德明財經科技大學

資訊安全組織管理規定

機密等級：一般

文件編號：Takming-ISMS-B-001

版　次：V 1.2

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	108.09.11	1	執行小組	修改稽核小組成員產生方式
1.2	109.02.04	1	執行小組	增加”資訊安全官”
1.2	109.02.04	4	執行小組	增加教育訓練時數

1. 目的

為有效推動與辦理德明財經科技大學(以下簡稱本校)資訊安全之各項工作，特成立資訊安全組織，以擬定本校資訊安全發展之方向、策略及步驟，進而使資訊安全管理制度持續穩健的運作。

2. 適用範圍

適用於本校。

3. 名詞定義

無。

4. 權責

4.1. 電子計算機暨資訊安全諮詢委員會

4.1.1.依據「電子計算機暨資訊安全諮詢委員會設置要點」設置，由校長一人擔任資訊安全長(兼召集人)，建立資訊安全管理制度並推動資訊安全相關事宜。

4.2. 資訊安全執行小組

4.2.1.由電算中心主任擔任資訊安全官(兼召集人)，統籌本校各項資訊安全管理規定規劃事宜，執行小組成員由召集人選定之同仁組成。

4.2.2.負責召集資訊安全管理審查會議，並追蹤其決議事項。

4.2.3.督導風險評鑑作業。

4.2.4.督導營運持續計畫之修訂與演練。

4.3. 資訊安全稽核小組

由主任秘書擔任召集人，由本校內控稽核人員組成稽核小組，負責資訊安全稽核事宜。

4.4. 資訊安全執行分組

4.4.1.評估人員進用之安全性。

4.4.2.辦理資訊安全教育訓練。

4.4.3.資訊資產之安全需求研議、使用管理及保護等事項。

4.4.4.建立資訊安全管控措施監督機制。

4.5. 資訊安全稽核分組

4.5.1.執行資訊安全管理之內部稽核作業。

5. 要求事項

5.1. 建立資訊安全組織全景

5.1.1.應依據行政管理會議(如主管會報、行政會議或校務會議等)中有關資通訊安全需求決議事項，或上級機關來文要求事項進行評估，並據此建立或調整資通訊安全範圍與目標。

5.1.2.應依據決議事項確認與該事項有關之利害相關團體與其要求，並留存文件化紀錄。

5.1.3.上述事項之識別與分析應每年至少審查一次，或於組織重大變更、新業務時重新檢視，並供管理審查時評估管理系統及其適用範圍調整必要性。

5.2. 成立資訊安全組織

5.2.1.資訊安全組織架構

5.2.1.1.設置「電子計算機暨資訊安全諮詢委員會」，由校長一人擔任資訊安全長(兼召集人)；本會委員依據「德明財經科技大學電子計算機暨資訊安全諮詢委員會設置要點」委任。

