行政院及所屬各機關資訊安全管理規範

88/11/16 行政院研考會（88）會訊字第 05787 號函頒

壹、資訊安全政策制定及評估

一、資訊安全政策制定

(一) 應依據電腦處理個人資料保護法、國家機密保護辦法與行政院及所屬各機關資訊安全管理要點等有關法令，衡酌機關業務需求，參考本規範訂定資訊安全政策，研訂資訊作業之安全水準，並以書面、電子或其他方式通知員工及與機關連線作業之有關機關（構）、廠商。

(二) 制訂資訊安全政策，應至少包括下列事項：

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，以及員工應遵守之規定，包括：
   (1) 政府法令及契約對機關資訊安全之要求及規定。
   (2) 資訊安全教育及訓練之要求。
   (3) 電腦病毒防範之要求。
   (4) 業務永續運作計畫。
3. 推行資訊安全工作之組織、權責及分工。
4. 員工應負的一般性及特定的資訊安全責任。

5. 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、資訊安全政策之評估

(一) 制訂之資訊安全政策，應定期進行獨立及客觀的評估，以反映政府資訊安全管理政策、法令、技術及機關業務之最新狀況，確保資訊安全之實務作業，確實遵守資訊安全政策，以及確保資訊安全實務作業之可行性及有效性。

(二) 資訊安全政策評估作業，可責由具有專業技術及知識之內部稽核單位、獨立客觀的資深主管人員，或是委請公正超然的民間專業組織或團體，進行資訊安全政策執行成果之評估。

(三) 應定期對所屬單位及人員進行資訊系統及技術應用之安全評估，以確保其遵守資訊安全政策及規定。

1. 應列入資訊安全評估的對象如下：

(1) 資訊設施及系統提供者。

(2) 資訊及資料擁有者。

(3) 使用者。

(4) 管理者。

(5) 系統維護者。

(6) 其他有關人員。

2. 資訊系統擁有者應配合定期的資訊安全評估，檢討相關人員是否遵守機關資訊安全政策、規範及有關安全規定。

3. 應定期檢討及評估各項軟、硬設備的安全性，以確保其符合機關訂定的安全標準；評估對象應包括作業系統之評估，以確保系統軟體及硬體的安全措施，正確及有效地執行。

4. 如專業人力及經驗不足，得委請民間專業組織團體或學者專家之協助。

5. 系統安全評估應由具有專業知識及豐富經驗的系統工程人員，在權責主管人員的監督下，以人工的方式執行，或是以自動化的軟體工具執行安全檢查，產生技術評估報告，以利日後解讀分析。

(四) 資訊安全政策及規定之宣達

1. 資訊安全政策及人員在資訊安全應扮演之角色及責任等有關規定，應在工作說明書或有關作業手冊中載明。

2. 工作說明書或作業手冊規定之資訊安全政策、說明及規定，應包括執行及維護資訊安全政策的一般性責任規定、保護特定資訊資產的特別責任規定，以及執行特別安全程序及作為的特別責任規定。

3. 員工如違反資訊安全相關規定，應依紀律程序處理。

貳、資訊安全組織及權責

1. 資訊安全組織

（一）應指定副首長或高層主管人員，負責推動、協調及督導下列資訊安全管理事項：

1、資訊安全政策之核定、核轉及督導。

2、資訊安全責任之分配及協調。

3、資訊資產保護事項之監督。

4、資訊安全事件之檢討及監督。

5、其他資訊安全事項之核定。

（二）得視需要成立跨部門資訊安全推行小組，推動下列事項：

1、跨部門資訊安全事項權責分工之協調。

2、應採用之資訊安全技術、方法及程序之協調研議。

3、整體資訊安全措施之協調研議。

4、資訊安全計畫之協調研議。

5、其他重要資訊安全事項之協調研議。

2. 資訊安全組織權責

（一）資訊安全責任分配

1、應訂定保護個人資訊資產及執行特定資訊安全作業，有關人員應負之責任。

2、應訂定有關人員在資訊安全作業應扮演之角色，責任分配之一般性指導原則，以作為各單位之權責分工依據。

3、每一系統應指定系統擁有者，並課予必要的安全責任。

4、應明定每一管理者應負的資訊安全責任。

5、應訂定每一系統的資訊資產項目，並訂定必要的安全程序及措施。

6、應指定每一項資訊資產及資訊安全程序的管理人員，並以書面、電子或其他方式告知其責任。

7、應訂定資訊安全之授權規定、授權等級及授權程序等並以書面、電子或其他方式記錄之。

（二）資訊安全分工原則

1、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，由資訊單位負責辦理。

（2）資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。

（3）資訊機密維護及稽核使用管理事項，由政風單位會同相關單位負責辦理。

2、設有稽核單位者，稽核使用管理事項由稽核單位會同政風單位辦理。

3、未設置資訊及政風單位者，由機關首長指定適當的單位及人員負責辦理資訊安全管理事項。

4、業務性質特殊者，得視實際需要由首長調整上述資訊安全分工原則。

（三）資訊設施之使用授權

1、引進及啟用新資訊科技（如軟體、硬體、通信及管理措施等），應於事前進行安全評估，瞭解新資訊科技之安全保護措施及水準，並依行政程序經權責主管人員核准，始得引用，以免影響既有的資訊安全措施。

2、新資訊科技設施之使用，應依下列行政程序辦理：

（1）業務上的核准程序

・每一項系統及設備的裝置及使用，應經權責主管人員的核准始得使用。

・系統及設備如有遠地連線作業需求，亦應獲得負責維護當地資訊安全之權責主管人員之同意。

（2）技術上的核准程序：所有連上網路的設施，或是由資訊服務提供者維護的設施,須經技術上的安全評估程序及權責主管人員之核准，始得上線使用。

（四）跨機關之合作及協調

1、資訊安全管理人員應與外部的資訊安全專家或顧問加強協調聯繫，相互合作，分享經驗，以評估機關可能面臨的資訊安全威脅，據以研擬及推動資訊安全實務措施。

2、應與業務密切相關的機關、執法機關、資訊服務提供者及通信機構等，建立及維持適當的互動管道，以便在發生資訊安全事件時，能迅速獲得外部的資源協助，即時解決相關問題。

3、記載資訊安全事項之有關文件或資訊，在提供外界使用及進行經驗交流時，應予適當的限制，以防止載有資訊安全細節的敏感性資訊，遭未經授權的人員取用。

（五）資訊安全顧問及諮詢

1、資訊安全人力、能力及經驗，如有不足之處，得委請外界的學者專家或民間專業組織及團體,提供資訊安全顧問諮詢服務。

2、對委請資訊安全顧問，或負責資訊安全之人員，各單位及人員應予必要的協助及支援。

參、人員安全管理及教育訓練

一、人員進用之評估

（一）人員進用之安全評估

1、進用之人員，如其工作職責須使用處理敏感性、機密性資訊的科技設施，或須處理機密性及敏感性資訊者，應經適當的安全評估程序。

2、人員進用之安全評估參考項目如下：

（1）個人性格。

（2）申請者之經歷。

（3）學術及專業能力及資格。

（4）人員身分之確認。

（5）財物及信用狀況。

（二）機密維護之責任約定

1、員工使用資訊科技設施，應依相關法令課予機密維護責任，並應儘可能簽署書面約定，以明責任。

2、當人員任用及約聘僱條件或契約有所變更時，尤其是人員離職或是約聘僱用契約終止時,應重新檢討機密維護責任約定之妥適性。

二、使用者資訊安全教育訓練

（一）資訊安全教育訓練

1、應定期對員工進行資訊安全教育及訓練，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。

2、應以人員角色及職能為基礎，針對不同層級的人員，進行適當的資訊安全教育及訓練;資訊安全教育及訓練的內容應包括：資訊安全政策、資訊安全法令規定、資訊安全作業程序，以及如何正確使用資訊科技設施之訓練等。

