中央研究院

資訊科學研究所

資產管理制度作業說明書

機密等級：□公開 ■內部 □敏感

編　　號：B330-I305

版　　本：1.4

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	112/04/13	資訊室			依 111 年總統府稽核修訂
1.2	113/10/18	資訊室			新增伍、五資通系統防護需求分級原則。
1.3	114/11/18	資訊室			依據 ISO27001 改版進行文件調整
1.4	115/03/31	資訊室			新增十四、對外開放伺服器管理

目錄

壹、目的

中央研究院資訊科學研究所（以下簡稱本所）為健全資訊資產之處理，訂定資產管理制度作業說明書（以下簡稱本說明書）以資遵循。

貳、依據

一、 資通安全管理法及其子法

二、 中央研究院資通安全暨個人資料保護政策及規範

三、 中央研究院資通安全管理規範實施要點

四、 ISO/IEC 27001 資訊安全管理系統（Information Security Management System，ISMS）

參、範圍

本所各項資訊資產之清查、鑑別、分類分級、評價與維護等管理作業。

肆、權責

一、 資安推動小組

維護並保存資訊資產清冊

二、 資訊資產管理單位

對該項資訊資產具有判斷資產價值、決定存取權限或新增、刪除、修改權限，以及執行資訊資產日常保護、異動與維護之作業，同時也是資訊資產的擁有單位。

三、 資訊資產使用單位

以實際或邏輯方式使用該項資訊資產之人員，對於被授權使用資產之單位或人員，應依各項安全程序正確使用操作資產。

伍、作業說明

一、 資訊資產採購與驗收

各項資訊資產之採購與驗收，由需求單位依據「資通安全管理法及其子法」、「政府採購法」及「中央研究院採購作業要點」之規定辦理採購與驗收。

二、 資訊資產鑑別

(一) 資訊資產管理單位應鑑別其所管轄內所有資訊資產之價值。

(二) 資安推動小組應鑑別所管轄之資訊資產，建立「資訊資產清冊」，定期更新與維護以確保資訊資產編號及清單之完整性。。

三、 資訊資產盤點與異動

(一) 資訊資產管理者應進行資訊資產盤點，建立「資訊資產清冊」，且至少每年依盤點及價值鑑別結果檢討一次以確保與現況一致。

(二) 當範圍內有以下的狀況發生時，則實施不定期更新及覆核，以確保「資訊資產清冊」之正確性及完整性。

1. 有新增、變更或移除資訊資產。
2. 資通系統有重大異動。
3. 作業環境調整或改變。

四、 資訊資產分類及價值評估

資安推動小組負責執行資訊資產分類及分級作業。

(一) 資訊資產分類

資訊資產分為五大類，分別為資訊類(IF)、軟體類(SW)、實體類(HW)、服務類(SE)及人員類(PE)，各分類說明如下表：

分類	說明
資訊類(IF)	經過處理以紙本或電子形式儲存之有價值的資訊，如：作業文件、系統文件、原始程式碼、資料庫資料、參數檔、稽核軌跡資料、申請表單、管理表單、訓練執行紀錄、專案合約管理資料、ISMS 相關紀錄、備份資料等。
軟體類(SW)	作業系統、應用系統、網站服務系統、應用工具軟體、資料庫管理系統（DBMS）、資通安全系統、一般套裝軟體等。
實體類(HW)	伺服器、儲存設備、通訊設備、週邊設備、個人電腦、公共使用電腦、行動裝置、日常作業事務機器(印表機、掃瞄器、傳真機、影印機)、物聯網設備(門禁設備、空拍機、監視器、戶外裝置...)等。
服務類(SE)	相關基礎設施及其他機關內部之支援服務，含基礎設施(市電、UPS不斷電系統、空調、消防、照明...)、實體環境（辦公室作業區域、電腦機房等）、通訊服務等。
人員類(PE)	主管、資訊人員、一般人員、駐點人員、委外廠商等。

