德明財經科技大學

資訊資產管理規定

機密等級：一般

文件編號：Takming-ISMS-B-004

版　次：V 1.3

初版日期：107.12.25

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	107.12.25	N/A	執行小組	初版
1.1	109.02.04	2，3，4	執行小組	修改資訊資產的分級標準為”機密”、”限制使用”、”內部使用”及”一般”
1.2	112.10.13	3	執行小組	修改資訊資產編號方式
1.3	114.01.28		推動小組	資訊安全改資通安全，執行小組改推動小組，資訊資產編號方式修改

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，以保護德明財經科技大學(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

適用於本校資通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

具本校資訊資產之所有權，並為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價、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. 各項資訊設備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. 各項資訊設備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「資訊作業管理規定」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指定專人負責並保管。

5.2.2. 各作業流程負責人應視需要隨時更新「資訊資產清冊」或依據

「資通安全推動小組」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。

5.3. 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「資通安全風險評鑑與管理規定」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「資通安全風險評鑑與管理規定」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「資通安全存取管理規定」要求。

5.5.2. 本校所有員工、承包者與第三方使用者應遵循「資訊資產管理規定」與「資訊作業管理規定」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「資訊資產管理規定」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. 保護等級應分析所考量資訊的機密性、完整性及可用性與其他要求。

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

依資訊資產之特性與實際需要進行資訊資產分級，分級原則依資訊資產的影響程度分級如下：

5.8.1. 機密

嚴重影響本校運作，造成運作停擺、聲譽嚴重受損或造成財務大量損失。

5.8.2. 限制使用

影響本校運作，但尚能部分持續運作，僅部分作業造成停擺或可能造成部分聲譽受損或財務損失。

5.8.3. 內部使用

若外洩可能造成個人、單位、本校困擾或有助外界取得不當利益。

5.8.4. 一般

可公開予大眾之資訊，不會造成輕微的聲譽受損或財務損失。

5.9. 資訊資產分類原則

資訊資產依其性質不同，分為 7 類：人員、文件、軟體、通訊、硬體、資料、環境。

5.9.1. 人員（People / PE）：包含全體同仁。

5.9.2. 文件（Document / DC）：以紙本形式存在之文書資料、報表等相關資訊，包含表單、計畫等紙本文件。

5.9.3. 軟體（Software / SW）：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。

5.9.4. 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。

5.9.5. 硬體（Hardware / HW）：主機設備等相關硬體設施。

5.9.6. 資料（Data / DA）：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。

5.9.7. 環境（Environment / EV）：相關基礎設施及服務，包含實體機房、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. 紙本文件須依資訊資產分級進行控管；一般硬體資產標示於硬體外觀以供區別。

5.10.3. 實體標示說明如下：

5.10.3.1. 機密(資產價值 4)為紅色標籤。

5.10.3.2. 限制使用(資產價值 3)為黃色標籤。

5.10.3.3. 內部使用(資產價值 2)為綠色標籤。

5.10.3.4. 一般(資產價值 1)無需標示。

5.10.4. 資訊資產編號

5.10.4.1. 由單位編號、資產分類、序號，3 部分組成：

5.10.4.1.1. 單位編號：使用單位主管分機號碼 4 碼。

5.10.4.1.2. 資產分類：如 5.9 所標示的分類英文縮寫 2 碼。

5.10.4.1.3. 序號：順序流水號。

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。

5.11.1.1. 機密

(1) 僅限業務執行人員與其主管，以及經主管授權之人員進行存取或複製。
(2) 以電子檔或電子媒體或紙本進行傳送時須加密或密封處理。
(3) 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。
(4) 以任何型式儲存均須置於上鎖區域保管，並設有存取控制。
(5) 銷毀時，紙本須以碎紙機銷毀；電子檔須刪除並清除暫存區；電子媒體需進行低階格式化或實體破壞。

5.11.1.2. 限制使用

(1) 僅限業務執行單位人員，以及經單位主管授權之人員進行存取或複製。
(2) 以電子檔或電子媒體或紙本進行傳送時須加密或密封處理。
(3) 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) 銷毀時，紙本須以碎紙機銷毀；電子檔須刪除並清除暫存區；電子媒體需進行低階格式化或實體破壞。

