文件編號：AS-02-001

文件名稱：資訊安全組織管理程序書

出 版 者：大葉大學-電算中心

機密等級：一般

使用本程序書前，請先至ISMS管理系統確認版次。

本文件歷次變更記錄：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版次 | 修訂日 | 修訂者 | 說 明 | 核准者 |
| V1.0 | 97/9/22 | 江國位 | 初版發行 | 吳清沂 |
| V1.1 | 97/10/21 | 江國位 | 新增6.2.10 | 吳清沂 |
| V1.2 | 97/11/07 | 江國位 | 新增資訊安全委員會之權責說明 | 林清同 |
| V1.3 | 97/11/24 | 江國位 | 修訂6.3管理審查輸入與輸出內容說明 | 林清同 |
| V1.4 | 100/10/04 | 江國位 | 新增6.1.1.4.5 | 張顧耀 |
| V2.0 | 103/10/09 | 江國位 | 新增6.1.1.3.3風險擁有者與風險評鑑結果之審議核定 | 張顧耀 |
| V2.1 | 103/12/11 | 江國位 | 修訂資安組織分工說明之人員能力資格認定，新增6.1.1.3.4、6.1.1.4.3、6.1.1.4.4、6.1.1.5.6、6.1.1.5.7、6.1.1.7.3 | 張顧耀 |
| V2.2 | 104/11/4 | 吳英傑 | 修訂6.3.2、6.3.3以符合ISO27001-2013版之內容 | 張顧耀 |
| V2.3 | 106/08/31 | 吳凰庭 | 1. 新增「6.3溝通程序」，以符合ISO27001:2013 7.3。 2. 新增「6.1.1.1.3」資安召集人負責事項；新增「6.1.1.2.8」資訊安全委員會負責事項；調整「6.1.1.3.2」，增加促進持續改進。以符合ISO 27001:2013 5.1。 | 張顧耀 |
| V2.4 | 107/10/18 | 吳凰庭 | 依據「ISO 27001:2013 A.06.01.03與權責機關之連繫」調整：   1. 新增6.1.1.8 權責機關。 2. 新增6.1.2填「資訊安全組織任務編組名單」。 3. 新增7.3資訊安全組織任務編組名單。 | 張顧耀 |
| V2.5 | 112/10/30 | 江怡慧 | 依教育部要求大專院校須全機關導入「ISMS」，進行修正資訊安全組織管理程序書之內容。 | 劉勇均 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

本程序書由資訊安全小組負責維護作業。

目 錄

[1 目的 1](#_Toc203633870)

[2 適用範圍 1](#_Toc203633871)

[3 權責 2](#_Toc203633872)

[4 參考資料 2](#_Toc203633873)

[5 定義 2](#_Toc203633874)

[6 作業程序 3](#_Toc203633875)

[7 相關文件 14](#_Toc203633876)

1. 目的
   1. 確保大葉大學（以下簡稱本校）資訊安全管理責任，以落實資訊安全政策之推動。
   2. 符合ISO27001標準下列控制目標：
      1. 錯誤日誌通報及確保矯正與預防措施之有效實施。
      2. 安全事件應循適當管理途徑儘快通報。
      3. 應要求資訊服務之使用者在注意到系統或服務有任何明顯、可疑安全弱點或威脅時進行通報。
      4. 資訊安全事件職責及處理程序。
      5. 從異常事件中學習檢討，落實預防管理目標。
      6. 搜集具有法律效用之證據，以供法律追究責任之佐證資料。
   3. 為確保本校內部資訊安全管理事項之推動，應建立適當資訊安全組織，以審核資訊安全政策、分配安全責任，並協調本單位資訊安全政策之實施。同時，建立與安全專家之聯繫，並在處理安全事件時諮詢專家之意見。
2. 適用範圍

本校資訊安全管理制度之建立、實施與控制等作業。

1. 權責

資訊安全組織負責本校資訊安全之維護與落實，權責範圍包括下列各項：

* 1. 資訊安全管理制度之審查。
  2. 資訊安全政策之研擬。
  3. 各組資訊安全事項權責分工之協調。
  4. 資訊資產面臨之風險監督。
  5. 應採用之資訊安全技術、方法及程序之協調研議。
  6. 資安事件之檢討及監督。
  7. 矯正預防措施之核准與監督。
  8. 其他重要資訊安全事項之協調研議。
  9. 辦理資訊安全教育訓練