(二) 資訊資產價值評估

依資訊資產之特性與實際需要進行資訊資產分級。資訊資產依據機密性、完整性及可用性性質區分不同價值，價值評分標準說明如下：

1. 機密性（Confidentiality）

確保只有被授權的人可以存取。

2. 完整性（Integrity）

保證資訊及處理方法的準確性和完整性。

3. 可用性（Availability）

確保被授權的人在需要時可以取得資訊和服務。

4. 資產價值等級＝MAX（機密性價值、完整性價值、可用性價值）。

5. 各類資訊資產價值評估標準如下

(1). 資訊類(IF)資訊資產價值評估標準

價值	機密性(C)	完整性(I)	可用性(A)
1	資產內容為得對外公開之一般性資料，在外流傳不會對組織造成損害者。	資產內容遭受未經授權的破壞或修改，對業務衝擊可忽略。	組織可以接受 5 個工作天(含)以上資產內容無法使用之情形。
2	資產內容為得對內公開之一般性資料，對內流傳不會對組織造成損害者。	資產內容遭受未經授權的破壞或修改，將對業務產生衝擊，但業務不致中斷。	組織可以接受 3 個工作天(含)以上至5天內資產內容無法使用之情形。
3	資產內容不涉及法規規定應保密或保護之資料，但洩漏後可能使組織遭受損害者。	資產內容遭受未經授權的破壞或修改，將對業務產生一定影響，且可能導致暫時性業務中斷，但可迅速處理改正。	組織可以接受 1 個工作天(含)以上至3天內資產內容無法使用之情形。
4	資產內容為法規規定應保密或保護之資料，洩漏後組織必須承擔法律責任及行政責任者。	資訊內容遭受未經授權的破壞或修改，將對業務產生重大影響，且可能導致暫時性業務中斷。	組織可以接受 4 小時(含)以上至1天內資產內容無法使用之情形。

價值	機密性(C)	完整性(I)	可用性(A)
5	資產內容為國家機密或保護之資料，洩漏後組織必須承擔法律責任及行政責任者。	資訊內容遭受未經授權的破壞或修改，將對業務產生重大影響，且可能導致長時間嚴重的業務中斷。	組織可以接受 4 個小時(含)以內資產內容無法使用之情形。

(2). 軟體類(SW)資訊資產價值評估表

價值	機密性(C)	完整性(I)	可用性(A)
1	資產不具保密價值，即使洩漏後也不會使組織安全遭受損害者。	資產遭受未經授權的破壞或修改，不會產生重大影響且(或)對業務之衝擊可忽略。	組織可以接受 5 個工作天(含)以上資產無法使用之情形。
2	資產為僅限組織內部應用之資訊，但揭露後應不致產生嚴重損害者。	資產遭受未經授權的破壞或修改，其產生之影響對業務衝擊輕微，可迅速處理改正。	組織可以接受 3 個工作天(含)以上至5天內資產無法使用之情形。
3	資產為具有保密價值之資訊，洩漏後可能使組織安全或形象遭受明顯損害者。	資產遭受未經授權的破壞或修改，將對業務產生明顯衝擊影響。	組織可以接受 1 個工作天(含)以上至3天內資產無法使用之情形。
4	資產為具有保密價值之資訊，洩漏後將引起組織安全遭受重大的損失者。	資產遭受未經授權的破壞或變更，將對業務產生重大影響，且可能導致暫時性業務中斷。	組織可以接受 4 小時(含)以上至1天內資產無法使用之情形。
5	資產為具有極高機密價值的資訊，資訊揭露予非授權者將危及國家安全者。	資產遭受未經授權的破壞或變更，將對業務產生重大影響，且可能導致長時間嚴重的業務中斷。	組織可以接受 4 個小時(含)以內資產無法使用之情形。

(3). 實體類(HW)資訊資產價值評估表

價值	機密性(C)	完整性(I)	可用性(A)
1	資產無此特性。	資產遭受未經授權的破壞或修改，不會產生重大影響且(或)對業務之衝擊可忽略。	組織可以接受 5 個工作天(含)以上資產無法使用之情形。

價值	機密性(C)	完整性(I)	可用性(A)
2	資產為僅限組織內部應用之資訊，但揭露後應不致產生嚴重損害者。	資產遭受未經授權的破壞或修改，其產生之影響對業務衝擊輕微，可迅速處理改正。	組織可以接受 3 個工作天(含)以上至5天內資產無法使用之情形。
3	資產為具有保密價值之資訊，洩漏後可能使組織安全或形象遭受明顯損害者。	資產遭受未經授權的破壞或修改，將對業務產生明顯衝擊影響。	組織可以接受 1 個工作天(含)以上至3天內資產無法使用之情形。
4	資產為具有保密價值之資訊，洩漏後將引起組織安全遭受重大的損失者。	資產遭受未經授權的破壞或修改，將對業務產生重大影響，且可能導致暫時性業務中斷。	組織可以接受 4 小時(含)以上至1天內資產無法使用之情形。
5	資產為具有極高機密價值的資訊，資訊揭露予非授權者將危及國家安全者。	資產遭受未經授權的破壞或修改，將對業務產生重大影響，且可能導致長時間嚴重的業務中斷。	組織可以接受 4 個小時(含)以內資產無法使用之情形。