5.11.1.3. 內部使用

(1) 僅限本校內部人員，以及經單位主管授權之外部人員進行存取或複製。
(2) 以任何型式儲存均須置於上鎖區域保管，並設有存取控制。
(3) 銷毀時，紙本須以碎紙機銷毀；電子檔須刪除並清除暫存區。

5.11.1.4. 一般

資產擁有者規定，並以不違反組織作業程序與法令、法規為原則。

5.11.2. 若發生機密外洩情事，除追查各相關人員之責任外，各相關人員與該外洩資訊之負責人得依組織相關條文予以處分，依據「人力資源安全管理規定」辦理。

5.12. 可移除式媒體的管理

5.12.1. 可攜式設備與媒體管理

5.12.1.1. 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。

5.12.1.2. 將機密資料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

5.12.2.1. 可攜式設備與媒體各單位自行採購，驗收完成後，由各單位或使用者妥善保管且負保管之責。

5.12.2.2. 單位內可攜式設備與媒體之互相借用時，借用人應負保管責任，不得將設備擅自轉借他人使用；借用完成後應刪除設備內之資料。

5.12.2.3. 本校可攜式設備僅限於公務使用，禁止使用於非法用途。

5.12.2.4. 個人專屬可攜式電腦使用時應謹防資訊外洩或是中毒。

5.12.2.5. 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。

5.12.2.6. 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。

5.12.2.7. 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密性，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

5.12.3.1. 私人可攜式設備與媒體，應評估風險後方可存取公務資料。

5.12.3.2. 權責單位主管或業務承辦人員應審慎評估外部人員於本校機房使用可攜式設備與媒體使用需求之必要性，如使用，須於進入前由權責單位主管允許，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）。處理內部使用等級以上資料工作區域（如：電腦機房），未經許可禁止使用相關設備進行拍攝或是螢幕畫面捕捉之行為，使用時需有工作區域管理人員在場陪同。

5.12.3.3. 外部人員使用可攜式電腦連接內部網路，依據「資通安全存取管理規定」辦理。

5.12.3.4. 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。

5.12.3.5. 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. 設備與媒體的汰除或再使用

5.13.1. 含有敏感性資訊的裝置宜實體銷毀，或宜以原始資訊將無法被擷取的技術毀損、刪除或覆寫資訊，而非僅使用標準的刪除或格式化功能。

5.13.2. 執行報廢作業必須是資訊資產超過折舊年限或損毀、故障，已不堪使用，或是已逾保存期限的紙本文件或表單。

5.13.3. 若屬未達耐用年限而提前報廢者，承辦人員應向部門主管提出申請核備，於核可後方得辦理報廢。

5.13.4. 資訊資產報廢時應由承辦人員上網填寫「資訊資產異動申請表」，交財產保管人覆核並呈主任許可後，移由學校總務處保管組辦理報廢事宜。

5.13.5. 主機、網路設備與儲存媒體報廢時，由承辦人員確認所報廢之資訊資產內之資訊是否已完全刪除或移除。

5.13.6. 資安作業之電腦報廢時，由使用單位確認所報廢之資訊資產內之資訊是否已完全刪除或移除，確認無誤後將需報廢之資訊資產轉至負責單位進行確認。

5.13.7. 實體類資訊資產若無殘值時，於主管確認無資安風險後，進行資源回收。

5.13.8. 含有機密級與限制存取資訊資產之儲存媒體必須消磁或利用工具清除資料，如無法進行時則進行實體破壞。報廢磁帶需進行燒毀，確保資料已被銷毀。紙本文件必須絞碎或採水銷處理或焚毀方式。

5.13.9. 資訊資產報廢作業完成後，應即時更新「資訊資產清冊」。

5.14. 傳輸中的實體媒體

5.14.1. 場域間資訊媒體的傳送宜使用可靠的運輸工具或遞送公司。

5.14.2. 資訊媒體的傳送應考量其機密等級，依據本辦法 5.11. 資訊資產處置要求辦理。

6. 參考文件

6.1. 資訊安全組織管理規定。

6.2. 資訊安全風險評鑑與管理規定。

6.3. 人力資源安全管理規定。

6.4. 資訊資產清冊。

6.5. 資訊資產異動申請表。

6.6. 資訊作業管理規定。

6.7. 資訊安全存取管理規定。