3、在同意及授權使用者存取系統前，應教導使用者登入系統的程序，以及如何正確操作及使用軟體。

4、對員工進行資訊安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

肆、電腦系統安全管理

一、電腦系統作業程序及責任

（一）電腦系統作業程序之訂定

1、應訂定電腦系統作業程序，並以書面、電子或其他方式載明之，以確保機關員工正確及安全地操作及使用電腦，並以其作為系統發展、維護及測試作業的依據。

2、電腦系統作業程序應載明執行每一項電腦作業的詳細規定：

（1）如何正確地處理資料檔案。

（2）電腦系統作業時程的需求，包括與其他系統的相互關係、作業啟動的最早時間及作業結束的最晚時間。

（3）處理電腦當機及發生作業錯誤之規定，以及其他電腦系統作業之限制事項。

（4）如果遭遇非預期的電腦系統作業技術問題時，如何與支援人員聯繫之規定。

（5）資料輸出處理的特別規定，例如：使用特別的文具，或是對機密資料輸出之管理、電腦當機或作業錯誤時，輸出資訊之安全處理規定等。

（6）電腦當機重新啟動及回復正常作業之程序。

（7）電腦及網路之日常管理作業，例如：開關機程序、資料備援、設備維護、電腦機房之安全管理；

電腦系統作業程序應視為正式文件，作業程序的更改必須經權責單位核准。

（二）資訊安全事件之管理

1、應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。

2、發生資訊安全事件之反應與處理作業程序，應納入下列事項：

（1）電腦當機及中斷服務。

（2）業務資料不完整，或資料不正確導致的作業錯誤。

（3）機密性資料遭侵犯。

3、除正常的應變計畫外（如系統及服務之回復作業），資訊安全事件之處理程序，尚應納入下列事項：

（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。

（4）與使用者及其他受影響的人員，或是負責系統回復的人員進行溝通及瞭解。

4、電腦稽核軌跡及相關的證據，應以適當的方法保護，以利下列管理作業：

（1）作為研析問題之依據。

（2）作為研析是否違反契約或是違反資訊安全規定的證據。

（3）作為與軟體及硬體之供應商，協商如何補償之依據。

5、應以審慎及正式的行政程序，處理資訊安全及電腦當機事件。作業程序應該包括下列事項：

（1）應在最短的時間內，確認已回復正常作業的系統及安全控制系統，是否完整及真確。

（2）應向管理階層報告緊急處理情形，並對資訊安全事件詳加檢討評估，以找出原因及檢討改正。

（3）應限定只有被授權的人員，才可使用已回復正常作業的系統及資料。

（4）緊急處理的各項行動，應予詳細記載，以備日後查考。

（三）資訊安全責任之分散

1、為降低因人為疏忽或故意，導致資料或系統遭不法或不當之使用，或遭未經授權的人員竄改，對關鍵性的資訊

業務，應將資訊安全管理及執行的責任分散，分別配賦相關人員必要的安全責任。必要時，應建立相互制衡機制。

2、如資訊人力資源許可，應儘可能分由不同的人員執行下列業務及功能：

（1）業務系統之使用。

（2）資料建檔。

（3）電腦作業。

（4）網路管理。

（5）系統行政管理。

（6）系統發展及維護。

（7）變更管理。

（8）安全管理。

（9）安全稽核。

（四）系統發展及系統實作之分開處理

1、系統發展及測試作業可能會有軟體變更及電腦資源共享之情形，為降低可能的風險，應將系統發展及系統實作的設施分開處理，以減少作業軟體或資料遭意外竄改，或是遭未經授權的存取。

2、系統發展及系統實作之分開處理，應考量下列安控措施：

（1）系統發展及系統實作的軟體，應儘可能在不同的處理器上作業，或是在不同的目錄或領域下作業。

（2）系統發展及測試作業應儘可能分開。

（3）編輯器及其他公用程式不再使用時，不得與作業系統共同存放。

（4）實作及測試用的系統，應使用不同的登入程序，以減少風險。

（五）資訊作業委外服務之安全管理

1、資訊業務委外時，應於事前審慎評估可能的潛在安全風險(例如資料或使用者通行碼被破解、系統被破壞或資料損失等風險)，並與廠商簽訂適當的資訊安全協定，以及課予相關的安全管理責任，並納入契約條款。

2、應納入資訊委外服務契約的資訊安全事項如下：

（1） 涉及機密性、敏感性或是關鍵性的應用系統項目。

（2）應經核准始得執行的事項。

（3）廠商如何配合執行機關業務永續運作計畫。

（4）廠商應遵守的資訊安全規範及標準，以及評鑑廠商遵守資訊安全標準的衡量及評估作業程序。

（5）廠商處理及通報資訊安全事件的責任及作業程序。

二、系統規劃

（一）系統作業容量之規劃

1、應隨時注意及觀察分析系統的作業容量，以避免容量不足而導致電腦當機。

2、應進行電腦系統作業容量之需求預測，以確保足夠的電腦處理及儲存容量。

3、應特別注意系統之作業容量，預留預算及採購行政作業的前置時間，俾利進行前瞻性的規劃，及時獲得必要的作業容量。

4、系統管理人員，應隨時注意及觀察分析系統資源使用狀況，包括處理器、主儲存裝置、檔案儲存、印表機及其他輸出設備及通信系統之使用狀況;管理人員應隨時注意上述設備的使用趨勢,尤應注意系統在業務處理及資訊管理上的應用情形。

5、應隨時掌握及利用電腦及網路系統容量使用狀況的資訊，分析及找出可能危及系統安全的瓶頸，預作補救措施之規劃。

（二）新系統上線作業之安全評估

1、應訂定新系統被認可及納入正式作業的標準，並在新系統上線作業前，執行適當的測試。

2、新系統被認可及納入正式作業的標準，應執行下列事項：

（1）應評估系統作業效能及電腦容量是否滿足機關的需求。

（2）應檢查發生錯誤後之回復作業及系統重新啟動程序的準備作業，以及資訊安全事件之緊急應變作業完備與否。

(3)應進行新系統正式納入例行作業程序之準備及測試。

（4）應評估新系統的建置是否影響現有的系統作業，尤其是對系統尖峰作業時段之影響。

（5）應辦理新系統作業及使用者教育訓練。

3、在發展重要的系統時，應確定系統的功能，以及確保系統的作業效能，使其足以滿足需求；例如，在系統發展的每一階段，應充分諮詢相關人員的意見。

4、新系統上線作業前，應執行適當的測試作業，以驗證系統功能符合既定的安全標準。

（三）預備作業之規劃

1、應規劃資訊系統設備損害或電腦當機時，可維持機關業務繼續正常作業的替代性預備作業方法。

2、每一系統的預備作業需求，應在業務永續運作的基礎上，由系統的擁有者加以界定；資訊服務提供者亦應為每一項系統研訂適當的預備作業計畫。

3、應定期測試預備作業的設備及程序。

（四）作業變更之管理

1、資訊設施及系統的變更，應建立控制及管理機制，以免造成系統安全上的漏洞。

2、作業變更之管理，應執行之事項如下：

（1）界定及記錄重大變更的事項。

（2）評估作業變更之可能衝擊。

（3）建立作業變更之程序。

（4）與相關使用者事前溝通作業變更之細節。

（5）作業變更不能順利執行時之回復作業程序及責任，或放棄執行作業變更之作業程序及責任。

三、電腦病毒及惡意軟體之防範

（一）電腦病毒及惡意軟體之控制

1、應採行必要的事前預防及保護措施，防制及偵測電腦病毒、特洛依木馬及邏輯炸彈等惡意軟體的侵入。

2、應依「事前預防重於事後補救」的原則，採行適當及必要的電腦病毒偵測及防範措施,促使員工正確認知電腦病毒的威脅，進一步提升員工的資訊安全警覺，健全系統之存取控制機制。

3、電腦病毒防範應考量的重要原則如下：

（1）應建立軟體管理政策，規定各部門及使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。

（2）應選用信譽良好、功能健全的電腦病毒防制軟體，並依下列原則使用：

・電腦病毒防治軟體應定期更新，並在廠商的指導下使用。

・使用防毒軟體事前掃瞄電腦系統及資料儲存媒體，以偵測有無感染電腦病毒。

・視需要安裝可偵測軟體遭更改的工具軟體，並偵測執行碼是否遭變更。

・應謹慎使用可掃除電腦病毒及回復系統功能的解毒軟體；使用前應充分瞭解電腦病毒的特性，以及確定解毒軟體的功能。

・應定期檢查軟體及檢查重要的系統資料內容，如發現有偽造的檔案或是未經授權的修正事項，應立即調查，找出原因。

・對來路不明及內容不確定的磁片，應在使用前詳加檢查是否感染電腦病毒。

・應建立防制電腦病毒攻擊及回復作業的管理程序，並課予相關人員必要的責任。

・為使電腦病毒影響機關正常運作之程度降至最低，應建立妥適的業務永續運作計畫，將必要的資料及軟體備份，事前訂定回復作業計畫。

四、軟體複製的控制

1、機關使用有智慧財產權的軟體，應遵守相關法令及契約規定。

2、軟體複製應考量之事項如下：

（1）不應保有及使用未取得授權的軟體。

（2）應將機關智慧財產權保護政策，以書面、電子或其他方式明確通知機關員工，禁止員工在未取得智慧財產權擁有者的書面同意前，將軟體複製到機器。

（3）除非取得授權，不應將專屬的軟體複製到機關以外的機器設備。

（4）須在原授權許可之外的機器上使用軟體時，應取得正式的授權或另行採購。

（5）應建立軟體使用的註冊管理機制，並定期稽核軟體使用情形。

五、個人資料之保護

1、應依據電腦處理個人資料保護法等相關規定，審慎處理及保護個人資訊。

2、應建立個人資料控制及管理機制，並視需要指定負責個人資料保護之人員，以便協調管理人員、使用者及系統服務提供者，促使相關人員瞭解各部門應負的個人資料保護責任，以及應遵守之作業程序。

六、日常作業之安全管理

（一）資料備份

1、應準備適當及足夠的備援設施，定期執行必要的資料及軟體備份及備援作業,以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

