交通部公路總局第三區養護工程處資訊安全政策

壹、資訊安全政策

一、資訊安全政策制定

（一）目的

公路總局第三區養護工程處（以下簡稱本處）為保護本處資訊資產，免於遭受破壞，不論這些破壞是來自於本處內部或外部以及來自人為、蓄意或意外，爰制定本資訊安全政策，以作為實施各項資訊安全措施之標準。透過本資訊安全政策之制定，明確宣示高階主管支持資訊安全之決心，並使相關人員有所依循。

（二）依據

本處透過適當的風險評估，明確分析資訊安全有關資產之主要性，並了解潛在風險;同時透過資訊安全管理機制，藉以控管風險至可接受之程度，且相關人員於執行政策所規範之事項時，皆需遵守「國家機密保護法」、「智慧財產權法」、「電腦處理個人資料保護法」、「行政院及所屬各機關資訊安全管理要點」及與客戶之合約規定。

（三）目標

為達到制定資訊安全政策目的，本處將依安全政策範圍訂定執行之工作規範，徹底實施，以確保下列安全功效。

1、保護資訊避免未經授權使用。

2、避免資訊揭露給予未經授權者，維護資訊機密。

3、避免未經授權者竄改資訊，保護資訊完整。

4、合法使用者及時取得所需資訊。

5、落實遵守資訊安全有關法律及規定，避免使用非法軟體。

6、建立系統備援機制，維持本處業務永續運作。

7、提供員工資訊安全訓練，強化整體安全認知

8、建置資訊安全控管設備及時偵測安全漏洞以防止電腦駭客入侵及病毒破壞。

9、建立即時通報系統，以期於安全事件發生時，可即時採取因應措施。

（四）涵蓋範圍

本資訊安全政策，包括下列事項：

1、 資訊安全之原則、標準，以及員工應遵守之規定，包括：

（1）本處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。

2、推行資訊安全工作之組織、權責及分工。

3、員工應負的一般性及特定的資訊安全責任。

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。

（五）適用性

本資訊安全政策所規範之事項，其適用之對象為本處職員及與本處有業務往來對象之人員；且涉及資訊安全管理之資產範圍者，皆有責任執行此一政策，並將獲得本局處管理階層的支援。

二、資訊安全政策之評估

（一）本資訊安全政策，訂定每年評估一次，進行獨立及客觀的評估，以反映本局處資訊安全管理政策、相關法令規範、資訊技術環境及業務之最新狀況，確保資訊安全之實務作業，確實遵守資訊安全政策，且確保資訊安全實務運作之可行性及有效性。

（二）資訊安全政策之評估，可責由具有專業技術及知識之外部稽核單位、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）每年一次對所屬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）資訊設備及系統提供者。

（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本資訊安全政策、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，以確保其符合本資訊安全標準；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如外部稽核單位之協助。

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，於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、透過公告程序，責成所屬人員瞭解本處資訊安全政策之相關規定，俾益其遵循。

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

一、資訊安全組織

（一）配合本處資訊安全政策之實施，「資訊安全推動工作小組」由本處處長擔任召集人，副處長擔任執行長，下設「安全處理小組」及「審查小組」，審查小組委員由本處各課室課長主任擔任，安全處理小組組長由交通資管中心主任擔任，組員由政風室、秘書室、交通資管中心、處外單位資訊人員推派，分別負責推動、督導、稽核、協調、管理、執行資訊安全事項。

二、資訊安全組織權責

（一）資訊安全責任

1、資訊安全相關政策、計畫、措施及技術規範之訂定，訂定保護個人資訊資產及執行所有資訊安全作業。

2、訂定各小組在資訊安全推動工作小組編制內應負擔之作業功能及扮演之角色，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、明定每一管理者應負的資訊安全責任。

4、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。

5、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。

6、訂定資訊安全之授權規定、等級及程序等，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）法規辦法的制定審核，由審查小組負責。

（2）資訊機密維護及稽核使用管理事項，由安全處理小組會同相關單位負責辦理。

（3）資料及資訊系統之安全需求研議、使用管理及保護等事項，由安全處理小組負責辦理。

（4）事件處理及通報、對外說明由安全處理小組負責。

2、業務性質特殊者，得視實際需要由高階主管調整上述資訊安全分工原則。

（三）資訊設備之使用授權

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，並依本處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：所有連線網路的設備，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，始得連線使用。

