文件編號	NCHU-ISMS-B-004	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	4.1	發行日期	113.09.23

國立中興大學
National Chung Hsing University

資訊資產管理辦法

機密等級:一般

文件編號:**NCHU -ISMS-B-004**

版　次:**4.1**

初版日期:**96.12.13**

文件制修訂紀錄			
修訂日期	修訂人員	修訂內容摘要	版次
96.12.13	陳建平	初版發行	1.0
98.07.07	陳建平	依據教育體系資通安全管理規範修訂相關資產分級、分類	1.1
98.8.18	陳建平	文件版型調整	2.0
98.12.22	陳建平	5.14.2實體標示內容修改	2.1

文件編號	NCHU-ISMS-B-004	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	4.1	發行日期	113.09.23

文件制修訂紀錄			
修訂日期	修訂人員	修訂內容摘要	版次
105.05.01	葉宏	修訂文件編號 文件名稱刪除「計算機及資訊網路中心」 修訂1.目的 改為本校 修訂2. 適用範圍 改為全校 修訂4. 權責 修訂5.2. 資產清冊5.3. 資訊資產擁有者負責事項 5.4. 資訊資產之價值鑑別與風險控管5.5. 資產之可被接受的使用 5.6. 資訊資產歸還 5.7. 資訊資產的分級原則5.8. 資訊資產的分級標準 5.9. 資訊資產分類原則5.10. 資訊標示 5.11. 資訊資產處置5.12. 可移除式媒體的管理5.13. 設備與媒體的汰除或再使用5.14. 傳輸中的實體媒體 修訂6.參考文件	3.0
109.07.13	王心嵐	增加參考文件「資訊資產控管方式說明表」和「資訊資產分級說明表」5.8增列參看「資訊資產分級說明表」,5.10.1「控管方式說明表」參考NCHU-ISMS-D-015表單	3.1
111.01.11	賴怡君	配合教育體系資安規範進行修訂，並廢止NCHU-ISMS-D-015資訊資產控管方式說明表。	4.0
113.09.23	張博凱	修訂資產類別將文件類與資料類合併，統一認定為資料類	4.1

文件編號	NCHU-ISMS-B-004	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	一般
版　本	4.1	發行日期	113.09.23

文件編號	NCHU-ISMS-B-004	文件類別	資訊安全管理系統
權責單位	計算機及資訊網路中心	文件密等	限閱
版　本	4.1	發行日期	113.09.23