(4). 服務類(SE)資訊資產價值評估表

價值	機密性(C)	完整性(I)	可用性(A)
1	資產無此特性。	資產內容部分遭受損害或錯誤，不會產生重大影響且(或)對業務之衝擊可忽略。	組織可以接受 5 個工作天(含)以上資產內容無法使用之情形。
2	資產內容涵括限組織內部應用之資訊，但揭露後應不致產生嚴重損害者。	資產內容部分遭受損害或錯誤，其產生之影響對業務衝擊輕微，可迅速處理改正。	組織可以接受 3 個工作天(含)以上至5天內資產內容無法使用之情形。
3	資產內容屬機密，洩漏後可能使組織安全或形象遭受明顯損害者。	資產內容部分遭受損害或錯誤，將對業務產生明顯衝擊影響。	組織可以接受 1 個工作天(含)以上至3天內資產內容無法使用之情形。
4	資產內容屬機密，洩漏後將引起組織安全遭受重大的損失者。	資產內容遭受損害或錯誤，將對業務產生重大影響，且可能導致暫時性業務中斷。	組織可以接受 4 小時(含)以上至1天內資產內容無法使用之情形。

價值	機密性(C)	完整性(I)	可用性(A)
5	資產內容屬機密，資訊揭露予非授權者將危及國家安全者。	資產內容遭受損害或錯誤，將對業務產生重大影響，且可能導致長時間嚴重的業務中斷。	組織可以接受 4 個小時(含)以內資產內容無法使用之情形。

(5). 人員類(PE)資訊資產價值評估表

價值	機密性(C)	完整性(I)	可用性(A)
1	人員負責之工作未涉及機密/敏感資訊者。	資產無此特性。	組織可以接受 5 個工作天(含)以上人員無法使用之情形。
2	人員作業過程中會使用機密/敏感資訊，洩漏後可能使組織安全或形象遭受輕微損害者。	人員技能不成熟或職務代理/交接不清楚，其產生之影響對業務之衝擊輕微，可迅速處理改正。	組織可以接受 3 個工作天(含)以上至 5 天內人員無法使用之情形。
3	人員作業過程中會使用機密/敏感資訊，洩漏後可能使組織安全或形象遭受明顯損害，且有權限下載大批資料者。	人員技能不成熟或職務代理/交接不清楚，將對業務產生明顯衝擊影響。	組織可以接受 1 個工作天(含)以上至 3 天內人員無法使用之情形。
4	人員負責組織機密資訊之管理工作，洩漏後將引起組織安全遭受重大的損失者。	人員技能不成熟或職務代理/交接不清楚，將對業務產生重大影響，且可能導致暫時性業務中斷。	組織可以接受 4 小時(含)以上至 1 天內人員無法使用之情形。
5	人員負責組織機密資訊之管理工作，資訊揭露予非授權者將危及國家安全者。	人員技能不成熟或職務代理/交接不清楚，將對業務產生重大影響，且可能導致長時間嚴重的業務中斷。	組織可以接受 4 個小時(含)以內人員無法使用之情形。