（四）跨部門機關之合作及協調

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，以評估本處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、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，將予適當的限制，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，得委請外部稽核單位或其他專業組織及團體，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、人員安全與管理

一、人員聘用之評估

（一）人員聘用之安全評估

聘用之人員，如其工作職責須使用處理敏感性、機密性資訊的資訊設備，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。

（二）機密維護之責任約定

1、資訊作業人員，應依相關法令課予機密維護責任，並簽署保密之書面約定，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。

3、人員離職或調離原業務部門時，相關的帳號應立即刪除或異動相關權限。

4、對於存取機密性或敏感性資訊或系統之員工，以及其他系統存取特定權限之員工應視情況建置必要之人力備援制度。

二、使用者資訊安全教育訓練

（一）資訊安全教育訓練

1、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、以人員工作角色及業務內容為基礎，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：本處資訊安全政策、資訊安全法令規定、資訊安全作業程序、各資訊系統之安全防範或安全訊息交流、機密性或敏感性資料之妥善收藏，以及如何正確使用資訊設備之訓練等。

3、在同意及授權使用者存取系統前，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、隨時對員工公告資訊安全相關訊息。

5、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，對外部的使用者，亦一併適用。

肆、資訊資產之分類與控管

一、資訊資產清冊之建立及保護

（一）建立與資訊系統有關的資訊資產清冊及安全分類，訂定本處資訊資產的項目、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、資料檔案、智慧財產等。

2、書面文件：合約、組織文件、人事紀錄、採購文件等。

3、軟體資產：應用程式、系統軟體、發展工具及公用程式等。

4、實體資產：電腦及通訊設備、磁性媒體資料及其他技術設備。

5、人員資產：員工、客戶、契約人員、清潔工、警衛等。

（三）資訊資產清冊應隨時更新，並確保完整性。

二、資訊安全之等級分類

（一）資訊安全分類原則

1、資訊安全等級評估方式：

風險值：即該項資產發生威脅事項時，對組織及系統之風險程度。

計算公式：風險值 = 資產重要度 × 威脅 × 弱點

各項值表示：1 -> 非常低
2 -> 低
3 -> 中
4 -> 高
5 -> 非常高

❖ 風險等級：依據資產之風險值判斷其等級，標準如下：

101 - 125 為『A』級，最高級：影響公共安全、秩序、生命財產。

71 - 100 為『B』級，高級：系統停頓，業務無法運作。

31 - 71 為『C』級，中級：業務中斷，影響系統效率。

1 - 30 為『D』級，普通：業務短暫停頓，可立即修復。

2、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。

3、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。

（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、磁性媒體、電子訊息及檔案資料等。

三、資訊安全之保護措施

（一）依據上述之資訊資產分類等級，執行適當之保護措施，例如：存取權限之審核等級、活動日誌之登入及覆核等等。

伍、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、重要資訊設備應裝置於獨立之機房內，並依機房門禁管制要點管制人員進出，以達保護、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、資訊設備安置時應遵循以下原則：

（1）設備應儘量安置於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）電腦作業區禁止抽煙及飲用食物。

（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、重要資訊設備應考量安置預備電源，並使用不斷電系統。

3、不斷電系統應定期維護測試，並依據維護廠商的建議，定期進行電池之更換。

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。

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，應有適當保護，避免暴露損毀。

（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。

（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）重要資訊設備應與專業資訊廠商簽訂維護契約，定期進行設備維護。

（2）設備的維護只能由授權的維護人員執行，且需有資訊人員陪同。

（3）應明確記錄有關之錯誤或警告之訊息。

（五）放置於外部空間之設備的安全管理

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、設置在本處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,在公共場所之電腦設備及資料儲存媒體應有人看管。

（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，例如設定適當密碼。

（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、磁帶等），應在報廢處理前詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體已確實移除。

（七）資訊設備誤用之防止

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，任何人皆不得存取系統存取。

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來決定。

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）管制區內不得攜入隨身碟、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由內部人員陪同，並記錄進出時間、攜帶之用品等；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）員工離職後，應立即撤銷進入管制區的權利。

（三）交通資管中心及機房之安全管理

1、支援重要業務運作的交通資管中心及電腦機房，應設立良好的實體安全措施；交通資管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、交通資管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） 交通資管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，應存放在遠離交通資管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） 應安裝適當的安全偵測及防制設備，例如：設置溫溼度計、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。

