量避免允許系統服務廠商以遠端登入方式進行系統維修，否則應經審慎評估簽報資訊主管核可，並應加強安全控管，建立人員名冊，課其相關安全保密責任。

（四）電腦主機之存取控制

為加強電腦主機之安全管制，應以安全有效的使用者通行碼管理系

統，鑑別使用者身分。

（五）應用系統之存取控制

1.原始程式之存取控制

(1) 對應用系統原始程式之存取，應建立嚴格的安全控制機制。

應建立所有存取程式原始碼資料庫的稽核軌跡。

(2) 應用程式彙集之程式館，應指派一位程式館管理人負責程式之進館、改進、存放等管制作業，並將管制情形作成紀錄留存備查。

(3) 應用系統維護人員應配合程式館管理人員，定期或不定期檢視程式館內維護之程式名稱及建立時間等，如有異常情形，應即查明原因，報請資訊單位主管人員處理。

2.資訊存取之限制

(1) 依資訊存取規定，配賦應用系統的使用者與業務需求相稱的資料存取及應用系統使用權限(例如限定使用者僅能執行唯讀、寫入、刪除或執行等功能)。

(2) 處理敏感性資訊的應用系統，系統輸出的資料，應僅限於與使用目的有關者，且視業務需要輸出到指定的端末機及位址。

(3) 重要資料委外建檔者，不論在機關內外執行，均應採取適當及足夠之安全管控措施，防止資料被竊取、竄改、販售、洩露及不當備份等情形發生。

3.系統公用程式之安全管理

應建立電腦系統公用程式之安全控制措施，嚴格限制及控制電腦公用程式之使用。

（六）系統存取及應用之監督

1.應建立系統使用情形之監督程序，確保使用者只能執行授權範圍內的事項。

2.應建立及製作例外事件及資訊安全事項的稽核軌跡,並保存一段的時間，以作為日後調查及監督之用。

（七）公司外部人員存取資訊之安全管理

1.如開放外界與其連線作業，應評估可能的安全風險，決定必須採行或應特別強化的資訊安全需求項目。

2.開放外界連線作業，應事前簽訂契約或協定，明定其應遵守之資訊安全規定、標準、程序、及應負之責任。

（八）系統存取之稽核

建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業；系統中之稽核紀錄檔案，應禁止任意刪除及修改。

七、系統發展及維護之安全管理

（一）系統安全需求規劃

1.系統安全需求分析及規格

新發展的資訊系統，或是現有系統功能之強化，應在系統規劃之需求階段，即將安全需求納入系統功能。

2.除由系統自動執行的安控措施之外，亦可考量由人工執行安控措施；在採購套裝軟體時，亦應進行相同的安全需求分析。

3.系統的安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，對機關可能帶來的傷害程度。

4.凡屬有關安全控管程式非經權責單位授權，不得擅自更改。

資訊系統安全需求應考量事項：

(1) 重要業務系統，應建立例行性的稽核制度，建立稽核軌跡。

(2) 資訊系統應保護機密性或敏感性資料，防止洩漏或被竄改，必要時應使用資料加密等技術保護。

(3) 重要的業務資料，應複製備份資料並異地儲存。

(4) 應訂定電腦不正常停機之立即回復作業程序，尤其是對高使用率的系統應有妥適的回復措施。

(5) 應保護系統避免未經授權的竄改或是修改。

(6) 應儘可能促使系統滿足稽核人員的安全控制需求。

(二) 應用系統之安全

1. 資料輸入之驗證

輸進應用系統的資料，應在事前查驗〔例如是否有超出設定範圍的數值等〕，以確保資料的真確性。

2. 系統內部作業處理之驗證

系統內部的作業，應建立驗證資料正確性的作業程序，避免正確輸入資料到應用系統中，卻因系統處理錯誤或是人為因素而遭受破壞。利用系統提供的功能，做資料處理作業控制或批次控制，以達到檔案資料更新處理後的一致性。