2、系統資料備份及備援作業，應符合機關業務永續運作之需求。

3、資料備份作業原則如下：

（1）正確及完整的備份資料，除存放在主要的作業場所外，應另外存放在離機關有一段距離的場所，以防止主要作業場所發生災害時可能帶來的傷害。

（2）重要資料的備份，以維持三代為原則。

（3）備份資料應有適當的實體及環境保護，其安全標準應儘可能與主要作業場所的安全標準相同；主要作業場所對電腦媒體的安控措施，應儘可能適用到備援作業場所。

（4）應定期測試備份資料，以確保備份資料之可用性。

（5）資料的保存時間，以及檔案永久保存的需求，應由資料擁有者研提。

（二）系統作業紀錄

1、電腦作業人員應忠實記錄系統啟動及結束作業時間、系統錯誤及更正作業等事項。

2、電腦作業人員的系統作業紀錄，應定期交由客觀的第三者查驗，以確認其是否符合機關訂定的作業程序。

（三）系統錯誤事項之紀錄

1、系統發生作業錯誤時，應迅速報告權責主管人員，並採取必要的更正行動。

2、使用者對電腦及通信系統作業錯誤的報告，應正式記錄，以供日後查考。

3、應建立明確的系統作業錯誤報告程序，以及相關的作業規定，要項如下：

（1）應檢查錯誤情形的紀錄，確保系統作業錯誤已經改正。

（2）應檢查更正作業是否妥適，確保更正作業未破壞系統原有的安控措施,及確保更正作業係依正當的授權程序辦理。

（四）電腦作業環境之監測

電腦作業環境如溫度、溼度及電源供應之品質等，應依據供應廠商的建議，建立監測系統，隨時監測電腦作業環境，並採取必要的補救措施。

七、電腦媒體之安全管理

（一）電腦媒體之安全管理

1、可隨時攜帶及移動的電腦媒體，應建立使用管理程序，以規範磁帶、磁碟及電腦輸出報告等媒體之使用。

2、電腦作業環境應建置下列安全控管措施：

（1）應儘量避免使用有明顯用途標示的資料儲存系統；電腦媒體儲存的資料內容，不應在媒體外部以明顯方式標示，以免被輕易地辨識。

（2）可重複使用的資料儲存媒體，不再繼續使用時，應將儲存的內容消除。

（3）對於要帶離辦公場所的儲存媒體，應建立書面的授權規定，並建立使用紀錄，以備日後稽核。

（4）儲存媒體應依製造廠商提供的保存規格，存放在安全的環境。

（二）機密性及敏感性資料之處理程序

1、應建立機密性及敏感性資料的處理程序，防止洩漏或不法及不當的使用。

2、應研訂處理機密性及敏感性資料的輸入及輸出媒體之安全作業程序，例如：文件、磁帶、磁片、書面報告及空白支票、空白收據等項目。

3、機密性及敏感性資料之安全處理作業，應包括下列事項：

（1）輸出及輸入資料之處理程序及標示。

（2）依授權規定，建立收受機密性及敏感性資料的正式收文紀錄。

（3）確保輸入資料之真確性。

（4）儘可能要求收受者提出傳送之媒體已送達的收訖證明。

（5）分發對象應以最低必要的人員為限。

（6）為提醒使用者注意安全保密，應在資料上明確標示資料機密等級。

（7）應定期評估機密性及敏感性資料的發文清單，及檢討評估內容。

（8）應確保資訊系統內部資料與外部資料之一致性。

（三）系統文件之安全

1、系統流程、作業流程、資料結構及授權程序等系統文件，應予適當保護，以防止不當利用。

2、系統文件的安全保護措施如下：

（1）應鎖在安全的儲櫃或其他安全場所。

（2）發送對象應以最低必要的人員為限，且應經系統擁有者的授權。

（3）電腦產製的文件，應與其他應用檔案分開存放，且應建立適當的存取保護措施。

（四）媒體處理之安全

1、儲存機密性及敏感性資料的電腦媒體，當不再繼續使用時，應以安全的方式處理。

2、應訂定電腦媒體的處理作業程序，以降低可能的安全風險。

3、電腦媒體之安全處理原則如下：

（1）內含機密性或敏感性資料的媒體，應以安全的方式處理，例如：燒毀或是以碎紙機處理，或將資料從媒體中完全清除。

（2）應建立須以安全方式處理的媒體項目清單，包括：

• 輸入文件，例如電傳文件。

• 複寫紙。

• 輸出報告。

• 印表機色帶。

• 磁帶。

• 可攜帶的磁片或是磁帶。

• 作業程序目錄。

• 測試資料。

• 系統文件。

• 其他。

4、委外處理的電腦文具、設備、媒體蒐集及委外處理資料,應慎選有足夠安全管理能力及經驗的機構作為委辦對象。

5、機密性及敏應性資料的處理過程，應以書面、電子其他方式記錄之，以利事後查考及稽核。

6、資訊累積一段時間再作彙總處理時，應特別注意及防止大量非機密性資料彙總成為敏應性或機密性資料。

（五）資料檔案之保護

1、應保護重要的資料檔案，以防止遺失、毀壞、被偽造或竄改。重要的資料檔案應依相關規定，以安全的方式保存。

2、超過法定保存時限的檔案，可依相關規定刪除或銷毀，惟應事前考量對機關造成影響。

3、資料檔案的管理，應遵循以下的步驟：

（1）訂定檔案保存、儲存、處理等指導原則作為執行的依據。

（2）檔案保存期限應依檔案型態及法定保存期限之規定擬訂。

（3）應建立及維護重要資訊資源之目錄。

（4）應採行適當的措施，保護重要檔案及資訊，防止資料遺失、毀壞及被偽造或竄改。

八、資料及軟體交換之安全管理

（一）資料及軟體交換之安全協定

1、機關間進行資料或軟體交換，應訂定正式的協定，將機密性及敏感性資料的安全保護事項及有關人員的責任列入。

2、機關間資料及軟體交換的安全協定內容，應考量下列事項：

（1）控制資料及軟體傳送、送達及收受的管理責任。

（2）控制資料及軟體傳送、送達及收受的作業程序。

（3）資料、軟體包裝及傳送的最基本的技術標準。

（4）識別資料及確定軟體傳送者身分的標準。

（5）資料遺失的責任及義務。

（6）資料及軟體的所有權、資料保護的責任、軟體的智慧財產權規定等。

（7）記錄及讀取資料及軟體的技術標準。

（8）保護機密或敏感性資料的安全措施（例如使用加密技術）

（二）電腦媒體運送及傳輸之安全

1、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、誤用或未經授權的取用。

2、電腦媒體運送及傳輸，應考量的安全措施參考要項如下：

（1）應審慎選用安全及可信賴的運送或傳送機構或人員，報請權責主管人員同意，並於事前執行傳遞人員或機構的安全評估程序。

（2）運送的物品應有妥適的包裝，以防止傳送過程中受損。

（3）對於機密及敏感性的資料，應採取特別的安全保護措施。

（三）電子資料交換之安全

1、機關與來往對象進行電子資料交換，應採行特別的安全保護措施，以防止未經授權的資料存取及竄改；資料電子交換如有安全及責任上的考量，應建立發文及收文證明的機制。

2、機關訂定的電子資料交換安全措施，應與電子資料交換的對象及資料加值服務業者共同協商，並徵詢電子資料交換相關組織之意見，以確保符合相關的標準。

（四）電子辦公系統之安全

1、應訂定電子辦公系統的使用政策及指導原則，以確保實施辦公電子化在業務及系統上之安全。

2、電子辦公系統應考量的安全事項如下：

（1）電子辦公系統如未能提供適當及足夠的安全保護措施，不應將敏感性資訊列入系統目錄。

（2）應訂定資料流通及分享的政策及管理措施（例如:應訂定電子佈告欄系統應用政策。）

（3）對於特定個人（如首長或負責處理機密性或敏感性資訊的人員）的行程資訊等，不宜開放公開存取，並予適當的限制。

（4）應評估以電子辦公系統處理機關重要業務的適當性（例如:評估以電子通信系統傳達命令及線上授權的妥適性。）

（5）應建立被授權使用電子辦公系統的員工、其他機關的員工及訂有契約廠商人員的名單，並建立使用者存取系統權限等資訊。

（6）特定的電子辦公設施，應限制只有特定人員才能使用。

（7）應訂定系統儲存資訊的保管作業及備援作業規定。

（8）電腦當機的備援作業規定。

伍、網路安全管理

一、網路安全規劃與管理

（一）網路安全規劃作業

1、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。

2、對於跨組織之電腦網路系統，應特別加強網路安全管理。

3、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。

4、網路安全管理應考量之事項如下：

（1）應儘可能將電腦作業及網路作業的責任分開。

（2）應建立管理遠端設備的責任及程序。

（3）應密切協調電腦及網路管理作業，以便發揮網路系統最大的服務功能，確保網路安全措施可以在跨部門的基礎架構上運作。

（二）網路服務之管理

1、系統的最高使用權限,應經權責主管人員審慎評估後，交付可信賴的人員管理。

2、網路系統管理人員應負責網路安全規範的擬訂，執行網路管理工具之設定與操作,確保系統與資料的安全性與完整性。

3、網路系統管理人員應負責製發帳號，提供取得授權的人員使用；除非有特殊情況，不得製發匿名或多人共享的帳號。

4、提供給內部人員使用的網路服務，與開放有關人員從遠端登入內部網路系統的網路服務,應執行嚴謹的身分辨識作業(如使用動態密碼辨識系統),或使用防火牆代理伺服器(Proxy Server)進行安全控管。

5、如果系統使用者已非合法授權的使用者時，網路系統管理人員應立即撤銷其使用者帳號；離（休）職人員應依機關資訊安全規定及程序，取銷其存取網路之權利。

6、網路系統管理人員除依相關法令或機關規定，不得閱覽使用者之私人檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權規定,使用自動搜尋工具檢查檔案。

7、網路系統管理人員未經使用者同意，不得增加、刪除及修改私人檔案。如有特殊緊急狀況，須刪除私人檔案，應以電子郵件或其他方式事先知會檔案擁有者。

8、對任何網路安全事件，網路系統管理人員應立即向機關內部或其他電腦安全事件緊急處理小組反應。

9、網路系統管理人員只能由系統終端機登入主機，並須保留所有登入、登出紀錄。

10、網路系統管理人員不得新增、刪除、修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾。

（三）網路使用者之管理

1、被授權的網路使用者（以下簡稱網路使用者），只能在授權範圍內存取網路資源。

2、網路使用者應遵守網路安全規定，並確實瞭解其應負的責任；如有違反網路安全情事，應依資訊安全規定，限制或撤消其網路資源存取權利，並依紀律規定及相關法規處理。

3、網路使用者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。

4、應禁止網路使用者以任何方法竊取他人的登入身份與登入網路通行碼。

5、應禁止及防範網路使用者以任何儀器設備或軟體工具竊聽網路上的通訊。

6、應禁止網路使用者在網路上取用未經授權的檔案。

7、網路使用者不得將色情檔案建置在機關網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。

8、應禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便。

9、應禁止網路使用者發送匿名信，或偽造他人名義發送電子郵件。

10、網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。

11、機關外部取得授權的電腦主機或網路設備，與機關內部網路連線作業時，應確實遵守之網路安全規定及連線作業程序。

（四）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，防止遠端撥接或遠端登入資料經由電話線路或網際網路傳送時，被偷窺或截取(如一般網路服務HTTP、Telnet、FTP 等的登入密碼)，及防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