（6） 資訊重大事件處理程序應以書面方式記載，並定期演練及測試。

（7） 不上班或無人看護時，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，防止未經授權的人員進出；為降低未經授權的人員進入電腦機房的風險，非必要之資訊設備不得攜入機房。

2、得設立臨時作業區供外部人員進行資訊物品之裝配作業。

（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，應存放在櫃子內並上鎖。

（2）機密性及敏感性資訊，不使用或下班時應該上鎖，放在上鎖的櫃子。

（3）個人電腦及電腦終端機短暫離開不再使用時，應該上鎖及啟動螢幕保護程式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。

陸、通訊與操作管理

一、電腦系統作業程序及責任

（一）操作基本原則

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，以確保相關人員正確及安全地操作及使用電腦，並以其作為系統開發、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：使用特別的工具，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）資通安全責任之分散

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，應將資通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不同業務及功能。

（三）系統開發及系統實作之實體分開處理

1、系統開發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，應將系統開發及系統實作的實體設備分開處理，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、系統開發及系統實作之實體分開處理，應考量下列安控措施：

（1）系統開發及系統實作的軟體，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）系統開發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。

（四）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（例如資料或使用者密碼被破解、系統被破壞或資料損失等風險），並與廠商簽訂適當的保密合約書，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）廠商如何配合執行本局業務永續運作計畫。

（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因素，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時，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業務的需求。

（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、開發重要的系統時，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，在系統開發的每一階段，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）系統之備援規劃

1、應規劃資訊系統設備損害或電腦當機時，可維持本處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，由系統規劃人員加以界定；並應為每一項系統研訂適當的備援作業計畫。

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、資訊設備及系統的變更，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）評估作業變更之重大影響。

（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、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、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，進而提升員工對資訊安全警覺，健全系統之存取控制機制。

3、確保所有連網之電腦均處於執行病毒防治軟體狀態：於伺服器主機安裝病毒防治軟體之伺服器版本，並撰寫批次檔，令使用者登入內部網路時即自動執行病毒防治軟體之偵測。

若使用者未安裝病毒防治軟體之終端機版本，則設定系統自動安裝該程式;若已安裝該終端機端軟體，則系統會自動執行，並進行病毒碼版本之比對;遇有終端機端病毒碼版本先於伺服器病毒碼版本，則自動更新病毒碼版本，確保所有連上內部網路之電腦均處於執行病毒防治軟體狀態，且病毒碼版本為最新版本。

4、另使用者不得自行卸載或終止病毒防治軟體之常駐與執行（調整病毒防治軟體伺服器端設定為卸載終端機端軟體時需輸入密碼）。

5、定期檢核電腦病毒防治軟體相關報表，以確保伺服器及終端機之正常運作。

6、其他電腦病毒防範相關原則及措施如下：

（1）應建立軟體之管理政策，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採購維護合約或定期更新，並依廠商的說明書使用。
- 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。
- 為使電腦病毒影響資訊設備正常運作之程度降至最低，應建立適當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、軟體使用管理之規範