1. 目的

訂定資訊資產分類與分級之原則並規範各類資訊資產之管理方式, 以保護國立中興大學(以下簡稱本校)各類資訊資產, 避免因人為疏失、蓄意或自然災害等風險所造成之傷害。

2. 適用範圍

適用於本校資訊安全與個人資料管理系統涉及之所有資訊資產。

3. 名詞定義

3.1. 資訊資產擁有者

具資訊資產所有權之單位或資訊資產管理授權之決策人員。

3.2. 資訊資產管理者

由資訊資產擁有者授權取得管理之責, 具資訊資產存取控管的權限。

3.3. 資訊資產使用者

從資訊資產管理者取得資訊資產之使用權, 以實際或邏輯方式使用該項資訊資產之人員。

4. 權責

4.1. 資訊資產擁有者

規劃資訊資產分類與分級方式, 並指派資訊資產管理者。

4.2. 資訊資產管理者

對保管之資訊資產進行資產評估、維護管理, 並規劃及執行適當的控制措施。

4.3. 資訊資產使用者

對於被授權使用之資訊資產, 應依各項安全程序, 正確使用及操作。

4.4. 單位主管

4.4.1. 負責指派專人維護資訊資產清冊。

4.4.2. 負責監督資訊資產分類、分級執行與管理。

5. 要求事項

5.1. 資訊處理設施的授權過程應制定安全控管

5.1.1. 各項資訊資產僅經授權人員始得使用。

5.1.2. 各資訊系統或相關設備之新增、異動或使用須經過授權程序, 並制定相關規定以維護其安全, 依據資訊資產管理要求辦理。

5.1.3. 各項資訊資產執行軟體或硬體變更時, 應檢查其與系統的相容性。

5.1.4. 使用個人的或私人擁有的資訊處理設施時, 應依據「資訊作業管理辦法」辦理。

5.2. 資產清冊

5.2.1. 「資訊資產清冊」之維護事宜由各單位資訊資產管理者負責並保管。

5.2.2. 各資訊資產管理者應視需要隨時更新「資訊資產清冊」或依據「資訊安全執行分組」訂定覆核時機，作為「資訊資產清冊」維護檢查時機。

5.2.3. 資訊設備於完成驗收時，須依據資訊資產管理要求之規定登錄資訊資產清冊，並由權責主管指派管理者。

5.2.4. 資訊資產報廢作業完成後，應即時更新「資訊資產清冊」。

5.3. 資訊資產擁有者負責事項

5.3.1. 本校各資訊資產應識別其資訊資產擁有者與管理者。

5.3.2. 資訊資產擁有者應確保與資訊處理設施相關的資訊資產加以適切的分類分級，並界定與定期審查資訊資產機密等級與存取限制，以及考量可適用的存取控制政策。

5.4. 資訊資產之價值鑑別與風險控管

5.4.1. 組織依據「資訊安全風險評鑑與管理辦法」執行各資訊資產價值鑑別。

5.4.2. 各資訊資產應識別其風險，並優先選擇重大風險進行處理，依據「資訊安全風險評鑑與管理辦法」辦理。

5.5. 資產之可被接受的使用

5.5.1. 資訊資產存取權限應遵循「資訊安全存取管理辦法」要求。

5.5.2. 本校所有員工、承包者與第三方使用者應遵循「資訊資產管理辦法」與「資訊作業管理辦法」對資訊資產之使用要求。

5.6. 資訊資產歸還

員工離職時除依本校人事相關法規辦理各項離職相關事宜外，亦須依據本校之「資訊資產管理辦法」歸還使用之資產。

5.7. 資訊資產的分級原則

5.7.1. 組織於進行資訊分級時應考量資訊的分類與相關的保護性控制措施，宜考量對分享或限制資訊的各項營運需求，以及該等需求相關的各項營運衝擊。

5.7.2. 防護需求等級應分析所考量資訊的機密性、完整性、可用性及法律遵循性與其他要求。

5.7.3. 資產擁有者宜負責定義資產的分類、定期審查、確保其隨時更新且處於適切等級。

5.8. 資訊資產的分級標準

依資訊之特性與實際需要進行資訊資產安全分級。各類資訊資產之分級為:機敏、限閱、一般。

5.8.1. 機敏

1. 含機密或敏感資訊，僅提供少數相關業務承辦人員及其權責

單位主管，或被授權之單位及人員使用。

2. 發生資通安全事件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。
3. 資訊資產存取權限原則須經由高階主管核准同意。

5.8.2. 限閱

1. 僅供組織內部人員或被授權之外部單位使用。
2. 發生資通安全事件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。
3. 資訊資產存取權限原則須經由權責單位主管核准同意。

5.8.3. 一般

1. 為一般性資料可對外公開，原則須遵守相關發布流程。
2. 發生資通安全事件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。
3. 資訊資產存取權限只須經由資訊資產管理者同意。

5.8.4. 資訊資產之分級應定期審核，視實需要予以調整及修正，以符合本校需求。

5.8.5. 不同等級之資訊資產合併使用或處理時，應以其中最高之等級為其分級。

5.9. 資訊資產分類原則

資訊資產依其性質不同，分為6類：人員、軟體、通訊、硬體、資料、環境。

5.9.1. 人員（People / PE）：包含全體同仁，以及委外廠商。

5.9.2. 軟體（Software / SW）：資通系統、作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。

5.9.3. 通訊（Communication / CM）：網路設備、網路安全設備、提供資訊傳輸、交換之線路或服務。

5.9.4. 硬體（Hardware / HW）：主機設備、硬體設施、可攜式設備及資通系統相關之設備等。

5.9.5. 資料（Data (Document) / DA）：以紙本形式存在之文書資料、報表等相關資訊或數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄、公文、列印之報表、表單、計畫文件及歸檔資訊等。

5.9.6. 環境（Environment / EV）：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

