中央研究院

資訊科學研究所

網路安全管理作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I310

版　　本：1.1

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
1.1	114/11/18	資訊室			依據 ISO27001 改版進行文件調整

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，有效管理本所網路設備，確保其安全性，對網路安全的操作管理部份，訂定網路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

本程序適用於本所提供服務內、外部使用者之網路管理相關作業。

肆、權責

一、 網路使用者

經授權並遵循相關規定，方得使用網路。

二、 網路管理者

依據「機器對外開放服務申請或異動(防火牆)」線上申請，獲取適當權限。

三、 網路業務單位權責主管

核准網路設備及連線申請，並督導網路設備之安全管理。

伍、作業說明

一、 網路使用規定

本單位同仁使用網路時應於授權範圍內存取網路資源，遵守臺灣學術網路規範等相關規定，以保護本所網路之安全。此外，應遵守下述規定：

(一)利用伺服主機或作業系統網路芳鄰的檔案分享功能提供他人存取檔案時，應僅針對必要對象開放使用權限，並避免將權限完全開放，使用完畢後後應關閉權限。

(二)敏感性資料及公文，避免以電子郵件或其他電子形式於網路傳遞，如有於網路傳輸的必要時，應施以加密措施。

二、 網路分區及網路存取管制

(一)為管制網路存取及避免資安事件擴大，網路應依其提供之服務或使用者之類型予以區分，如 IP 位址網段，並產製網路架構圖。

(二)各網路分區原則不得互相連線，如有連線需求，須請提出申請，於核可後方得使用。各網段之防火牆規則(policies)應採用白名單機制。

(三)訪客僅開放對外瀏覽網頁所需之必要服務埠(port，如:TCP port 80、443 等)且不開放與其他網段連線。

(四)對外服務區原則不開放對外連線。

(五)防火牆規則開通以最小化為原則，限制來源及目的 IP 位址(來源 IP 位址與目的 IP 位址範圍不宜過大)、且僅開通需要的服務埠及設定規則開通時效性。

(六)如需開通或變更存取控制策略時，應填寫「機器對外開放服務申請或異動(防火牆)」線上申請，經主管同意後開放。

(七)防火牆規則異動申請經審核通過後，申請人應隨時注意使用期間(時段）之必要性，遇有系統續用、調整、停用或使用屆期時，應主動申請防火牆規則續用、調整或撤銷。

(八)防火牆規則異動申請經審核通過後，申請人應隨時注意使用期間(時段）之必要性，遇有系統續用、調整、停用或使用屆期時，應主動申請防火牆規則續用、調整或撤銷。資訊室資訊人員對於限期之網路服務連結申請應採列管措施，遇有屆期或逾期者，則主動關閉防火牆規則，不另行通知；對於職務異動或服務內容變動者，應主動檢討其申請或使用之防火牆規則，查有非必要對其開放之防火牆規則時，應通知後取消該防火牆規則。

(九)應限制對外部惡意網站之存取，以降低資安風險。

三、 網路設備管理

(一)為確保網路設備之機密性、完整性及可用性，應依據「B330-I305 資產管理制度作業說明書」之規定控管。

(二)網路設備應由專人管理、維護，並留有紀錄。

(三)網路設備部署前，應進行安全與作業影響評估。

(四)網路設備安裝時應考量場地之安全與通風散熱。

(五)為保護網路設備，若電源不穩定，宜搭配不斷電設備。

(六)為維持網路運作，重要網路設備應訂定故障修復時限。設備若由廠商保固或維護，契約應書載明修復時限與違約罰則。

四、 遠端連線管理

(一)需使用遠端管理網路連接設備時，應於網路連接設備中設定適當之存取控制清單，限制遠端管理之來源位置。

(二)廠商維護方式以到場服務為原則，若有遠端連線作業之必要時需填寫「機器對外開放服務申請或異動(防火牆)」進行控管，對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路連線方式(如https)及時間以確保網路安全。