（一）本處軟體之使用、複製、交換及管理等程序，俾符合智慧財產權及資訊安全相關規範。

（二）軟體之取得程序

1、軟體採購之評估：交通資管中心主管檢視各部門之電腦化需求，必須以下列條件考慮決定該項需求是否自製或外購：

（1）本處現有的軟體設備下，是否達到該項需求。

（2）該項需求是否為多數人之需求，或只是某使用者單一需求。

（3）該需求是否有類似軟體在現有市場出售。

（4）現有出售軟體其成本與效益回收是否可以接受。

（5）比較自製及外購之成本。

（6）外購軟體是否可取得原始碼。

（7）外購軟體系統架構及功能是否完整且符合需求。

（8）外購軟體本處售後服務是否完善。

（9）外購軟體擴充性之優劣。

2、軟體之取得方式：

（1）若在評估階段之軟體，先請軟體廠商對本處內部做簡介，經部門主管或使用者認可，在符合需求及成本下，方決定購買。

（2）決定購買之軟體，統一由交通資管中心向合法廠商購入。

（三）軟體之使用與複製

1、本處員工使用有智慧財產權的軟體，應遵守相關法令及契約規定。新進員工均應簽訂「智慧財權同意書」，恪遵該約定書各項有關電腦軟體使用規定。

2、所有的軟體均在合法的權限下提供給使用者。

3、本處自行開發軟體及相關文件之智慧財產權歸屬於本處所有。

4、軟體使用及複製應考量以下事項：

（1）不應使用及保有未取得授權的軟體。

（2）應將本處之智慧財產權保護政策，以書面、電子或其他方式明確通知員工，禁止員工在未取得智慧財產權擁有者的書面同意前，將軟體複製到機器或使用。

（3）除非取得授權，不得將專屬的軟體複製到本處以外的機器設備。

（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）非一般公務所需軟體，非經部門主管許可不得借用及安裝，若因公務所需，需安裝非一般公務所需軟體，應填具「軟體需求申請表」，經核定後方得安裝、使用。

（四）軟體使用之稽核

1、定期稽核：

定期每月採不預訂時間及隨機方式抽查個人電腦軟體使用狀況（原則上各部門平均抽查一部）;遇有非法使用軟體之情事，並將查核結果會知該部門主管，另安排時間複查。

（五）軟體之管理與報廢

1、重要軟體應依程序登錄至本處資訊資產清冊中，所有軟體並應製作列表控管。

2、原版軟體購入後，皆予以拷貝乙份，作為合法備份使用。

3、原版軟體磁片或光碟與 License 均列冊管理並鎖入檔案櫃中，以免原版軟體損毀或遺失。

4、軟體購入後，應依軟體授權規定安裝，安裝完成後，原版軟體、授權證明、說明書等相關文件送交交通資管中心統一列管。

5、軟體之報廢依下列原則處理：

（1）軟體因更新需求購入後，先行觀察與現行作業系統及作業程序是否存有不相容情況，若無不相容情況得報廢之。前述觀察期間至少維持六個月。

（2）軟體報廢由負責軟體管理之單位（交通資管中心）負責辦理。報廢前先填具軟體報廢申請單，經核可後報廢之。

（3）為避免報廢軟體不當流出，軟體報廢時應由交通資管中心人員執行，並經測試確認軟體已完全無法執行。

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、使用者及交通資管中心人員，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備，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，應符合本處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，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，並記錄測試相關程序及結果，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，應訂定相關規定。

（6） 光碟及磁帶之標籤處標明所儲存之資料內容，包含檔案名稱及日期。

（二）系統作業紀錄

1、電腦作業人員應確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核，以確認其是否符合本局訂定的作業程序。

（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，並採取必要的補救措施。

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，確保系統作業錯誤問題已經排除。

（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全控管措施，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、電腦媒體設備之安全管理

（一）電腦媒體設備之安全管理

1、可攜式電腦安全管理

（1）內部人員配備之可攜式電腦

a、配備可攜式電腦之人員應維持使用環境之封閉性，儘量避免與本處外之電腦媒體設備進行檔案傳輸及交換。若因業務需要讀取外來磁片或檔案時，應先行掃瞄該磁片或檔案是否存有病毒。

b、於本處外部使用可攜式電腦時，應做好電腦安全管理工作，避免可攜式電腦遺失、無人管理或可攜式電腦內之檔案或資料遭竊取等。

（2）外部人員攜入可攜式電腦

a、維護廠商或委辦專案之承辦廠商，因業務需求得攜帶可攜式電腦進入本處。廠商攜入可攜式電腦時應經過申請登記程序，經相關業務部門核准後始得攜入。

b、外部人員攜入之可攜式電腦需連結至本處內部網路亦應經過申請程序，並經核准後方得連結本處內部網路。c、使用網路相關權限應由交通資管中心做適當之授權。

c、外部人員之可攜式電腦若要與機房內之機密級主機直接連線並傳輸資料時，應有相關人員陪同在場，避免資料遭不當竊取。

（二）機密性及敏感性資料之處理程序

1、針對本處歸類屬機密性及敏感性資料者加強安全保護，以防止洩漏或不法及不當的使用。

2、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）系統文件之安全管理

1、系統流程、作業流程、資料結構及授權程序等系統相關文件，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。