2、為提升大型主機或伺服器主機連線作業之安全性，應視需要使用電子簽章及電子信封等各種安全控管技術，以建立安全及可信賴的通信管道。

（五）防火牆之安全管理

1、機關與外界網路連接的網點，應加裝防火牆，以控管外界與機關內部網路之間的資料傳輸與資源存取。

2、防火牆應具備網路服務的轉送伺服器（即代理伺服器,Proxy Server)以提供 Telnet、FTP、WWW、Gopher 等網路服務的轉送與控管。

3、網路防火牆的安裝與網路架構之規劃及設置，應依機關訂定的資料安全規定及資料安全等級分類，以最經濟有效的方式配置。

4、防火牆應由網路系統管理人員執行控管設定，並依機關制定的資訊安全規定、資料安全等級及資源存取的控管策略，建立包含身份辨識機制、來訊服務(incoming service)、去訊服務(outgoing service)與系統稽核的安全機制，有效地規範資源被讀取、更改、刪除、下載或上傳等行為以及系統存取權限等資訊。

5、網路系統管理人員應由系統終端機登入防火牆主機，禁止採取遠端登入方式，以避免登入資料遭竊取，危害網路安全。

6、防火牆設置完成時，應測試防火牆是否依設定的功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定的安全目標。

7、網路系統管理人員應配合機關資訊安全政策及規定的更新，以及網路設備的變動，隨時檢討及調整防火牆系統的設定，調整系統存取權限，以反應最新的狀況。

8、防火牆系統軟體，應定期更新版本，以因應各種網路攻擊。

（六）軟體輸入控制

1、應禁止網路使用者使用非法軟體。

2、經由網際網路下載軟體，宜由網路系統管理人員事前測試及掃瞄，確認安全無虞後方可安裝及執行。

3、應考量在網路上各檔案伺服器安裝防毒軟體，防止病毒在網路上擴散。

4、網路使用者應定期以電腦病毒掃瞄工具執行病毒掃瞄，並瞭解病毒與惡意執行檔可能入侵的管道，採行防範措施。

5、網路使用者如偵測到電腦病毒入侵或其他惡意軟體，應立即通知網路管理者;網路管理者亦應將已遭病毒感染的資料及程式等資訊隨時提供使用者,以避免電腦病毒擴散。

6、電腦設備如遭病毒感染，應立即與網路離線，直到網管人員確認病毒已消除後，才可重新連線。

（七）網路資訊之管理

1、對外開放的資訊系統，應儘可能安裝在一部專用的主機上，並以防火牆與機關內部網路區隔，提高內部網路的安全性。

2、對外開放的資訊系統，應針對蓄意破壞者可能以發送作業系統指令或傳送大量資料(如電子郵件、註冊或申請

資料)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。

3、機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。

4、網路系統管理人員應負責監督網路資料使用情形，檢查有無違反資訊安全規定之事件發生。

5、對外開放的資訊系統所提供之網路服務(FTP,Gopher,HTTP 等)，應做適當的存取控管，以維護系統正常運作。

6、對外開放的資訊系統，如存放民眾申請或註冊的私人資料檔案，應研究以加密方式處理，並妥善保管，以防止被竊取或移作他途之用，侵犯民眾隱私。

二、電子郵件之安全管理

（一）電子郵件安全管理機制

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。

3、訂定電子郵件的安全管理規定，應評估下列事項：

（1）訊息遭未經授權的截取及竄改的安全弱點。

（2）發生資料錯誤、錯投及誤投的安全弱點。

（3）電子郵件服務的可靠性及可用性。

（4）使用電子郵件改變對內及對外的溝通方式，對行政流程的衝擊（例如，加快發送的速度，以及從機關對機關的通信模式，改為個人對個人的模式等。）

（5）電子郵件法律效力的考量，例如：來源證明、送達、發送及收受等。

（6）評估出版電子郵件目錄的安全性。

（7）使用者從遠端存取電子郵件帳號之安全控管。

4、密等以上的公文及資料，不得以電子郵件傳送；敏感性資訊如有電子傳送之必要，得經加密處理後傳送。

5、為防範假冒機關員工名義發送電子郵件，並達到身分辨識及不可否認的目地,必要時應以電子簽章方式簽發電子郵件。

6、電子郵件附加之檔案，應事前檢視內容有無錯誤後方可傳送。

7、對來路不明的電子郵件,應交由網路系統管理者處理，不宜隨意打開電子郵件,以免啟動惡意執行檔,使網路系統遭到破壞。

三、全球資訊網之安全管理

（一）全球資訊網

1、內部使用的瀏覽器，應作防火牆代理伺服器的設定。

2、內部使用的瀏覽器，應設定為對下載的每一檔案做電腦病毒或惡意內容的掃描。

3、應考量網際網路新技術(如 Java，ActiveX 等)的可能安全弱點，並採取適當的防護措施以確保內部網路安全。

4、HTTP 伺服器應透過組態的設定，使其啟動時不具備系統管理者身份。

5、應對 HTTP 伺服器可存取的範圍，限制在僅能存取檔案系統的某一特定區域。

6、對於通用閘通道介面手稿(Common Gateway Interface Script)的執行與使用，應予嚴密監控，以防止不法者利用來執行系統指令，獲取系統內重要的資訊或破壞系統。

（二）企業網路（Intranet）

1、內部的電子化作業，應視需要使用電子簽章安全機制，以明責任，俾利線上公文簽核或查詢文件。

2、機關間資料如透過專線傳送(如封閉網路系統)，應依資料安全等級，依相關安全規定做適當的加密處理。

3、機關間的敏感性資料如透過網際網路傳送，宜經由虛擬專用網路(VPN)處理，以確保資料的隱密性。

（三）網路設備備援與系統備援

1、為維持機關網路的持續正常運作，各重要網路設備應有備援。

2、網路硬體設備應加裝不斷電系統，以防止不正常的斷電狀況。

3、為確保內部網路與外界的服務持續暢通，內部網路與外界網路的連接，應有一個以上的替代路徑。

4、網路系統中各主要主機伺服器(包括防火牆主機)應有備援主機，以備主要作業主機無法正常運作時之用。

5、網路系統中之防火牆與各主機應定期做系統備份，包括完整系統備份，系統架構設定備份以及稽核資料備份。

（四）網路入侵之處理

1、網路如發現有被入侵或有疑似被侵入情形，應依事前訂定的處理程序，採取必要的行動。

2、網路入侵的處理步驟如下:

（1）立即拒絕入侵者任何存取動作，防止災害繼續擴大;當防護網被突破時，系統應設定拒絕任何

存取;或入侵者已被嚴密監控，在不危害內部網路安全的前題下，得適度允許入侵者存取動作，以利追查入侵者。

（2）切斷入侵者的連接，如無法切斷則必須關閉防火牆;或為達到追查入侵者的目的，可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的連接。

（3）應全面檢討網路安全措施及修正防火牆的設定，以防禦類似的入侵與攻擊。

（4）應正式記錄入侵的情形及評估影響的層面。

（5）立即向權責主管人員報告入侵情形。

（6）向機關內部或外部的電腦安全緊急處理小組反應，以獲取必要的外部協助。

三、網路安全稽核

（一）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、對於通過防火牆之來源端主機 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。

（二）警示系統

1、應依資訊安全規定，視需要建立警示系統（例如:當有不明的使用者連續嘗試侵入時，系統自動發出警示訊號等），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。

2、警示系統的功能應包括下列事項：

（1）記錄警示事件於警示檔。

（2）發送電子郵件給網路系統管理者。

（3）在系統終端機上顯示訊息。

（4）發送一 SNMP 警示訊號到網路管理系統。

（5）啟動管理控制台的警示器。

（6）執行一特定應用程式。

（三）網路入侵之追查

1、對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並連合相關單位(如網路服務公司)，追蹤入侵者。

2、入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知檢警憲調單位，請其處理入侵者之犯罪事實調查。

四、憑證機構之安全管理

（一）憑證機構之安全評估

1、基於業務需要，須自行或委託專業機構建置憑證機構（certificate authority），或選用具公信力的憑證機構時，應綜合考量憑證機構之技術、管理、人員及財務的安全風險等。考量事項如下：

（1）獨立性。

（2）承擔風險之財務資源及財物管理能力。

（3）系統安全管理能力。

（4）永續經營能力。

（5）硬體、軟體及通信設施之可信賴性。

（6）系統稽核管理能力。

（7）緊急應變計畫。

（8）人員管理及內部控制。

（9）其他。

（二）憑證機構之技術安全

1、憑證機構金鑰之產生、儲存、使用、備份、銷毀、更新及復原作業等，應建立嚴格的安全管理機制。

2、憑證機構資訊系統(含應用系統、密碼模組等)之安全驗證，應遵照權責主管機關訂定之規範作業，以確保其安全性。

3、憑證機構使用之數位簽章或加密金鑰長度，應依權責主管機關建議之參考值，視系統的安全需求設定。

4、對外採購加密技術時，應請廠商提供輸出國核發之輸出許可文件，並應避免採購具有金鑰代管或金鑰回復之產品。

陸、系統存取控制

一、資訊系統存取控制規定

1、應訂定資訊系統存取控制規定，界定存取控制之需求，並以書面、電子或其他方式記錄之。

2、應將業務系統之存取控制需求，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政策，並明定使用單位及使用人員的系統存取權利。