(三)非經主管授權或允許，禁止執行遠端連線存取作業。

五、 網路流量管理

(一)宜監控與記錄重要網路設備流量，並即時通報異常狀況。

(二)若重要網路設備流量異常，網路管理者應立即調查異常原因採取防護措施，維持網路之正常使用。

六、 防火牆管理

(一)防火牆應保留日誌(Event 或 Log)6 個月，不得新增、刪除或修改內容，避免於資通安全事件發生後造成追蹤查詢之困擾。

(二)日誌的產生應包含事件類型、發生時間（注意是否與本院進行鐘訊同步作業）、位置及任何與事件相關之使用者身分識別等資訊，採單一日誌，並考量納入日誌管理設備之必要，以確保輸出一致性。

(三)每 6 個月例行性檢視日誌 之綜合分析報告，分析異常狀況，及早發現潛在的資安威脅，以維持系統正常穩定運作。

(四)當日誌處理失效且依規定需即時通報者，應於時效內通報本所。

(五)防火牆設定或規則變更前應執行備份，並執行設定組態檔案(Config Files)定期備份。

(六)應每年定期盤點防火牆規則並記錄於「機器對外開放服務申請或異動(防火牆)」，檢查是否有不必要之連線規則。

七、 雲端服務作業

採用雲端服務時，其服務協議或合約內容係預先定義且不接受協商，本所欲取用公有雲之雲端服務前，應先了解雲端服務提供之服務層級協議（SLA, Service Level Agreement）內容是否符合本院資安要求及現行法令、法規規定。

(一)雲端服務規劃：

1. 採用雲端服務時，需進行可行性評估，可參考「B330-I314_委外安全管理作業說明書」進行評估購置，確保所使用服務類型或技術，不得牴觸現行法律或內部規定。
2. 雲端服務供應商及代理商不得為大陸地區廠商。
3. 雲端服務供應商及代理商所在地理位置與儲存本所資料的所在地不得在大陸地區（包含香港與澳門），並不得跨該等境內傳輸相關資料。
4. 雲端服務需有相關第三方檢測或認證單位之檢測安全報告，並提供日誌保存功能，包括記錄登入名稱、時間、帳號與權限變更及資料存取等內容，應確保其完整性與正確性並符合本院保存年限（至少六個月）要求。
5. 雲端服務平台依照其服務種類，提供該服務之防入侵機制、監測活動管理及防範惡意軟體等措施。
6. 雲端服務供應商或代理商須具有安全事件管理機制，包括事件通報流程、事件處理流程。
7. 依照「B330-I305_資產管理制度作業說明書」，應列於資訊資產清冊，必要時進行風險評鑑作業，以能適時提出合宜改善計畫。

(二)雲端服務取得：

以政府電子採購網共同供應契約平台之雲端服務供應商或具良善資訊安全管理作為能力，須取得 ISO/IEC 27001 資訊安全管理系統認證為選商考量。

(三)雲端服務使用：

1. 資通系統建置於雲端服務時，應符合「資通安全責任等級分級辦法」之系統防護需求等級。

2. 雲端服務平台應提供定期儲存與備份雲端資料之功能，並善盡保管責任。

3. 若雲端服務平台若發生疑似資訊安全事件時，應主動通知本所雲端服務管理者，雲端服務管理者依「中央研究院資通安全管理規範實施要點」做後續辦理。

4. 資料於雲端服務進行傳輸時，需使用標準化網路協定，如涉及敏感性資料傳輸，應採用加密網路傳輸協定，以確保資料機密性與完整性。

5. 雲端服務供應商及代理商，除執行受託業務外，應保證不得存取客戶資料， 且不得為委託範圍以外之利用。

6. 雲端服務供應商或代理商須監視雲端服務運行持續性，定期提供維護紀錄報告。

(四)雲端服務退出：

雲端服務平台應提供退出所需之功能如下，以確保雲端資料自有權，並應評估下載過程之安全性、完整性。

1. 雲端資料下載功能。

2. 雲端資料刪除功能（包含備份文件及處理中文件）。

陸、參考文件

一、B330-I305 資產管理制度作業說明書

二、B330-I314 委外安全管理作業說明書

三、中央研究院資通安全管理規範實施要點

四、中央研究院資訊科學研究所網路及電腦使用規則

五、中央研究院資訊科學研究所網路分區

柒、使用表單

一、**「機器對外開放服務申請或異動(防火牆)」電子表單。**

二、B330-I310-02 防火牆規則清查表