3、系統文件管理者及權責如下：

（1）系統文件應指定專人管理，管理者遇請假時，亦應有職務代理人代理其管理職務。

（2）系統文件使用者及管理者，涉及接觸機密資料者，應由權責主管先行做安全查核。

4、借用應經申請程序，由主管核定後擲交管理者辦理借用手續。

5、系統或程式經核准上線後，管理者應於兩週內更新相關系統文件，並將舊版系統文件確實以碎紙機銷毀。

（四）媒體設備處理之安全

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

2、應訂定電腦媒體設備的處理作業程序，以降低可能的安全風險。

3、電腦媒體設備之安全處理原則如下：

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

柒、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、對於跨區域之電腦網路系統，應特別加強網路安全管理。

3、利用公共網路傳送機密性及敏感性資訊，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）應建立管理遠端資訊設備的責任及程序。

（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區域的基礎架構上運作。

（二）網路服務之管理

1、網路系統的最高使用權限，應經權責主管人員審慎評估後，交付可信賴的專業人員管理。

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（Fire wall）、代理伺服器(Proxy Server)進行安全控管。

5、如果系統使用者已為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)職人員應依本處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本處規定，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，應以電子郵件或其它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本處內部或資訊安全處理小組反應。

9、網路系統管理人員針對存放重要資訊之主機，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。

11、應建置網路入侵偵測系統，確實即時監控網路活動狀況，當異常存取情事與活動發生時，該系統應能提供多種反應回報方式通知相關網路系統管理人員，以達及時監控與反映之功效。

（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）,僅能在授權範圍內存取授權之網路資源。

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，限制或撤銷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碼與密碼交付他人使用。

4、禁止網路使用者以任何方法竊取他人的登入身份識別碼與密碼。

5、禁止及防範網路使用者以任何儀器設備或軟體工具竊聽及截取網路上的通訊封包或資料。

6、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本處網路，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、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、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、本處外部取得授權的電腦主機或網路設備，與本處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。

12、禁止工作時間瀏覽非業務相關資訊。

（四）主機安全防護

1、存放機密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資料竊取與破壞等情事。

2、為提升伺服器主機連線作業之安全性，應視需要使用電子簽章及加密等各種安全控管技術，以建立安全及可信賴的通信管道。

（五）軟體輸入控制

1、應禁止網路上的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進行安裝及執行。

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。

（六）網路資訊之管理

1、對外開放的資訊系統，應儘可能安裝在乙部專用的主機上，並以防火牆與本處內部網路區隔，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)導致網路系統作業癱瘓等情事，預先作好有效的防範，以免影響網路服務品質。

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。如有必要，須採用加強之保護措施。

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(HTTP)，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。

7、網路系統管理人員於收到資訊系統異常狀況通知訊息(System Alarm)時，應立即向權責主管反映並作適當緊急應變處理，如有必要，將資訊系統自網路離線，以避免更大之資訊災害發生。

二、防火牆安全管理

（一）本處與外界網路連接的網點，應加裝防火牆，以區隔網際網路與企業內部網路，並且適當控制企業內部網路與網際網路間資料的傳輸與資源的存取。

（二）網路防火牆的安裝與網路架構之規劃及設備，應依本處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。

（三）防火牆應由網路系統管理人員執行控管設定，並依本處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，建立包括身分辨識機制、來訊服務（incoming service）、去訊服務（outgoing service）與系統稽核的安全機制，有效的規範資源被讀取、更改、刪除、下載或上傳等行為以及系統存取權限等資訊。

（四）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。如有必要，則需限定來源 IP，然以不超過三個 IP 為原則。

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

（六）網路系統管理人員應配合本處資訊安全政策及規定的更新，以及網路設備的變更，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。

（七）防火牆系統軟體，應定期更新版本，以因應各種網路攻擊。

（八）應適當開啟防火牆相關服務、封包、資料、管理、等稽核功能，並由系統管理人員定時檢視與分析稽核記錄檔案，並適當保留相關記錄，以利未來異常之追蹤，當發現異常活動記錄時應立即向主管反映與立即處置。

（九）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，應依據資訊安全事件通報處理程序，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相關系統主機;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)向本處內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、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、密等以上的公文及資料，不得以電子郵件傳送；機密性及敏感性資訊如有電子傳送之必要，得經加密處理後傳送。

5、為防範假冒本處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。

8、應於電子郵件伺服器加裝病毒或入侵偵測系統，避免因惡意攻擊之電子郵件流入企業內部網路。

捌、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需求相稱，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、機密性或敏感性報表系統、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，才能配賦給使用者權限；另外，應將系統存取特別權限之授權資料建檔，以明責任及義務，以備日後查考。