五、 資通系統防護需求分級

(一) 依據「資通安全責任等級分級辦法」之「附表九、資通系統防護需求分級原則」（如下表）執行資通系統分級。

(二) 本項資通系統係指軟體類之應用系統，其機密性、完整性及可用性價值評分 5 對應防護需求等級高，價值評分 3 及 4 對應防護需求等級中，價

值評分 1 及 2 對應防護需求等級普。

(三) 資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

(四) 資通系統防護等級評估完成後，應依其等級以「資通系統防護基準檢核表」執行控制措施。

防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

六、 資訊資產群組劃分

資訊資產管理者可考量資訊資產在特定條件下歸類為同一群組，以利進行風險評鑑作業。可依下列原則進行資訊資產群組歸類：

(一) 價值相同。

(二) 性質相同且數量較多。

(三) 存在於相同實體、邏輯環境。

(四) 遭遇弱點、威脅相同。

七、 資產編碼

(一) 將資訊資產五類給予代碼(資訊類 IF、軟體類 SW、實體類 HW、服務類 SE 及人員類 PE) 。

(二) 資訊資產編號之編碼方式，以 8 碼為原則。第 1~3 碼為系統代碼可以是全部數字、全部英文或英數字組合；如果為共用資訊資產請用 ALL 編碼為原則，第 4 碼為區隔線，第 5~6 碼為資產類別代碼，第 7 碼為區隔線，第 8～10 碼為資訊資產流水編號。(如 ALL-IF-001)

八、 資訊資產分級管控與標示

(一) 紙本文件須依內部公文相關規定辦理。

(二) 一般硬體資產，除依本院財產編號標籤原則辦理外，需依資訊資產編號辦理，並依下述資訊資產分級管控作業進行標示:

1. 敏感：以紅色標籤標示。
2. 內部使用：以藍色標籤標示。
3. 公開資訊：不標示。

九、 資訊資產之風險控管

各項資訊資產應依「風險評鑑作業說明書」之規定識別風險，並優先選擇重大風險進行處理以及控管。

十、 資訊資產使用與管理

(一) 敏感資訊於傳送及儲存時均需標示安全等級並予以加密保護。欲複製、攜出或查閱時，應提出申請載明申請用途，經業務單位主管核准後始得攜離或使用。

(二) 可攜式儲存媒體（磁帶、磁碟片、隨身碟、可攜式磁機、光碟……等）若儲存敏感資訊時需保存於加鎖之櫥櫃內。

(三) 資產(設備)攜出之安全管理

1. 電腦（包含伺服器主機、桌上型個人電腦、可攜式電腦）攜出外部使用時，應啟動系統個人防火牆功能，非必要應避免連結網路。
2. 電腦（含可攜式設備）借用攜出人員應負保管之責，妥善使用及保管。
3. 電腦（含可攜式設備）攜出使用不得任意安裝或下載軟體使用，應遵循本所相關資通安全管理規定。
4. 電腦（含可攜式設備）攜(借)出使用完畢歸還時，管理人員應視狀況進行防毒檢查，降低本所遭受攻擊的風險。

(四) 資訊類(IF)資產管理

資訊資產之保管人應負責資產保管、清點之責任。

(五) 軟體類(SW)資產管理

軟體資產之保管人應負責資產保管之責任，資產之清點由業務承辦人員負責。

(六) 實體類(HW)資產管理

1. 應標示設備名稱、用途及保管人；媒體資產應標示編號、內容及日期。
2. 實體資產之保管人應負責資產保管之責任，硬體故障維修與資產清點應由業務承辦人員負責。
3. 設備及媒體報廢或改為其他用途時，資產保管人與業務承辦人員應檢查其內容是否包含敏感資訊，或者是合法之軟體，務必確認其內容已被適當的處理後（格式化、刪除內容或實體銷毀），方可移交至相關人員後續處理。
4. 電腦機房安全管理依「電腦機房安全管理作業說明書」之規定辦理。

(七) 人員類(PE)資產管理

人員類資產依「人員管理暨資通安全訓練作業說明書」及「委外安全管

理作業說明書」之規定辦理。

(八) 服務類(SE)資產管理

服務類資產依「委外安全管理作業說明書」之規定辦理。

十一、 資訊資產報廢

(一) 實體類及服務類資產報廢

1. 實體類及服務類資訊資產需移作他用時，其相關設定與儲存媒體的資料必須清除。
2. 實體類及服務類資產報廢時，資訊資產使用單位應申請(如：公文)，經審核後即可進行資訊資產報廢程序。可重複使用之資料儲存媒體，於不再繼續使用時，應將儲存之內容完全消除。
3. 實體類及服務類資產價值為 4 者，經呈報召集人核准後，方可執行報廢；資訊資產價值未達 4 者，經權責主管核准後，方可執行報廢。
4. 資產保管單位依據審核之結果，辦理更新「資訊資產清冊」。
5. 當儲存媒類須報廢或再利用時，應採用以下任一種措施進行銷毀：
    a. 清除硬碟資料
    b. 利用消磁機或專業資料清除軟體工具，清除硬碟資料。
    c. 光碟一律將反光層抹除或折斷銷毀。
    d. 磁帶或磁片應以工具破壞實體，使其無法使用。
    e. 內含「敏感」等級(含)以上資料的儲存媒體，嚴格禁止僅使用一般格式化方式進行資訊資產報廢程序，應採用上述方式進行銷毀。