5.2.1.2.「電子計算機暨資訊安全諮詢委員會」下設「資訊安全執行小組」及「資訊安全稽核小組」，另設立「資訊安全執行分組」與「資訊安全稽核分組」。

5.2.1.3.「資訊安全執行分組」成員由「資訊安全執行小組」召集人指派，負責統籌規劃各項資訊安全作業及相關教育訓練。若考量人力因素，得擬由外部人員協助辦理。

5.2.1.4.「資訊安全稽核分組」為任務編組，成員由「資訊安全稽核小組」召集人指派，負責評估資訊安全管理制度之落實與遵行情形。

5.2.1.5.「電子計算機暨資訊安全諮詢委員會」資訊安全組織成員職掌詳列於「德明財經科技大學電子計算機暨資訊安全諮詢委員會設置要點」。

5.2.2.職務權責區分

5.2.2.1.人員的職務須考量適當的權責區隔，基於業務上之需要，各項工作應訂定工作職務代理人，盡可能符合權責區隔之原則。

5.2.2.2.權責主管應指派人員擔任適當職務，並更新至網頁資訊。

5.3. 資訊安全組織工作職掌

5.3.1.電子計算機暨資訊安全諮詢委員會

5.3.1.1.依據「德明財經科技大學資訊安全政策」辦理。

5.3.2.資訊安全執行小組

5.3.2.1.資訊安全責任之分配及協調。

5.3.2.2.應採用之資訊安全技術、方法及程序之協調研議。

5.3.2.3.整體資訊安全措施之協調研議。

5.3.2.4.資訊安全政策之方向指導。

5.3.2.5.審查資訊資產風險評鑑報告。

5.3.2.6.資訊安全風險處理計畫之審查。

5.3.2.7.資訊安全稽核作業之指示，並覆核資訊安全稽核報告。

5.3.2.8.資訊安全管理制度矯正措施之審查。

5.3.2.9.核定與督導資訊安全管理制度之運作。

5.3.2.10.調查與處理重大資訊安全事件。

5.3.2.11.資訊安全管理制度績效之檢討。

5.3.2.12.審查業務營運持續計畫，並督導其執行。

5.3.2.13.審查資訊安全管理制度文件。

5.3.2.14.其他資訊安全管理相關事宜之決策。

5.3.3.資訊安全執行分組

5.3.3.1.依照「資訊安全執行小組」會議之決議，執行相關計劃。

5.3.3.2.建立資訊安全管控措施監督機制。

5.3.3.3.檢討資訊安全管理制度之變更管理、運作與成效。

5.3.3.4.檢核及追踪主機、應用系統、管制區域及網路存取權限及紀錄。

5.3.3.5.規劃資訊安全教育訓練及宣導事宜。

5.3.3.6.確認整體防毒措施機制運作正常並發佈病毒警訊。

5.3.3.7.協助建立網路安全及資料庫安全措施。

5.3.3.8.入侵偵測及異常事件之監控。

5.3.3.9.協助建立應用系統安全措施。

5.3.3.10.確認機房管制區域之實體安全機制運作正常。

5.3.3.11.處理資通安全事件通報事宜。

5.3.3.12.覆核資訊安全管理系統稽核報告。

5.3.3.13.於「資訊安全執行小組」管理審查會議，提報資訊安全管理系統執行績效與相關事項。

5.3.3.14.識別適用之法令。

5.3.4.資訊安全稽核分組

5.3.4.1.擬定稽核計劃。

5.3.4.2.執行稽核項目。

5.3.4.3.撰寫資訊安全稽核報告。

5.3.4.4.針對稽核結果提出建議。

5.3.4.5.追蹤改善方案之執行成果。

5.4. 保持與權責機關與特殊利害相關團體的聯繫

5.4.1.為確保資訊安全事件發生時，儘速執行事件處理，須與權責或外部單位隨時保持聯繫，例如：主管機關、資通安全會報、消防單位等...；並建立與組織資訊安全管理制度相關之「外部單位聯絡清單」。

5.4.2.應隨時與資訊安全技術相關團體維持聯繫，獲取資訊安全技術及產品資訊與知識，以及處理資訊安全事件或執行系統修補資訊等。並將資訊建立於「外部單位聯絡清單」。

5.5. 提供資源

5.5.1.依據「目標達成計畫與量測表」與管理審查會議之決議適當分配資源。

5.6. 維持組織內人員資訊安全能力與認知

5.6.1.人員資訊安全教育訓練

5.6.1.1.依所需職務之角色及業務內容，指派接受適當教育訓練、或具備證照或具有經驗人員，執行資通安全管理相關任務。每

年教育訓練累計時數：資訊安全人員 12 小時，資訊人員 6 小時，一般人員 3 小時。

5.6.1.2.如進行資訊安全教育訓練則可安排以下類別訓練，例：

資訊安全管理/技術課程。

資訊安全稽核訓練課程。

主管資訊安全課程。

5.6.1.3.應保存文件化資訊(如：如證書、證照、培訓紀錄等)，作為人員勝任之證據。

5.6.2.資安宣導

5.6.2.1.組織可利用內部網路系統（Intranet）、廣播、海報...等方式，隨時對組織員工公告資訊安全威脅、資安新聞、病毒最新情況與相關因應方式，以提升員工資訊安全意識。

5.6.3.依據「人力資源安全管理規定」辦理。

5.7. 運作之規劃及控制

5.7.1.各單位應依據管理制度各階文件的相關資訊安全程序與管控措施，以及「目標達成計畫與量測表」與「風險處理計畫表」內相關執行措施，進行資訊安全作業並應保存執行證據。

5.7.2.應確保各項委外執行作業，依據「資訊作業委外安全管理規定」進行控制與管理。

5.8. 監督、量測、分析及評估

5.8.1.資訊安全執行分組應針對已施行之常態性作業流程或控制措施建立監督機制，如機房管理、網路管理作業審查等。

5.8.2.資訊安全執行分組依據「目標達成計畫與量測表」，定期進行監督與量測，並以該量測結果做為評估資訊安全目標達成情形。

5.8.3.應每年檢視「目標達成計畫與量測表」之量測結果與執行情形，並檢討量測項目與目標水準是否需進行調整之必要，做成改善決議。

5.9. 資訊安全獨立審查—管理審查

5.9.1.「資訊安全執行小組」召集人應定期(每一年至少執行一次)召開管理審查會議，並將報告與決議事項於「電子計算機暨資訊安全諮詢委員會」進行報告(可配合組織內之主管會議同時進行)。本管理審查會議，討論事項如下：

(1)過往管理審查之議案的處理狀態；

(2)資通訊安全管理要求的變更，如上級機關要求、最高行政管理會議決議事項；

(3)管理目標與指標量測結果；

(4)內外部稽核結果；

(5)資安事故與不符合項目之矯正情形；

(6)風險評鑑結果及風險處理計畫執行進度；

(7)持續改善之機會。

5.9.2.管理審查決議事項應包含持續改善機會與管理制度變更需求之決議。

5.10. 資訊安全管理系統持續改善

5.10.1.資訊安全管理系統應持續改善管理制度的合宜性、適切性及有效性。

5.11. 法規遵循性

5.11.1.識別適用之法令

「資訊安全執行分組」應定期識別適用之法令，並彙整或修訂於「外來文件一覽表」。

5.11.2.智慧財產權

應要求員工遵守智慧財產權等相關法令，並依據軟體管理相關規定申請與使用軟體。

為確保員工均遵守智慧財產權，組織應於稽核時，稽核軟體使用情形。

5.11.3.個人資訊的資料保護與隱私

應要求員工遵守個人資料保護法、行政院所屬各機關資訊安全管理要點及相關規定。相關法令法規彙整於「外來文件一覽表」。

5.11.4.組織紀錄的保護

紀錄依紀錄型式(例如：變更紀錄、資料庫紀錄、錯誤日誌、稽核日誌和運作程序)進行分類，訂定保存期間和儲存媒體型式(例如：紙張、磁片、磁帶、硬碟或光碟片等儲存媒體)。並應依據資訊等級進行適當地處置與保護。

6. 參考文件

6.1. 資訊安全政策。

6.2. 文件暨紀錄管理規定。

6.3. 人力資源安全管理規定。

6.4. 資訊安全風險評鑑與管理規定。

6.5. 稽核管理規定。

6.6. 外部單位聯絡清單。

6.7. 資訊安全組織成員名冊。

6.8. 資訊安全組織架構圖。

6.9. 目標達成計畫與量測表。

6.10. 外來文件一覽表。

6.11. 風險處理計畫表。

6.12. 資訊作業委外安全管理規定。