（三）使用者密碼之管理

1、應建立使用者密碼之管理制度。

2、建立密碼管理制度，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密碼之責任；如屬於群組軟體之使用者，應確保工作群組的密碼，僅限群組成員使用，並於群組人員有變動時，應儘速變更工作群組的密碼，以降低安全風險。

（2）為維持密碼的機密性，應以配賦臨時性密碼，並強迫使用者立即更改密碼的方式處理；使用者忘記密碼時，可提供臨時性的密碼，以利系統辨認使用者。

（3）應以安全的方法將臨時的密碼交付使用者，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密碼的機制。

（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）使用者密碼之管理

1、使用者選擇及使用密碼時，應遵守本處資訊安全規定。

2、應以安全有效的使用者密碼管理系統，鑑別及控管使用者身分。

3、應依下列原則配賦、管理及使用密碼：

（1）要求必須使用密碼並以嚴謹的程序核發密碼，明確規定使用者應負的責任。

（2）個人應負責保護密碼，維持密碼的機密性。

（3）應允許使用者自行選擇及變更密碼；系統應具備密碼輸入錯誤之更正功能。

（4）應避免將密碼記錄在書面上，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。

（5）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。

（6）使用者密碼的長度最少應由七位長度組成。

（7）應儘量避免以下列事項作為密碼：

- 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。
- 本處、單位名稱、識別代碼或是其他相關事項。
- 電話號碼。
- 使用者密碼、使用者姓名、群體使用者之密碼或是其他系統密碼。
- 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。

（8）使用者第一次登入系統時，系統應要求更改臨時性密碼。

（9）自動化登入系統之密碼，不宜存放在巨集或是功能鍵中。

（10）應定期更換密碼，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密碼。

（11）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密碼的更改周期為高。

（12）在登入系統程序中，系統不應顯示使用者的密碼資料。

（13）使用者密碼應與應用系統資料分開存放，

（14）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。

4、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的密碼。（例如:使用單向加密演算法將密碼加密）

（二）暫時不使用或無人看管資訊設備之安全管理

1、暫時不使用，或無人看管的資訊設備，應研擬適當的安全保護措施；安置在辦公區域內的資訊設備（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資訊設備管理規定，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資訊設備之安全管理，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，不宜只關閉通信系統或是終端機。

（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終端機的安全。

四、網路存取之安全控制

（一）網路服務之限制

1. 欲使用本處任何網路系統者，須先填具「使用者帳號申請單」，並確實填妥申請單上的各項欄位資料後，送交本處交通資管中心處理，未按表填寫申請者，得不予受理。

2. 本處網路系統管理者，須確實了解網路使用申請者的需求，具以建置新的網路使用者帳號及密碼，並賦予正確的網路使用權限。

3. 使用者應在授權範圍內存取網路系統服務事項。

（二）網路連線作業之控制

1、為確保系統安全，跨區域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）限制只能在特定的時間或日期進行系統存取。

（三）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安全性風險。

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完善、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）應建立自動化的終端機身分鑑別及控管系統，以鑑別及控管從特定位址連上網路的使用者身分。

（二）終端機登入程序

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）在登入系統程序中，建議應顯示“只有被授權的使用者才可存取系統”等警告性的資訊。

（2）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。

（3）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。

（4）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相關資訊。
- 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。

（5）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。

（三）使用者身分辨識

1、應對使用者核發使用者帳號，以明責任歸屬；使用者帳號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帳號。但應採取額外的安全控制措施，明確規範使用者的責任。

（四）終端機作業時間限制

1、安置在高風險地區，且不經常使用的終端機（例如，設置在公共場所或本處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。

（五）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終端機，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。

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）處理機密性或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相關人員。

（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、應用程式原始碼目錄，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，應指定乙位管理人員。

3、不應核發無限制存取應用程式原始碼之權限。

4、開發中或是維護中的應用程式，應與實務作業之程式原始碼目錄區隔，不應放置在一起。

5、應用程式原始碼目錄之更新，以及核發應用程式原始碼供程式設計人員使用，應由原始碼目錄管理人員執行。

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目錄的稽核軌跡。

8、舊版的原始程式應妥慎保管，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、系統文件、作業控制、資料定義及操作程序等資訊。

