中央研究院

資訊科學研究所

電腦系統安全管理作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I312

版　　本：1.0

核准日期：115 年 4 月 24 日

文件制／修訂紀錄表

版次	修訂日期	修訂單位	修訂者	核准者	修訂內容
1.0					新擬訂文件

目錄

壹、目的

中央研究院資訊科學研究所（以下簡稱本所）為維持本所資通系統之正常運作，有效管理本所電腦軟硬體設備，確保及監控系統與資料之安全性，對資通安全的操作管理部份，訂定電腦系統安全管理作業說明書（以下簡稱本說明書）。

貳、依據

一、 中央研究院資通安全暨個人資料保護政策及規範

二、 中央研究院資通安全管理規範實施要點

參、 範圍

本說明書所稱電腦系統，包含本所網路設備、群組計算設備、伺服主機、資料儲存設備、附設或嵌入於儀器之電腦設備等，及其作業系統與應用系統。

肆、權責

一、 使用人員

(一) 妥善使用相關設備。

(二) 負責通知資訊設備異常及故障情況。

二、 設備管理者

(一) 負責採購、保管與定期檢查資訊設備。

(二) 負責設備故障維修作業，無法自行排除之故障聯繫廠商執行維修。

(三) 檢測資訊設備所安裝之系統是否符合作業標準，並查核所安裝之軟體是否經合法授權。

(四) 負責陪同外部維護人員進行設備維護。

(五) 依據「B330-I305_資產管理制度作業說明書」，善盡維護實體資產及保管機密資料的責任。

(六) 依據資產使用年限及使用狀況，進行資產報廢申請。

(七) 負責資訊設備備品之管理，辦理資訊設備盤點作業。

三、 權責主管

(一) 指派專人負責保管資訊設備。

(二) 監督資訊設備維護管理相關工作。

伍、作業說明

一、 為保障本所資通作業環境安全，伺服器與個人電腦應配合資服處套用政府組態基準(GCB)，若有未套用之規則，應進行紀錄於「B330-I312-02_GCB 例外管理項目清單」並說明未套用原因及配套措施。

二、 伺服器與個人電腦在不影響業務運作，應確認已安裝端點防護軟體及防毒軟體，並需定期進行軟體更新及檢查。

三、 伺服器與個人電腦應使用本機防火牆限制端點存取，關閉不需要的通訊埠(TCP/UDP Port)。

四、 資安風險較高之通訊埠（如遠端連線及網路芳鄰）預設應予關閉，如有使用需求，須提出申請並加強管控，避免遭不當利用。

五、 伺服器與個人電腦應於安全性更新及弱點修補發佈後依據「中央研究院資通安全管理規範實施要點」完成更新作業(包含作業系統、Java、Adobe、office…等)。

六、 如接獲外部單位通報之弱點應於接獲通報後依據「中央研究院資通安全管理規範實施要點」完成弱點修補；若未依限完成修補，應限制網路連線。

七、 如主機/設備汰舊換新舊不再使用，應於新主機/設備上線穩定運作後關閉、集中保管並依保存年限進行報廢，儲存於該主機/設備的電磁資訊應予以抹除。

八、 系統或設備之原廠服務已終止支援(EOS)時應儘速進行汰舊換新或有適當管控措施。

九、 物聯網設備(網路印表機、門禁系統、網路攝影機）應只採用內部 IP 位址，原則不允許與 Internet 連線，如有需求，應該限制存取來源，並應依照網路安全管理辦理，宜依設備功能屬性考量採用封閉型網路架構，不與其他設備互連。