4、資訊系統存取控制規定之研擬，應考量事項如下：

（1）個別業務應用系統之安全需求。

（2）資訊傳佈及資料應用之名義及授權規定。

（3）相關法規或契約對資料保護及資料存取之規定。

二、使用者之存取管理

（一）使用者註冊管理

1、對於多人使用的資訊系統，應建立正式的使用者註冊管理程序。

2、使用者註冊管理程序，應考量的事項如下：

（1）查核使用者是否已經取得使用該資訊系統之正式授權。

（2）查核使用者被授權的程度是否與業務目的相稱，是否符合資訊安全政策及規定（例如:有無違反權責分散原則。）

（3）應以書面、電子或其他方式，告知使用者之系統存取權利。

（4）要求使用者簽訂約定，使其確實瞭解系統存取的各項條件及要求。

（5）在系統使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。

（6）應建立及維持系統使用者之註冊資料紀錄，以備日後查考。

（7）使用者調整職務及離（休）職時，應儘速註銷其系統存取權利。

（8）應定期檢查及取銷閒置不用的識別碼及帳號。

（9）閒置不用的識別碼不應重新配賦給其他的使用者。

（二）系統存取特別權限之管理

1、應嚴格管制系統存取特別權限。

2、應特別保護的系統，如有必要賦予使用者系統存取特別權限，應依下列的授權程序管理：

（1）應確認系統存取特別權限之事項，例如作業系統、資料庫管理系統、以及須賦予系統存取特別權限的人員名單。

（2）應依執行業務之需求，視個案逐項考量賦予使用者系統存取特別權限；系統存取特別權限之配賦，應以執行業務及職務所必要者為限。

（3）應建立申請系統存取特別權限之授權程序，並只能在完成正式授權程序後，才能配賦給使用

者；另外，應將系統存取特別權限之授權資料建檔，以明責任及備日後查考。

（三）使用者通行碼之管理

1、應建立使用者通行碼之管理制度。

2、建立通行碼管理制度，應考量下列事項：

（1）應儘量以簽訂書面約定之方式，要求使用者善盡保護個人通行碼之責任；如屬於群組軟體之使用者，應確保工作群組的通行碼，僅限群組成員使用。

（2）為維持通行碼的機密性，應以配賦臨時性通行碼，並強迫使用者立即更改通行碼的方式處理；使用者忘記通行碼時，可提供臨時性的通行碼，以利系統辨認使用者。

（3）應以安全的方法將臨時的通行碼交付使用者，避免經由第三者，或是以未受保護的電子郵遞等電子方式交付給使用者，並應建立確認使用者是否收到臨時的通行碼的機制。

（4）系統如經評估須建立更高等級的安全機制，可利用電子簽章等安全等級更高的存取控制技術。

（四）系統存取權限之檢討評估

1、為有效控管資料及系統存取，應定期檢討及評估使用者之存取權限。

2、系統存取權限之評估，應考量事項如下：

（1）系統存取權限評估，以每六個月評估一次為原則。

（2）系統存取特別權限之評估，以每三個月評估一次為原則。

（3）定期檢討系統存取特別權限之核發情形，防止有人未經正式的授權程序取得特別權限。

三、系統存取之責任

（一）使用者通行碼之管理

1、使用者選擇及使用通行碼時，應遵守機關資訊安全規定。

2、應依下列原則配賦、管理及使用通行碼：

（1）以嚴謹的程序核發通行碼，明確規定使用者應負的責任。

（2）個人應負責保護通行碼，維持通行碼的機密性。

（3）應避免將通行碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。

（4）當有跡象足以顯示系統及使用者密碼可能遭破解時，應立即更改密碼。

（5）使用者密碼的長度最少應由六位長度組成。

（6）應儘量避免以下列事項作為通行密碼：

・年、月、日等時間資訊。

・個人姓名、出生日、身分證字號或汽機車牌照號碼。

・機關、單位名稱、識別代碼或是其他相關事項。

・電話號碼。

・使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

・重複出現兩個字以上的識別字碼。

・以全部數字或是全部字母組成密碼。

・英文或是其他外文字典的字。

・電腦上使用者的名字。

・電腦主機名稱、作業系統名稱。

・地方名稱。

・專有名詞。

・任何人的名字。

（7）使用者第一次登入系統時，系統應要求更改臨時性通行碼。

（8）自動化登入系統之通行碼，不宜存放在巨集或是功能鍵中。

（9）應定期更換通行碼，原則上以每三個月更新一次為原則，最長不得超過六個月；應儘量避免重複或循環使用舊的通行碼。

（10）對有存取系統公用程式等特別權限的帳號，使用者密碼的更改頻率應較一般通行碼的更改周期為高。

3、須存取多人使用之系統，或須進入不同的系統平台，應考量使用安全等級較高較高的通行碼。（例如:使用單向加密演算法將通行碼加密）

（二）暫時不使用或無人看管設備之安全管理

1、暫時不使用，或無人看管的設備，應研擬適當的安全保護措施；安置在辦公區域內的設備（例如:工作站或檔

案伺服器），如一段時間內無人使用或看管，應採行特別的安全保護措施，以防止未經授權的系統存取。

2、應將暫時不使用及無人看管的設備管理規定，明確告知所有的使用者或服務廠商，並賦予安全保護的責任。

3、暫時不使用或無人看管設備之安全管理，應考量事項如下：

（1）當作業結束時，應關閉有效的通信管道。

（2）當通信結束時，應完全登出電腦系統，不宜只關閉電腦系統或是端末機。

（3）當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及端末機的安全。

四、網路存取之安全控制

（一）網路服務之限制

1、個別使用者或是從特定端末機存取電腦及網路服務之安全規定，應依業務存取控制規定辦理。

2、使用者應在授權範圍內存取網路系統服務事項。

（二）強制性的通道

1、從使用者端末機連接電腦系統之線路，應適當加以控制（例如:建立強制性的通道），以減少未經授權存取系統或電腦設施之風險。

2、應建立強制性的通道，防止未被授權的使用者從不同的管道進入電腦系統。

3、建立強制性的通道應考量的安全措施如下：

（1）指定專線及電話號碼。

（2）自動將通訊埠連上特定的應用系統及安全通道。

（3）限制使用者只能選擇特定的路線。

（4）防止無限制的網路漫遊。

（三）使用者身分鑑別

1、開放機關以外的使用者從公眾網路，或從機關網路以外的網路與本機關連線作業,應建立遠端使用者身分鑑別機制，以降低未經授權存取系統的風險。

2、可考量使用「詰問及回應」（challenge/response）或資料加密等安全技術，鑑別網路使用者之身分。

（四）網路節點之身分鑑別

1、應建立遠端電腦系統（尤其是開放使用者從公眾網路進入系統）與本機關連線作業之身分鑑別安全機制。

2、建立遠端電腦系統連線作業之身分鑑別機制，應評估業務的可能風險及對業務的衝擊及影響,設定適當的安全水準。

3、可使用「詰問及回應」或線上加密(非對稱型)等技術，執行網路節點身分鑑別,同時也可使用專屬私用網路使用者位址之檢查設施，鑑別連線作業的來源。

（五）遠端診斷連線作業埠之控制：機關對供維修廠商以遠端登入方式進入 電腦網路系統進行維修的通信作業埠，應採取特別的安全控管機制。

（六）網路之分隔

1、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的領域，以降低可能的安全風險。

2、不同領域的網路系統，每一領域應以特定的安全設施加以保護；例如，可設置防火牆及網路閘門，隔開不同的網路系統，以安全的閘道控制不同領域的網路系統。

3、應依據訂定的系統存取控制政策及需求決定，將規模龐大的網路分成數個不同領域的網路系統,並考量成本因素及使用網路路由器及閘門技術對作業效率之影響。

（七）網路連線作業之控制

1、為確保系統安全，跨機關的網路系統可限制使用者之連線作業能力。例如，以網路閘門技術依事前訂定之系統存取規定，過濾網路之傳輸作業。

2、限制網路連線作業能力之安全控制措施如下：

（1）只允許使用電子郵遞系統。

（2）只允許單向的檔案傳輸。

（3）允許雙向的檔案傳輸。

（4）使用互動式的系統存取。

（5）限制只能在特定的時間或日期進行系統存取。

（八）網路路由控制

1、分享式的網路系統（尤其是跨機關的網路系統），應建立網路路由的控制，以確保電腦連線作業及資訊流動，不會影響應用系統的存取政策。

2、網路路由的控制，應建立實際來源及終點位址之檢查機制；網路路由的控制可以硬體或軟體方式執行，並應事先評估瞭解不同方式的安全控制能力。

（九）網路服務之安全控制

1、使用公用或私有網路，應評估使用該項網路服務之可能風險。

2、使用公用或私有網路，應評估網路服務提供者之安全措施是否足夠、是否提供明確的安全措施說明，並應考量使用該項網路對維持資料傳輸機密性、完整性及可用性等各種安全影響。

五、電腦系統之存取控制

（一）應建立自動化的端末機身分鑑別系統，以鑑別從特定位址連上網路的使用者身分。

（二）端末機登入程序

1、使用者存取電腦系統，應經由安全的系統登入程序。

2、登入程序應具備下列的功能：

（1）不應顯示系統及應用系統識別碼，直到成功登入系統。

（2）在系統登入程序中，應顯示“只有被授權的使用者才可存取系統”等警告性的資訊。

（3）系統不應在登入程序中，提供未經授權的使用者有關登入系統的說明或協助性的訊息。

（4）只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性；如果登入發生錯誤，系統不應顯示那一部分資料是正確的，那一部分資料是錯誤的。