9、應用程式原始碼目錄之維護及複製，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，以作為日後查考及監督之用。

2、系統稽核軌跡應包括下列事項：

（1）使用者帳號。

（2）登入及登出系統之日期及時間。

（3）儘可能記錄終端機的識別資料或其位址。

（4）儘可能紀錄終端機之異常行為。

（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當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）機密及敏感性資源的使用情形。

3、特殊監督工具之使用，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、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評估，決定必須採行或應特別強化的資訊安全需求項目。

2、外部存取本處資訊系統之風險分析評估，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）第三者之存取對本處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處的資訊設備。

（二）第三者存取之安全契約

1、第三者存取本處之資訊設備，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恪遵之本處資訊安全規定、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）第三者應遵守的本處資訊安全規定。

（2）第三者可以使用的系統存取方法，以及使用者帳號及密碼的管理規定。

（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乙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）與第三者簽約的本處業務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，可確保本處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）確保第三者恪遵資訊安全規定的機制。

（16）對第三者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）第三者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，並與系統服務提供者協議。

（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、系統稽核工具應與開發中或是實作的系統分隔，且應存放在安全的地點。

3、在使用系統稽核工具時，應有系統服務提供者監督，以防止濫用系統稽核工具，確保系統資訊安全。

4、應注意系統稽核工具是否會影響本處系統之正常運作，以避免影響業務正常運作。

玖、系統開發與維護

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；新開發的資訊系統，或是現有系統功能之強化，皆應明定系統之資訊安全需求，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，亦可考量由人工加強安控措施；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，對本處可能帶來的影響程度。

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）評估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及補救措施。

（3）系統之資訊安全需求分析，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）應於相關文件規定系統之資訊安全控制措施，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、輸入應用系統的資料，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，對本處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。

（三）資料加密

1、對機密性及敏感性的資料，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，如本處內部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）作業用的應用程式執行檔更新作業，應限定只能由授權的管理人員才可執行。

（2）儘可能將執行檔存放在作業系統內。

（3）執行檔尚未測試成功，且未被使用者接受前，不應在作業系統執行。

（4）應建立應用程式執行檔的更新稽核紀錄。

（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，由專人負責複製作業。

（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）系統變更作業之控制程序

1、應建立正式的系統變更控制程序，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非正式區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、建立系統變更控制程序，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。
- 應規範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。
- 系統變更後，公告該系統使用者，並註明異動之範圍、時間及可能之影響。
- 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。如確定舊版系統文件無須再使用，應依照系統文件報廢銷毀程序處理之。
- 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，以及危害鑑別及控管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。

拾、永續經營管理

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備援作業安排，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。

3、將測試結果做成書面文件，並檢討尚需修正或改進之處，以確保計劃之可行性。

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半年要檢查評估一次，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、資訊安全事件通報處理程序

（一）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）資訊系統環境遭入侵或破壞。

（3）業務資料不完整，或資料不正確導致的作業錯誤。

（4）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通安全規定的證據。

（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。

（二）資訊安全事件之通報

1、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「資訊安全事件通報處理程序」訂定的通報管道，迅速通報權責主管單位及人員立即處理。

2、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。

（三）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，應由專業人員陪同處理，不應任由系統使用者自行修改並且備份。

（四）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。

（五）檢討作業

1、針對已發生且解決之安全事件，應於事後檢討何處須再加強安全預防程序。

拾壹、內部稽核及其他

一、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）在系統終端機上顯示訊息。

（3）發送警示訊號到網路管理系統。

（4）啟動管理控制台的警示器。

（5）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(如網路服務本局)，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。

3、保留相關追查紀錄以供作為日後證據之一。

二、系統安全稽核

（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之稽核資料。

（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正式的系統分隔，且應存放在安全的地點。

三、外部稽核作業

（一）外部稽核依據

1、稽核作業可分為內部稽核及外部稽核，其中外部稽核作業得委由民間專業機構辦理。

2、委託外部機構進行外部稽核作業前，應簽訂委辦合約，要求外部稽核單位不得洩漏本處有關資料或機密並訂立適當之違約罰責。

（二）外部稽核作業

1. 委外機構進行外部稽核實應遵守本處各項資訊安全規範。

2. 外部稽核進行查核時，各部門應予配合。

3. 外部稽核所查各項缺失暨建議，各部門應著手修正。

四、軟體使用規範

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。