3. 資料加密

對高敏感性的資料，應在傳輸或儲存過程中以加密方法保護。

4. 訊息真確性之鑑別

應利用訊息鑑別技術，偵測資料內容是否遭受未經授權的竄改，或驗證傳送之訊息內容是否遭受破壞。對重要的應用系統，應使用訊息鑑別技術保護資料內容之真確性。

(三) 應用系統軟體之安全

1. 作業軟體之控制

在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統的風險，作業用的應用程式更新作業，應限定只能由

授權的管理人員才可執行，且應建立應用程式的更新稽核紀錄。作業用的應用程式均應以目的程式為原則；除非核准，不得以原始程式作業。

2. 系統測試資料之保護：

應保護及控制測試資料，避免以含有個人資料的真實資料庫進行測試；如使用真實的資料進行測試時，應於事前將足以辨識個人的資料變更。測試完畢後，真實資料應立即從測試系統中刪除。真實資料的複製情形予以記錄，以備稽核運用。

（四）系統變更及維護環境之安全

1. 應用系統變更作業之控制程序

應建立正式的變更控制程序，並嚴格執行，以降低可能的安全風險；變更作業之控制程序，應確保系統安全控制程序不會被破壞，並確保程式設計人員只能存取系統作業所需的項目，且任何的系統變更作業，皆應獲得權責主管人員的同意。

2. 應依事前訂定的授權規定，執行變更作業，其控制程序應考量的事項：

(1) 在實際執行變更作業前，變更作業的細項建議，應取得權責主管人員之核准。

(2) 系統文件在每次完成變更作業後，應立即更新，舊版的系統文件亦應妥善保管及處理。

(3) 系統文件應有版別及啟用日期之識別。

(4) 所有的系統變更作業請求，皆應建立紀錄供稽核運用。

3. 作業系統變更之技術評估：

作業系統更新前應評估其對應用系統是否造成負面的影響，或產生安全問題。作業系統變更的評估及測試結果，如須進行必要的調整，應納入年度計畫。

4. 系統維護環境之安全控管

(1) 對廠商之軟體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。

(2) 核發短期及臨時性之系統辨識及通行密碼供廠商使用，於使用完畢後應立即取消其使用權限。

(3) 委商建置或維護軟硬體設施時，應在機關相關人員監督及陪同下為之。

八、資訊資產安全管理

(一) 資訊資產目錄之建立及保護

1.建立一份與資訊系統有關的資訊資產目錄，訂定機關資訊資產的項目，擁有者及安全等級分類等。

2.各機關制定資訊資產項目應包括下列項目：

(1) 資料資產：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、業務永續運作計畫等。

(2) 軟體資產：應用軟體、系統軟體、發展工具及公用程式等。

(3) 實體資產：電腦及通訊設備、媒體資料及其他技術設施。

(4) 技術服務資產：電腦及通信服務、其他技術性服務（如電源、空調)。

(二) 資訊安全等級分類

1.應依據「國家機密保護辦法」、「個人資料保護法」、及「行政資訊公開辦法」等相關法規、建立資訊安全等級之分類標準以及相對應的保護措施。

2.資訊安全分類標準應考量資料的機密性、資料正確性及可用性，以減少未經授權的系統存取或系統損害對機關業務造成衝擊。

3. 資訊安全可區分機密性(例如稅捐稽徵法第三十三條規定之稅務資料)、敏感性（如屬個人資料）及一般性等三類。

4. 界定資訊安全等級之責任，應由資料的原始產生者，或是指定的系統所有者負責。

5. 訂定之資訊安全等級分類時，應特別注意其與公司的資訊安全等級，在定義及標準，應取得一致。

九、實體及環境安全管理

（一）設備安全管理

1. 設備（應含電腦、電力及通訊纜線等）應安置在適當的地點並予以保護，以減少環境不安全引發的危險及減少未經授權存取系統的機會。

2. 電源供應應考量安置預備電源，並將不斷電系統失效之後的應變措施納入，對於特別敏感性或是特別重要的系統，應採取額外強化的安全措施。

3. 應妥善地維護設備，以確保設備的完整性及可以持續使用。

4. 設置在外部以支援業務運作的資訊設備，應同樣遵守資訊安全管理授權規定，維持與內部資訊設備一樣的安全水準。

5. 含有儲存媒體的設備項目(如硬碟)，應在處理前詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體已經被移除。