5.10. 資訊標示

5.10.1. 資訊的標示應涵蓋實體與電子格式的資訊資產。

5.10.2. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。

5.11. 資訊資產處置

5.11.1. 針對不同等級的資訊類資訊資產, 建立適當的資訊控管程序, 以確保資訊資產受到適當等級之保護。

5.11.2. 機敏

1. 電子傳送:
   (1) 處理資料及文件, 若其適用其他相關法規限制不得以電子方式傳送, 從其規定。
   (2) 以電子檔傳送時應加密;電子媒體遞送時應加密後再進行密封處理。
2. 實體資訊資產遞送:
   (1) 內部傳遞應以親送方式進行, 外部傳遞則應以親送或掛號方式寄送。
   (2) 機密文書須密封按人工傳遞方式, 可參考「文書處理手冊」之規定辦理。
3. 儲存:
   任何型式儲存均須置於上鎖區域保管, 並設有存取控制。
4. 銷毀:
   (1) 紙本型態:以碎紙機銷毀。
   (2) 電子檔案:刪除並清除暫存區。
   (3) 電子媒體:進行低階格式化或實體破壞。

5.11.3. 限閱

1. 電子傳送:
   以電子檔傳送時應加密;電子媒體遞送時應加密後再進行密封處理。
2. 實體資訊資產遞送:不予以限制。
3. 儲存:
   以任何型式儲存均須置於上鎖區域保管, 並設有存取控制。
4. 銷毀:
   (1) 紙本型態:以碎紙機銷毀。
   (2) 電子檔案:刪除並清除暫存區。
   (3) 電子媒體:進行低階格式化或實體破壞。

5.11.4. 一般

1. 電子傳送、實體資訊資產遞送、儲存:不予以限制。
2. 銷毀:
   (1) 紙本型態:以碎紙機銷毀。
   (2) 電子檔案:刪除並清除暫存區。
   (3) 電子媒體:進行低階格式化或實體破壞。

5.11.5. 資料保存期限宜依資料型態及法定保存期限之規定擬定。

5.12. 可移除式設備與媒體的管理

5.12.1. 可攜式設備與媒體管理

1. 使用可攜式設備與媒體時, 應謹慎防範資訊洩漏或妨害組織利益等情節發生, 資料攜入或攜出, 主管應盡控管之責, 提醒使用人員自我要求。
2. 將「機密」或「限閱」等級之資訊資產存放於可攜式設備與媒體時, 應採取適當加密處理或保護措施, 避免遺失時洩漏資訊。

5.12.2. 本校可攜式設備與媒體管理

1. 本校可攜式設備僅限於公務使用, 禁止使用於非法用途。
2. 禁止安裝使用非法與未經核准之軟體、非業務需用之套裝軟體或應用軟體, 經察覺後一律刪除, 並呈報權責單位主管。
3. 可攜式電腦應確實按規定安裝防毒軟體, 並定期檢查作業系統修正程式與更新病毒碼為最新版本。
4. 可攜式設備與媒體遺失時應通報權責主管, 並評估資料遺失是否具有機敏性, 依情節之重大程度決定是否向上呈報。

5.12.3. 非本校可攜式設備與媒體管理

1. 私人可攜式設備與媒體, 應評估風險後方可存取公務資料。
2. 單位主管或業務承辦人員應審慎評估外部人員於本校機敏、限閱等級資訊資產儲存區域使用可攜式設備與媒體使用需求之必要性, 如使用須符合單位管理機制或由單位主管允許, 若申請者違反使用規範, 本校將採取適當行為(如:列為禁止往來名單或是要求廠商更換人員)。
3. 外部人員使用可攜式設備連接內部網路, 依據「資訊安全存取管理辦法」辦理。
4. 使用外來的可攜式媒體, 主機應確認安裝防毒軟體, 以避免電腦、系統與網路受到病毒威脅。
5. 未經授權核可, 禁止以設備及媒體執行網路偵測、弱點掃描、封包收集分析等高危險性軟體。

5.13. 媒體的汰除

5.13.1. 含有機敏資訊的媒體(包含內建於硬體及通訊資訊資產）宜安全地汰除, 例如:燒毀或撕碎, 或清除資料後由施行單位內其他應用系統使用。

5.13.2. 宜備妥程序以識別可能需要安全汰除的項目。

5.13.3. 許多施行單位提供媒體的收集和汰除服務;宜謹慎選擇有適切控制措施和經驗的合適外部團體。

5.13.4. 機敏資訊的汰除應予存錄, 填報「銷毀記錄表」, 以利事後查詢與稽核。

6. 參考文件

6.1. 資訊安全組織管理辦法。
6.2. 資訊安全風險評鑑與管理辦法。
6.3. 資訊資產清冊。
6.4. 銷毀記錄表