（5）應限制系統登入不成功時可以再嘗試的次數，原則上以三次為原則，系統並應：

・記錄系統登入不成功的事件。

・在使用者嘗試登入系統失敗後，應強迫必須間隔一段時間之後才能再次登入。

・應中斷資料連結作業。

（6）在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

（7）應限制系統登入程序的最長及最短時間，如果超出時間限制，系統應自動中斷登入。

（8）在成功登入系統後，應顯示下列的資訊：

・上一次成功登入系統的日期及時間。

・上一次成功登入系統之後，有無被系統拒絕登入的詳細資料。

（三）使用者身分辨識

1、應對使用者核發使用者識別碼，以明責任歸屬；使用者識別碼不應顯示任何足以辨識使用者特別權限的訊息，例如：顯示其為管理者或監督者。

2、只有在例外的情況下，可為整體效益，經權責主管人員之同意，核發群組內人員共享同一使用者識別碼。但應採取額外的安全控制措施，明確規範使用者的責任。

（四）使用者通行碼之管理

1、應以安全有效的使用者通行碼管理系統，鑑別使用者身分。

2、安全有效的使用者通行碼管理系統，應考量的事項如下：

（1）要求必須使用通行碼，以明定系統的使用責任。

（2）應允許使用者自行選擇及更改通行碼；系統應具備資料輸入錯誤之更正功能。

（3）要求使用者必須使用最低長度的密碼（建議使用最少六位長度的通行碼）

（4）要求使用者定期更改通行碼（建議以三個月一次為原則，最長不宜超過六個月）。

（5）以更頻繁的次數定期更新系統存取特別權限的通行碼（例如系統公用程式之存取通行碼）。

（6）使用者自行選擇密碼時，應在第一次登入系統時強迫使用者更改臨時性的密碼。

（7）應建立使用者密碼的歷史紀錄，最好保存至少一年的使用紀錄，並避免使用者重複使用相同的密碼。

（8）在登入系統程序中，系統不應顯示使用者的密碼資料。

（9）使用者密碼應與應用系統資料分開存放。

（10）應使用單向加密演算法儲存使用者密碼。

（11）在軟體完成安裝作業後，應立即更改廠商預設的使用者密碼。

（12）應利用工具檢查，或由使用者自行考量通行碼是否安全可靠，參考基準如下：

・是否使用與日期有關的年、月、日。

・是否使用公司名稱、識別碼或是其他參考性資訊作為通行碼。

・是否以使用者識別碼，團體識別碼或其他系統識別碼作為使用者通行碼。

・是否使用重複出現兩個字以上的識別字碼作為通行碼。

・是否使用全數字或是全字母作為通行碼。

（五）端末機作業時間限制

1、安置在高風險地區，且不經常使用的端末機（例如，設置在公共場所或機關辦公場所以外的地區），或是對高風險的系統提供服務，應限定其作業時間，以防止未經授權的人員存取系統。

2、應設定系統的作業時間限制，包括間隔一定時間後自動清除螢幕上的資訊，以及依據事前訂定的時間限制，結束應用系統及網路通信。

（六）連線作業時間之控制

1、有高風險的應用系統，應限制使用者的連線作業時間。

2、對處理機密及敏感性系統的端末機，應限定連線作業及網址連線時間，以減少未經授權存取系統的機會。

3、限定連線作業時間的措施如下：

（1）只允許在設定的時間內與系統連線。

（2）如無特別延長作業時間的需求，應限制只能在正常的上班時間內進行連線作業。

（3）應限制連線的網址。

六、應用系統之存取控制

（一）資訊存取之限制

1、應依資訊存取規定，配賦應用系統的使用者（包括應用系統支援人員)與業務需求相稱的資料存取及應用系統使用權限。

2、資訊存取的控制措施如下：

（1）以選單方式控制使用者僅能使用系統的部分功能。

（2）適當地編輯作業手冊，限制使用者僅能獲知或取得授權範圍內的資料及系統存取知識。

（3）控制使用者存取系統的能力（例如限定使用者僅能執行唯讀、寫入、刪除或執行等功能。）

（4）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，且只能輸出到指定的端末機及位址。

（二）系統公用程式之安全管理

1、應嚴格限制及控制電腦公用程式之使用。

2、電腦公用程式之安控措施如下：

（1）設定使用者密碼以保護系統公用程式。

（2）將系統公用程式與應用系統分離。

（3）將有權使用系統公用程式的人數限制到最小的數目。

（4）應建立臨時使用公用程式的授權制度。

（5）應限制系統公用程式之可用性，例如變更公用程式的使用時間授權規定。

（6）應記錄系統公用程式的使用情形，以備日後查考。

（7）應訂定系統公用程式的授權規定，並以書面或其他電子方式為之。

（8）應移除非必要的公用程式及系統軟體。

（三）原始程式資源之存取控制

1、對應用系統原始程式資料之存取，應建立嚴格的安全控制機制。

2、原始程式資源之存取控制，應考量下列事項：

（1）應用程式原始碼資料庫，應儘可能不要存放在作業系統的檔案中。

（2）每一項應用程式原始碼，應指定一位管理人員。

（3）不應核發無限制存取應用程式原始碼之權限。

（4）發展中或是維護中的應用程式，應與實務作業之程式原始碼資料庫區隔，不應放置在一起。

（5）應用程式原始碼資料庫之更新，以及核發應用程式原始碼供程式設計人員使用，應由原始碼資料庫管理人員執行。

（6）程式目錄清單應放置在安全的環境中。

（7）應建立所有存取程式原始碼資料庫的稽核軌跡。

（8）舊版的原始程式應妥慎典藏保管，詳細記錄使用的明確時間，並應保存所有的支援應用程式軟體、作業控制、資料定義及操作程序等資訊。

（9）應用程式原始碼資料庫之維護及複製，應依嚴格的變更控制程序進行。

（四）機密及敏感性系統之獨立作業

1、對機密及敏感性的系統，應考量建置獨立的或是專屬的電腦作業環境。

2、建置獨立的或是專屬的電腦作業環境，應考量的事項如下：

（1）應由系統擁有者決定應用系統是否屬於機密或敏感性，並以書面記錄之。

（2）機密及敏感性的應用系統須在分享式的電腦環境中執行時，應界定其他須共享資源的系統項目，並經系統擁有者的同意。

七、系統存取及應用之監督

（一）事件記錄

1、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。

2、系統稽核軌跡應包括下列事項：

（1）使用者識別碼。

（2）登入及登出系統之日期及時間。

（3）儘可能記錄端末機的識別資料或其位址。

（二）系統使用之監督

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；個別系統接受監督的程度，應依風險評估結果決定。

2、系統使用監督應考量事項如下：

（1）系統存取失敗情形。

（2）檢查系統登入的模式，確定使用者識別碼是否有不正常使用或是被重新使用的情形。

（3）查核系統存取特別權限的帳號使用情形及配置情形。

（4）追蹤特定的系統交易處理事項。

（5）敏感性資源的使用情形。

3、系統使用之監督作業，應經權責主管人員之正式授權始得為之。

（三）電腦作業時間校正：應定期校正電腦系統作業時間，以維持系統稽核紀錄的正確性及可信度，俾作為事後法律上或是紀律處理上的重要依據。

八、機關外部人員存取資訊之安全管理

（一）外部連線作業之風險評估

1、如開放外界與其連線作業，應評估可能的安全風險；如因業務需要，須與外界連線作業時，應予事前進行風險分析，決定必須採行或應特別強化的資訊安全需求項目。

2、外部存取本機關資訊系統之風險分析，應充分考量下列事項：

（1）第三者需要存取的資訊類型及資訊的價值等。

（2）第三者採行的資訊安全措施及安全保護水準。

（3）第三者之存取對本機關資訊架構可能產生的安全風險及影響。

3、除非已經與第三者協議確定，並已執行適當的安全措施，且簽訂書面約定，妥善規範連線單位應遵守的規定，否則不宜提供第三者存取本機關的資訊設備。

（二）第三者存取之安全契約

1、第三者存取本機關之資訊設施，應於實際存取作業前，簽訂正式的契約或協定，俟契約或約定生效後始能提供存取服務。

2、契約或協定內容應規定第三者須遵守之資訊安全規定、標準及必要的連線條件。

3、與第三者簽訂安全契約之參考條款如下：

（1）第三者應遵守的一般性資訊安全規定。

（2）第三者可以使用的系統存取方法，以及使用者識別碼及通行碼的管理規定。

（3）每一項資訊系統的使用作業說明。

（4）應要求第三者建立及維持一份有權存取系統的人員名單。

（5）資訊系統可以開放連線使用的期程及時間。

（6）簽約單位應負的安全保密責任。

（7）保護資訊資產的作業程序。

（8）第三者應負的法律責任，例如電腦處理個人資料保護法相關規定。

（9)監督及撤銷使用者系統存取權限之權利及相關規定。

（10）硬體、軟體建置及系統維護的責任。

（11）稽核第三者是否履行契約責任的權利。

（12）智慧財產權及資訊公開的限制。

（13)契約終止時，可確保機關資訊及資產安全回收或是銷毀的措施。

（14）必要的實體保護措施。

（15）確保第三者遵守資訊安全規定的機制。

（16)對使用者進行作業方法、程序及安全教育訓練之相關規定。

（17）防止電腦病毒散佈之措施。

（18）使用者存取系統之授權規定及程序。

（19）調查及報告資訊安全事件之作業程序。

（20）其他下包廠商及相關參與者的責任關係。

九、系統稽核規劃

（一）系統稽核控制

1、對作業系統進行查核之稽核需求及實際稽核作業，應審慎規劃，並經權責主管人員同意始得為之，以免影響業務正常運作。

2、系統稽核應考量事項如下：

（1）系統稽核需求及查核範圍，應經權責主管人員同意。

（2）應限定以唯讀方式存取軟體及資料。

（3）不能以唯讀方式進行系統存取時，應獨立複製另外一份系統檔案供稽核作業之用，且應於稽核作業完成後，立即消除檔案。

（4）執行查核所需的技術資源，應於事前明確界定，並準備妥當。

（5）執行特別的及額外的查核，應於事前明確界定需求及範圍，並與服務提供者協議。

（6）執行稽核作業的所有系統存取作業，應予監督及留下記錄，以備日後查考。

（7）稽核作業程序、需求及責任規定，應以書面或其他電子方式為之。

（二）系統稽核工具之保護

1、應保護系統稽核工具（例如軟體及資料檔案）以防止誤用或被破解。

2、系統稽核工具應與發展中或是實作的系統分隔，且應存放在安全的地點。

柒、系統發展及維護之安全管理

一、系統安全需求規劃

（一）系統安全需求分析及規格訂定

1、應在資訊系統規劃之需求分析階段，即將安全需求納入；新發展的資訊系統，或是現有系統功能之強化，皆應明定資訊安全需求，並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、資訊系統安全需求分析應考量事項如下：