(二) 軟體資產報廢

1. 軟體資產需報廢時，資訊資產使用單位應申請(如：公文)，經審核後，方可進行報廢程序。

2. 軟體之資訊資產價值為 4 者，經呈報召集人核准後，方可執行移除；資訊資產價值未達 4 者，經權責主管核准後，方可執行移除。
3. 資訊資產保管單位依審核後之結果辦理更新「資訊資產清冊」。

(三) 資訊類資產報廢

1. 資訊安全管理制度相關文件廢止時，依照【B330--I301 文件控管作業說明書】辦理。
2. 其餘資訊類資產報廢時，使用單位應申請(如：公文)，經審核後，由資訊資產保管單位辦理更新「資訊資產清冊」。
3. 「內部」等級以上文件須以碎紙機進行銷毀，並刪除電子檔，該單位之主管人員應善盡督導之責。
4. 資訊類資訊資產價值為 4 者，經呈報召集人核准後，方可執行報廢；資訊資產價值未達 4 者，經權責主管核准後，方可執行報廢。

十二、 組態管理

本所組態管理範圍係為確保與資訊系統相關聯之硬體、軟體、系統及網路於所要求安全設定下正常運行，且組態未遭未經授權或不正確變更而更改：

(一) 建立組態樣本及組態清單文件化

應定義和實施流程及工具，以軟硬體、網路、新安裝之系統與設備以及運作中的系統於其生命週期內執行定義好的組態(含安全組態)並將安全組態填寫於「B330-I305-02 組態管理清單」；有關系統類別參照「資通系統防護基準檢核表範本」之組態設定。

(二) 組態審查

應定期檢視適用範圍內之安全組態基準之合適性，以確保安全組態基準能符合下列其一標準：內規標準、國際標準、行業標準、監管機構或其他標準要求。

(三) 組態設定及變更

若無法遵循安全組態基準，欲變更或不採納特定基準，應說明變更或

不採納之理由，有必要時應提出補償性控制措施，並與系統支援相關單位討論，討論結果應經相關單位主管核閱並同意後方能異動安全組態基準之內容。

組態變更作業執行後，系統管理人員、網路設備管理人員及資料庫管理人員應確認系統運行的情況，並持續針對系統組態進行監控，於異常狀況時進行因應。

(四) 系統設備組態現況與標準組態差異比對審查作業，應定期檢視，並記錄審查結果，就差異狀況根據變更流程進行修正。

十三、 預防資料洩漏

(一) 預防敏感性資料與具個人隱私資料(Personally Identifiable Information,PII)的資料於處理、傳輸與儲存時，應謹慎管制，降低非經授權的存取或誤用。

(二) 敏感性與具 PII 資料以資訊資產清冊進行盤點，有新增或異動須提報主管審核通過並加密儲存處理後，方可進行相關操作。

十四、 對外伺服器管理

(一) 應將對外伺服器納入管理，並確實建立、維護及定期更新盤點資料，藉由 IP 管理系統每季弱點掃描，ISMS 系統每年清查，建立相關機制。

(二) 盤點資料應足以識別對外資產(資訊所網路分區、對外服務專區)，並可合理說明其業務必要性及管理措施等狀態。

(三) 應定期辦理對外伺服器之管理檢視與安全維護，持續確認其運作情形、控制措施有效性及改善作業落實情況。

(四) 對外伺服器如有新增、異動、移轉或停用情形，應即時更新盤點資料。

陸、參考文件

一、 資通安全管理法及其子法

二、 B330-I306 風險評鑑作業說明書

三、 B330-I301 文件控管作業說明書

四、 B330-I304 人員管理暨資通安全訓練作業說明書

五、 B330-I313 電腦機房安全管理作業說明書

六、 B330-I314 委外安全管理作業說明書

柒、使用表單

一、 資訊資產清冊(系統)

二、 B330-I305-02 組態管理清單

三、 資通系統防護基準檢核表範本