6. 為了防止資訊設施被誤用，提供的資訊設施，如有業務目的以外的使用，或是超出授權目的以外的使用需求，應經權責主管人員的核准，並課予相關人員的責任，若有不當使用情形應作適當的紀律處理。

（二）周邊安全管理

1. 周圍環境之安全：

(1) 實體環境的安全保護，應以事先劃定的各項周邊設施為基礎，並設置必要的障礙（如：門禁指紋管理），以達安全控管的目的。

(2) 實體環境的安全保護程度，應視資訊資產及系統價值的安全風險而決定。

2. 人員進出管制：

管制區內應有適當的進出管制保護措施（如：配資訊單位專人陪同），並記錄來訪人員進出時間和目的，以確保只有被授權的人員始得進入（如：電腦機房、媒體檔案庫房等）

3. 電腦廠商的資訊人員或維護服務人員，只有在被要求或是被授權的情形下，才能進入管制區域，並視需要限制（例如限制存取敏感性的資料）及監督其活動。

（三）電腦機房安全管理：

1. 電腦機房應設立良好的實體安全措施。

2. 凡進入電腦機房之人員，除應由資訊室專人陪同外，應於機房門口設置檢核或監錄等保護措施。

（四）辦公桌面之安全管理：

1. 應考量採用辦公桌面的淨空政策，以減少文件及磁碟片等在辦公時間外，遭人取用、遺失或被破壞的機會。

2. 個人電腦及電腦終端機不再使用時，應關機、離線或是其他控制措施。

（五）財產移轉的安全管理：

電腦設備、資料或軟體，未經許可，不得帶離辦公室。

十、業務永續運作計畫之規劃及管理

（一）業務永續運作之規劃

1. 應建立跨部門的業務永續運作計劃程序，研訂及維護業務持續運作之計畫。

2. 業務永續運作的規劃作業，應研析並降低人為或是意外因素對重要業務運作可能導致的威脅，使重要業務在資訊作業系統、資料檔案及人員發生事故、設施失敗或是受損害時，仍可持續運作。

3. 業務永續運作計畫應考量，評估各種災害對業務作業可能的衝擊、人員責任界定以及緊急應變措施之安排、建立作業程序及流程、進行員工教　育及訓練、測試緊急應變計畫、定期更新緊急應變計畫。

4. 業務永續運作計畫應考量訂定緊急應變作業程序、預備作業程序、回復作業程序、測試作業程序及相關人員之權責。

（二）業務永續運作計畫之測試

為使應變計畫維持有效性及相關人員確實瞭解計畫的最新狀態，應定期測試及演練，測試計畫可以個別計畫的方式進行，以減少測試完整計畫的需求及頻率。

（三）業務永續運作計畫之更新

1. 業務永續運作計畫應配合業務、組織、人員及法令等事項之變動，更新計畫內容。

2. 業務永續運作計畫之變更，應建立控管機制，並指定專人負責。

（四）資訊安全事件緊急處理機制

1. 應建立資訊安全事件的正式通報程序及管道，並訂定通報之後應採行之行動及措施。

2. 資訊安全事件發生時，應依事前訂定的通報管道，迅速通報權責主管單位。

十一、資訊安全稽核

（一）稽核計畫與執行

為加強資訊業務作業管制，有效運用電腦設備資源，應建立資訊安全稽核制度，由稽核單位查核。

（二）稽核業務應採內部稽核與外部稽核兩種方式實施：

1. 內部稽核：應於每年十二月底前，將次年資訊作業內部稽核計畫報請主管同意，復據以實施定期或不定期之內部稽核業務。

2. 外部稽核：視各受檢業務狀況，接受外部機關定期或不定期派員實施外部稽核業務。

（三）稽核績效與檢討

1. 實施稽核作業時，應詳實紀錄查核情形，並撰寫查核檢討報告，簽報主管核閱備查。

前項有關查核紀錄與檢討報告等，應由查核單位妥為保管，以供權責機關實施外部稽核時之參考。

2. 稽核報告之建議事項，應由業務主辦單位訂定改進方案據以執行，並辦理複核等管考工作。