（1）評估保護資訊機密性、整合性及可用性的需求。

（2）找出及決定各種不同的安全控制措施，以防範、偵測電腦當機或發生安全事件時，能立即執行回復作業。

（3）資訊安全需求分析，應特別考量下列事項：

・對資訊及系統之存取控制。

・重要業務，應建立例行性的稽核制度，並為特定查核之事項建立稽核軌跡。

・重要的資料，應在資料處理過程的每一階段，或是特別選定的某一階段，檢查及保護資料的真確性。

・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。

・應遵守法規或契約上對資訊安全控制的要求。

・重要的業務資料，應複製備份資料。

・應訂定電腦當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。

・應保護系統避免未經授權的竄改或是修改。

・應使系統以安全的方式為一般人員操作及使用。

・應儘可能促使系統滿足稽核人員的安全控制需求。

（4）應於相關文件規定資訊安全控制措施，以利使用者及電腦支援人員明瞭電腦系統內建之安控系統功能。

二、應用系統之安全

（一）資料輸入之驗證

1、輸進應用系統的資料，應在事前查驗，以確保資料的真確性。

2、資料輸入應考量的安控措施如下：

（1）應檢查是否有以下的錯誤：

・是否有超出設定範圍的數值。

・資料檔案是否有錯誤的文、數字。

・資料是否有毀損或是不正確。

・是否有超出設定數值的上限或是下限。

・是否有未經授權的資料或是不一致的控制性資料。

（2）應定期檢查主要欄位或資料檔案的內容，以確保資料的有效性及真確性。

（3）應檢查輸入的書面資料是否有被竄改情形。

（4）應建立資料檢驗證程序及資料錯誤更正的作業程序。

（5）應明定資料輸入過程中相關人員的責任。

（二）系統內部作業處理之驗證

1、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。

2、系統內部作業是否採取特別的資料處理控制程序，應視應用系統的性質及資料遭破壞，對機關業務的影響程度而定。

3、系統內部作業處理之驗證方法如下：

（1）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。

（2）比對本次開始作業與前次結束作業的檔案資料是否一致。

（3）查證系統產生的資料是否正確。

（4）在中央及遠端電腦系統之間，應檢查資料、下載及上傳軟體，或軟體更新後系統之真確性。

（5）將紀錄及資料檔案以數學函式求算雜湊值，防止被更改。

（三）資料加密

1、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。

2、是否使用加密方法，應進行風險評估，以決定採取何種等級的安全保護措施。

3、使用加密技術時，如機關資訊專業人力及經驗不足，可請外界的學者專家提供技術諮詢服務。

4、應遵守權責主管機關訂定的資料保密規範，及使用權責主管機關檢驗合格或認可的加密模組,以確保加密技術產品的安全功能。

（四）訊息真確性之鑑別

1、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。

2、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。

3、是否使用訊息鑑別技術，應依安全風險評估結果，採行最適當的鑑別方法。

三、應用系統檔案之安全

（一）作業軟體之控制

1、在作業系統上執行應用軟體，應嚴格執行下列控制程序，減少可能危害作業系統的風險：

（1）作業用的應用程式館更新作業，應限定只能由授權的管理人員才可執行。

（2）儘可能將執行碼存放在作業系統內。

（3）執行碼尚未測試成功，且未被使用者接受前，不應在作業系統執行。

（4）應建立應用程式館的更新稽核紀錄。

（5）應保留舊版的軟體，以作為緊急應變措施之用。

（二）系統測試資料之保護

1、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；如須應用真實的資料，應於事前將足以辨識個人的資料去除。

2、在使用真實的資料進行測試時，應採行下列的保護措施：

（1）適用在實際作業系統的存取控制措施，亦應適用在測試用的系統。

（2）真實資料被複製到測試系統時，應依複製作業的性質及內容，在取得授權後始能進行。

（3）測試完畢後，真實資料應立即從測試系統中刪除。

（4）真實資料的複製情形應予以記錄，以備日後稽核之用。

四、系統變更及維護環境之安全

（一）變更作業之控制程序

1、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、建立變更控制程序，應考量的事項如下：

（1）應依事前訂定的授權規定，執行變更作業：

・規定系統使用者提出變更需求之權責，以及接受系統變更建議之授權程序。

・規定系統完成變更作業後，系統使用者是否認可之權責。

・規定只有被授權的使用者可提出系統變更之請求。

・規定檢視系統安全控制及檢視系統真確性的程序，以確保系統變更作業不致影響或破壞系統原有的安全控制措施。

・應找出系統變更作業需要修正的電腦軟體、資料檔案、資料庫及硬體項目。

・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。

・在執行變更作業前，應確保系統變更作業能為使用者接受。

・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。

・應建立軟體更新的版本控制機制。

・所有的系統變更作業請求，皆應建立稽核紀錄。

（二）作業系統變更之技術評估

1、作業系統應定期更新（例如安裝新的版本）；作業系統變更時，應評估其對應用系統是否造成負面的影響，或是產生安全問題。

2、作業系統變更之評估程序，應考量的事項如下：

（1）評估應用系統的安全控制措施及查驗系統之真確性，以確保其未受作業系統變更之影響。

（2）作業系統變更的評估及測試結果，如須進行必要的調整，應納入年度計畫及預算。

（3）作業系統的變更應即時通知相關人員，以便在作業系統變更前，相關人員可以進行適當及充分的評估作業。

（三）套裝軟體變更之限制

1、廠商提供的套裝軟體，應儘可能不要自行變更或修改，如因特殊需要須修改，應考量以下的事項：

（1）是否會破壞系統內建的安全控制，以及危害鑑別系統真確性作業的風險。

（2）應取得套裝軟體開發廠商的同意。

（3）應考量以標準化的系統更新方式，請廠商進行必要的變更。

（4）應考量如自行變更套裝軟體，日後進行軟體維護的可能性。

（5）套裝軟體如須變更，應保留原始的軟體，並將變更的資料予以記錄，以備日後軟體再更新之用。

捌、資訊資產之安全管理

一、機關資訊資產目錄之建立及保護

（一）應該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。

（二）資訊資產參考項目如下：

1、資訊資產：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支援程序、業務永續運作計畫、預備作業計畫等。

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、磁性媒體資料及其他技術設備。

4、技術服務資產：電腦及通信服務、其他技術性服務（電源及空調）。

二、資訊安全之等級分類

（一）資訊安全分類原則

1、應依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，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，應考量資訊分享及限制的影響、未經授權的系統存取或是系統損害對機關業務的衝擊，尤其要考量資料的機密性、資料真確性及可用性。

3、機關資訊安全分類，可依據相關法規，區分機密性、敏感性及一般性等三類。

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

5、當須執行或參考其他機關訂定之資訊安全等級分類時，應特別注意其與本機關的資訊安全等級分類，在定義及標準上是否相同。

（二）資訊安全等級標示

1、已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

2、應納入安全等級分類的項目，包括書面報告、螢幕顯示、磁性媒體、電子訊息及檔案資料等。

玖、實體及環境安全管理

一、設備安全管理

（一）設備安置地點之保護

1、設備應安置在適當的地點並予保護，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、設備安置應遵循的原則如下：