十、 定期執行資通系統與物聯網設備安全檢測作業。

十一、 針對資通系統與物聯網設備安全檢測掃描結果的高、中度風險弱點應辦理修補作業或採取替代防護措施。

十二、 即時通訊軟體管理機制，依照全院「即時通訊軟體規範」辦理。

十三、 電腦病毒及惡意軟體之防範

(一) 病毒防護軟體由本所電腦資訊人員進行規劃評估與建置或配合資服處要求佈建。

(二) 本所連外網路宜使用入侵偵測防禦系統，電腦資訊人員須隨時監控非法入侵之行為，並收集入侵證據作為法律控訴之證物。

(三) 本所同仁應使用合法具版權軟體，避免上網下載來路不明之軟體、資料。

(四) 與外部交換資料時，使用資料前應啟動病毒防護軟體偵測。

(五) 本所同仁應注意病毒防護與更新資訊。

(六) 本所同仁操作電腦時，發現病毒應立即清除，如無法自行清除病毒時，需通知電腦資訊人員協助處理。

十四、 作業存取控制管理

本所資通系統之存取管制必需考慮業務及如下之安全需求，同時符合資通安全政策。伺服器主機或設備應指定專責管理人員，如管理人員離職或調職應指派新的管理人員接手並妥善交接。

(一) 電腦帳號管理

1. 本所同仁與外部人員有操作資通系統需求時，應填寫「B330-I309-01_資通系統帳號使用申請表」，由資通系統權限管理人員依申請權限配發帳號及密碼。
2. 使用者帳號名稱不應帶有足以辨識使用者權限的資訊。
3. 作業系統中只允許必要之帳號存在，非必要之帳號應予刪除，特別是客戶（guest）與匿名（anonymous）帳號一定要取消其登入之權限。
4. 應每年至少一次清查使用者帳號，確保使用者帳號資料之正確性與使用必要性，並依實際狀況辦理帳號取消、停用或權限調整，並將清查的結果填入「B330-I309-02_帳號清查紀錄單」後送清查單位主管審核。

(二) 通行碼之使用

擁有本所同仁資通系統帳號、通行碼之人員。於登入系統時，應盡到善良使用者的責任，並遵守密碼複雜度原則如 K@tVs0wD（英文字母、大小寫、數字及特殊字元，可參考「B330-I309 存取控制作業說明書」，此外，應保持高度之警戒心，防範不法人士以社交工程方法（Social Engineering）騙取帳號及通行碼入侵。

(三) 系統維護帳號及系統特殊權限帳號管理

本所各系統及設備授權委外廠商辦理安裝或維護，委外廠商人員於合約簽訂時簽署保密合約後，由管理人員審查控管。

1. 應嚴格管控系統之權限，僅授權予必要人員，並將系統權限授權資料建檔，以備日後之查考。
2. 系統的維護及特殊權限，應每年至少清查一次，清查的結果應送系統管理人員之主管審核。
3. 人員（包含本所同仁、工讀生及委外廠商人員）離職應刪除或變更其狀態(如停用、刪除)。

(四) 使用者身分鑑別

為保護資通的安全，本所非公開資訊之應用服務應採用使用者帳號、通行碼登入管控，作業記錄（Log）應包含使用者登入之資訊及網路 IP 位址。

(五) 連線作業時間的限制

本所應設定系統登入程序之時間限制，如果超出時間限制，系統將自動登出。

(六) 個人電腦之資產保管人應每年填寫「B330-I312-01 主機暨個人電腦自我審查表」由權責主管指定專人進行複查且複查人員間得彼此交互複查。

(七) 時間同步

本所之伺服主機與網路設備，應參照本院鐘訊源設定網路時間同步，建議若無法自動同步則採手動方式至少每月一次進行時間同步作業。

十五、 伺服器主機管理

(一) 系統軟體安裝管理

1. 主機系統中啟動的應用服務，如非必要，不得以系統預設最高管權限帳號；如 administrator、sa 或 root 權限的帳號來執行，降低應用系統被入侵的風險。

2. 主機系統負責人員於安裝系統軟體或應用軟體時，應僅針對必要使用之部分進行安裝，主機系統則應僅啟動必要之服務。
3. 新建置或安裝之軟體，安裝完成後應立即更新設備預設之密碼。
4. 避免修改套裝軟體，有必要修改時需採嚴格管制。
5. 系統公用程式(Utility)需進行安全管控，至少應：
   (1) 嚴格限制及控制電腦公用程式之使用，將有權使用系統公用程式的人數限制到最小的數目。
   (2) 移除非必要的公用程式及系統軟體。

(二) 作業安全管理

1. 主機作業系統軟體與應用系統軟體的修補程式是處於最新的狀態。
2. 未經授權許可不得閱覽、增加、刪除或修改其他使用者上傳之檔案；如發現有可疑之網路安全情事（如病毒或特洛依木馬等），通知資通安全小組進行適當的工具追蹤檢查相關檔案，採取必要處理措施，事後再行知會該檔案擁有者，如確定為感染病毒，為避免病毒擴散，應逕行掃毒或刪除檔案再行知會該檔案擁有者。
3. 重要系統主機之資產保管人應每年填寫「B330-I312-01_主機暨個人電腦自我審查表」由權責主管指定專人進行複查且複查人員間得彼此交互複查。
4. 紀錄(Log)應轉存至具有帳號權限管控之日誌主機(Log Server)中，且應至少保存 6 個月以上。
5. 至少每季定期檢視伺服器主機維運情形並紀錄於「B330-I312-04_伺服主機系統檢視表」。

十六、 安全性監控

系統監控與稽核軌跡（Log trail）之稽查應包括下列項目：

(一) 使用者帳號系統登入的記錄，確定使用者帳號是否有異常使用的情形。

(二) 系統特殊權限帳號使用的情形及配置情形。

(三) 系統存取失敗情形。

(四) 例外事件及資通安全事項的稽核記錄。

系統監控與稽核軌跡（Log trail）之稽查至少應定期執行，並留下稽查

記錄。

十七、 系統安全管理

(一) 稽核監視系統與事件紀錄管理

1. 網路與安全監視系統

應設置或使用防火牆、入侵偵測系統或網路管理系統對網路使用狀態進行監視，並應定期檢視相關紀錄以達到監視的目標。

2. 主機稽核(Log)系統

資通系統應保留所有系統紀錄，電腦資訊人員不得新增、刪除或修改稽核資料檔案，避免於安全事件發生後造成追蹤查詢之困擾。

(二) 系統弱點檢測及修補

為強化資通系統的安全，降低系統軟體已被揭露的漏洞或是應用軟體留下的後門，甚或是不當引入的木馬程式對本所造成安全的危機，執行系統弱點檢測(如: 弱點掃瞄、資安健診、滲透測試等)是一種適當的防護手段，另單位應就政府機關資安弱點通報或外部情資公告之弱點，清查單位內受影響之電腦系統，安排期程落實修補。

(三) 弱點檢測的方法與策略

本所弱點檢測的策略為本所自行、委外或向本院資服處申請對本所各主機系統服務進行檢測，偵測不當的服務與軟體的弱點或後門，模擬外部惡意攻擊者所能接觸到的範圍，可以真實檢測出目前實際暴露在 Internet 可能被利用的弱點。

弱點檢測之頻率為每年執行一次或視情況不定期執行。

(四) 弱點檢測的後續處理

1. 弱點檢測結果初步分析

弱點檢測報表應按風險高低分類，做為漏洞修補優先順序之參考依據。

2. 漏洞修補評估

辦理漏洞修補前，應與各相關系統負責人討論初步檢測分析結果，評估漏洞修補之影響範圍、修補方法，施作時程等並完成修補。

修補的方式可為更新作業系統 patch、關閉無需之服務、更新軟體版本、限制服務提供目標等方法，另於評估過程亦應確認弱點是否為誤判，必要時

得以人工檢視進行，並紀錄於「B330-I312-03_弱點修補紀錄表」。

3. 系統漏洞修補期限

針對前兩個等級風險弱點項目，應依據「中央研究院資通安全管理規範實施要點」完成修補，無法修補則應提出其他改善或保護措施。

4. 弱點修補追踪:

(1) 自行、委外或由資服處統一檢測之系統，應於修補期限內就指定之修補範圍完成修補及回報，並紀錄於「B330-I312-03_弱點修補紀錄表」保存相關紀錄備查。

陸、參考文件

一、 B330-I309-01_資通系統帳號使用申請表

二、 B330-I309-02_帳號清查紀錄單

柒、使用表單

一、 B330-I312-01_主機暨個人電腦自我審查表

二、 B330-I312-02_ GCB 例外管理項目清單

三、 B330-I312-03_弱點修補紀錄表

四、 B330-I312-04_伺服主機系統檢視