（1）設備應儘量安置在可減少人員不必要經常進出的工作地點。處理機密性及敏感性資料的工作站，應放置在員工可以注意及照顧的地點。

（2）需要特別保護的設備，應考量與一般的設備區隔，安置在獨立的區域。

（3）應檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等可能的風險。

（4）電腦作業區應禁上抽煙及飲用食物。

（5）在特定的作業環境下，可考慮使用鍵盤保護膜。

（6）除考量同一樓層地板可能導致的的危險外，應考量鄰近建築樓層地板可能導致的危險。

（二）電源供應

1、電腦設備之設置，應予保護，以防止斷電或其他電力不正常導致的傷害;電源供應依據製造廠商提供的規格設置。

2、應考量安置預備電源，並使用不斷電系統。

3、機關擬訂資訊安全事件緊急處理應變計畫，應將不斷電系統失效之後的應變措施納入;不斷電系統應依據製造廠商的建議，定期進行測試。

4、應謹慎使用電源延長線，以免電力無法負荷導致火災等危害安全情事。

（三）電纜線安全

1、電力及通信用的電纜線，應予適當的保護，以防止被破壞或是資料被截取。

2、電力及通信纜線的保護原則如下：

（1）連接資訊設施的電源及通信線路，應儘可能地下化；如果不能地下化，應採取足夠的替代保護措施。

（2）應該考量保護網路通信線路的措施，以防止遭截取或是受到破壞。

（3）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。

（四）設備維護

1、應妥善地維護設備，以確保設備的完整性及可以持續使用。

2、設備維護的原則如下：

（1）應依據廠商建議的維修服務期限及說明，進行設備維護。

（2）設備的維護只能由授權的維護人員執行。

（3）應將所有的錯誤或是懷疑的錯誤，予以明確記載。

（五）設備放置在外部空間之安全管理

1、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。

2、設置在機關外部的資訊設備安全措施原則如下：

（1）如果未採取電腦病毒防範措施，執行業務所使用的個人電腦，不應在家裡使用。

（2）外出差勤時，電腦設備及資料儲存媒體在公共場所應有人看管。

（3）外勤使用之攜帶型電腦，易於被偷取、遺失或是遭未經授權的取用，應提供適當的存取保護措施，例如設定通行碼或是將檔案資料加密。

（4）應隨時注意設備製造廠商提供的保護使用說明書。

（5）各種安全風險如損害、偷竊或竊聽等，可能會因不同的安置地點而有所不同；在決定最適當的安全措施時，應該將不同地點的安全風險納入考量。

（六）設備處理之安全措施

含有儲存媒體的設備項目（例如硬碟），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。

（七）資訊設施誤用之防止

1、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。

2、如從監督性的資訊，或是從其他方法發現資訊設施有不當使用情形，應作適當的紀律處理。

3、應以書面或其他電子方式明確告知使用者的系統存取授權範圍。

4、員工以及其他第三者，除非獲得正式的授權，任何人皆不得進行系統存取。

二、周邊安全管理

（一）周圍環境之安全

1、實體環境的安全保護，應以事前劃定的各項周邊設施為基礎，並以設置必要的障礙（例如:使用身分識別卡之安全門），達成安全控管的目的。

2、每項資訊設施的實體保護程度，以及實體障礙設置的位置，應依資訊資產及服務系統的價值及安全的風險決定。

3、實體環境的安全保護原則如下：

（1）周圍設施的安全措施，應視擬保護的資訊資產或資訊服務系統的價值而定。

（2）應明確界定有那些周邊設施，須列為安全管制的對象。

（3）支援資訊作業的相關設施如影印機、傳真機等，應安置在適當的地點，以降低未經授權的人員進入管制區的風險，及減少敏感性資訊遭破解及洩漏的機會。

（4）對非相關的人員不應提供過多有關管制區的作業細節。

（5）為了安全的目的，以及防止可能的不當行動，未經授權的人員在辦公室單獨作業應予適當的管理。

（6）資訊作業如有委外者，自行管理的設備應安置在特定的區域，並與資訊服務提供者管理的設備分開。

（7）資訊支援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。

（8）非經授權，管制區內不得設置照像、錄音及錄影等設備。

（二）人員進出管制

1、管制區內應有適當的進出管制保護措施，以確保只有被授權的人員始得進入。

2、進出管制考量應考量的事項如下：

（1）來訪人員進入管制區應予適當的管制，並記錄進出時間；來訪人員只有在特定的目的或是被授權情形下，才能進入管制區。

（2）在管制區內，所有的人員應配載身分識別標示，並隨時注意身分不明或可疑的人員。

（3）員工離職後，應立即撤銷進入管制區的權利。

（三）資料中心及機房之安全管理

1、支援重要業務運作的資料中心及電腦機房，應設立良好的實體安全措施；資訊中心及電腦機房地點的選定，應考量火災、水災、地震等自然及人為災害的可能性，並考量鄰近空間的可能安全威脅。

2、資料中心及機房安全應考量的事項如下：

（1）主要的設施應遠離大眾或是公共運輸系統可直接進出的地點。

（2）資料中心及電腦機房的建築，應儘可能不要有過於明顯的標示；在建築物內部及外部的說明，應以提供最低必要的指引或配置說明為限。

（3）各樓層的配置說明及內部的電話聯絡簿，應以不讓有心人士循線找出電腦設施的所在地為原則。

（4）危險性及易燃性的物品，應存放在遠離資料中心或電腦機房的安全地點。非有必要，電腦相關文具設備不應存放在電腦機房內。

（5）備援作業用的設備及備援媒體，應存放在安全距離以外的地點，以免資料中心或電腦機房受到損害時也一併受到毀損。

（6）應安裝適當的安全偵測及防制設備，例如熱度及煙霧偵測設備，火災警報設備、滅火設備及火災逃生設備；各項安全設備應依廠商的使用說明書

定期檢查；的員工應施予適當的安全設備使用訓練。

（7）資訊安全緊急處理作業程序應以書面方式記載，並定期演練及測試。

（8）不上班或沒有人看護時，門窗應予閉鎖，並應考量窗戶的外部保護措施。

（四）物品及設備配送及裝載之管理

1、電腦機房應設置適當的保護措施，防止未被授權的人員進出；為降低未被授權的人員進入電腦機房的風險，可視需要設立一個獨立的物品及設備配送及裝載作業區域。

2、物品及設備作業區的安全需求應依風險評估的結果而決定。

（五）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之外遭未被授權的人員取用、遺失或是被破壞的機會。

2、應考量事項如下：

（1）文件及磁碟片在不使用或是不上班時，應存放在櫃子內。

（2）機密性及敏感性資訊，不使用或下班時應該上鎖，最好是放在防火櫃之內。

（3）個人電腦及電腦終端機不再使用時，應以上鎖、通行碼或是其他控制措施保護。

（4）應該考量保護一般郵件進出的地點，以及無人看管的傳真機。

（六）財產移轉之安全管理

電腦設備、資料或軟體，在沒有管理人員書面授權的情形下，不應被帶離辦公室。

拾、業務永續運作計畫之規劃及管理

一、業務永續運作之規劃

（一）業務永續運作之規劃程序

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，使重要業務在系統發生事故、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，應考量下列事項：

（1）界定重要的業務作業程序，並訂定其優先順序。

（2）評估各種災害對業務可能的衝擊。

（3）維持永續運作之人員責任界定，以及緊急應變措施之安排。

（4）建立永續運作之作業程序及流程，並以書面或其他電子方式記載。

（5）應就緊急應變程序及作業流程，進行員工教育及訓練。

（6）應測試緊急應變計畫。

（7）應定期更新緊急應變計畫。

（二）業務永續運作規劃架構

1、應建立及維持單一的永續作業計畫架構，使各種不同層次及等級的計畫相互連貫,並應訂定測試計畫及維護計畫之優先順序。

2、每項業務之永續運作計畫，應明定行動之條件，以及員工執行計畫之責任;研擬新的資訊計畫，應與緊急應變計畫程序相一致(例如疏散計畫、現有電腦服務系統的預備作業安排，以及通信及空間的配置。)

3、在業務永續運作之整體架構內，應訂定不同層次及等級的計畫，每一層次及等級的計畫，應涵蓋不同的計畫重點及負責回復作業的人員安排。

4、業務永續運作計畫，應考量的作業程序如下：

（1）訂定緊急應變作業程序，規定如何在發生危害機關業務運作或危及生命的重大事件發生時，應立即採取的行動。

（2）訂定預備作業程序，規定如何將必要的機關業務活動或是支援性的服務，移轉至另外一個臨時的作業地點。

（3）訂定回復作業程序，規定如何採取回復作業。

（4）訂定測試作業程序，規定如何及何時執行測試作業。

5、每一層次的計畫以及每一項個別計畫，都應指定一位計畫執行督導人員。

6、緊急應變作業、人工預備作業及回復作業計畫等，應指定適當的單位或人員負責。

7、技術服務的預備作業安排（例如電腦及通信系統）應由技術服務提供者負責。

二、業務永續運作計畫之測試

1、業務永續運作計畫可能因事前的假設不正確、規劃不周全或設備及人員的職務調整變更,而無法發揮預期的作用，應定期測試及演練，以確保計畫的有效性，並使相關人員確實瞭解計畫的最新狀態。

2、應擬訂測試作業的時程，定期進行測試，使應變計畫維持在有效及最新的狀態;測試計畫可以定期測試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、組織及人員的調整變更而定期更新,以發揮計畫投資的效益及確保計畫持續有效。

2、應納入計畫更新之事項如下：

（1）採購新的設備，或是更新作業系統。

（2）使用新的問題偵測及控制技術（例如火災偵測）。

（3）使用新的環境控制技術。

（4）人員及組織上的調整變動。

（5）機關及人員地址及電話號碼的變動。

（6）契約當事者或是供應商的調整變動。

（7）業務流程的變動，新建或是撤銷作業流程。

（8）實務作業的變更。

（9）法規上的變更。

3、應指定專人負責計畫變更事宜，個別計畫原則上至少每一個月要檢查評估一次,完整的計畫至少應每年檢討評估一次。

4、應建立計畫變更的控制機制，以確保計畫變更前，以及賦予員工相關責任前,能將相關的訊息告知相關人員。

四、資訊安全事件緊急處理機制

（一）資訊安全事件之通報

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、員工如發現或懷疑有資訊安全事件時（包括系統有安全漏洞、受威脅、系統弱點及功能不正常事件等），應依事前訂定的通報管道,迅速通報權責主管單位及人員立即處理。

3、員工及與機關簽訂資訊安全協定的外部人員，皆應明確告知各種資訊安全事件的反應及報告程序,使其瞭解相關的處理程序。

（二）資訊安全弱點之反映

1、員工應隨時注意資訊系統或資訊服務施設內部之安全弱點、可能面臨的威脅，並迅速告知直屬業務主管或是系統服務廠商。

2、系統安全上的弱點，應由專業人員處理，不應任由系統使用者自行修改。

（三）軟體功能不正常之反映

1、使用者發現軟體功能有異常時，應迅速告知資訊支援單位或是服務廠商處理。

2、應建立軟體功能不正常之反映及處理程序：

（1）注意螢幕上出現的徵兆或訊息。

（2）立即停止使用電腦，迅速通知資訊支援單位。

（3）檢視軟體功能不正常的設備，再次啟動前，應以離線方式處理。

（4）在任何狀況下，使用者不應自行移除功能不正常的軟體；系統回復作業應由受過適當訓練及有經驗的人員執行。