1. 參考資料
   1. 大葉大學「資訊安全政策」
2. 定義

關鍵業務：指本校核心業務及相關資通系統。

1. 作業程序
   1. 資訊安全組織
      1. 資訊安全組織分工說明
         1. 資安召集人負責事項
            1. 資訊安全政策與目標之督導。
            2. 管理審查會議結果之督導。
            3. 支援其他相關管理角色在其職責範圍內展示他們的領導力。
         2. 資訊安全委員會負責事項
            1. 資訊安全/管理審查會議之參與成員由資訊安全長、一級行政單位主管、院級教學單位主管組成。
            2. 資訊安全管理事項之諮詢與協助。
            3. 資訊安全管理系統之建議。
            4. 資訊安全政策與目標之調整，並確認政策與目標一致性。
            5. 管理審查會議之督導。
            6. 資訊安全管理制度之推動。
            7. 協調應變資源之分配及使用。
            8. 傳達資訊安全管理有效實施、符合資訊安全管理系統要求的重要性。
         3. 資安代表負責事項
            1. 召開管理審查會議、資訊安全會議。
            2. 資訊安全管理制度相關事務之分配、協調、考核與督導，以促進持續改進。
            3. 風險擁有者與風險評鑑結果之審議核定。
            4. 資安成員資格、能力條件之規劃及審核。
         4. 資訊安全小組負責事項
            1. 制定與維護資安政策、資安目標與各項標準作業程序。
            2. 界定與檢討資訊安全管理制度之範圍與控制措施。
            3. 建立與維護業務持續營運計畫。
            4. 各項資安管理文件與記錄之建立與管制。
            5. 擬定資訊安全教育訓練計畫及辦理各項資訊安全相關的教育訓練活動。
            6. 制定風險管理制度，執行風險管理作業。
            7. 持續不斷的評估與檢討風險管理之具體成效。
            8. 建立資訊安全事件緊急應變暨復原措施。
            9. 監控、記錄與調查資訊安全事件。
            10. 受理資訊安全事件回報與事件處理。
            11. 執行「資訊安全小組」所決議之事項。
            12. 制定資訊安全內部稽核作業程序
            13. 擬定與執行資訊安全內部稽核計畫。
            14. 撰寫資訊安全稽核報告。
            15. 執行稽核改善建議事項，並追蹤缺失事項之執行情形。
            16. 執行矯正措施之改善。
            17. 評估與檢討資訊安全內部稽核成效。
            18. 研討新資訊安全產品或技術。
            19. 透過以下途徑執行相關資安情資蒐集、分析與分享：

* 數位發展部
* 內政部警政署165全民防騙網
* 國家資通安全研究院
* TWCERT/CC 台灣電腦網路危機處理暨協調中心
* 相關資網通硬軟體原廠公告或通知
* 防毒軟體廠商
* 媒體消息
  + - 1. 緊急處理組負責事項

緊急處理組為任務編組。由資訊安全長指派資安代表，召集業務相關人員若干名組成。相關權責及作業內容分述如下：

* + - * 1. 召集人：

由資安代表擔任之，當重大資安事件發生時，負責聯絡召集緊急處理組。

協調及督導各核心業務流程負責人執行作業，並協調資源之調派使用。

依據事故評估之結果，得依現況建請資通安全長決議是否宣布災變，以及是否啟動業務持續計畫。

當災變發生時，配合救災單位負責搶救人員、物資與設備等及現場指揮工作。

負責災後協調指揮清理災害現場。

負責規劃原作業場所之現場復原工作。

* + - * 1. 各核心業務流程負責人：

負責召集相關人員，發展、維護、更新修訂及執行各災害復原程序。

負責召集相關人員進行計畫之測試演練。

負責原作業場所或異地備援場所之應變、處理、復原及運轉測試工作。

負責災害現場證據收集，以利未來訴訟與損害求償事宜。

災害現場評估損害狀況及執行原作業場所之現場復原工作。

* + - 1. 權責機關

相關權責機關（如教育部、數位發展部）。

* + 1. 選派各項業務專精人員組建「資訊安全組織任務編組名單」。
  1. 控制程序
     1. 為確保對資訊安全措施有明確的方向，且得到管理階層的實際支援，應建立資訊安全組織，以合理的分配資訊安全責任和有效的資源管理，促進本校內部之資訊安全。
     2. 為明確保護資訊資產和執行其安全控管程序，應明確說明資訊安全責任及各管理人員所負責的範圍。
     3. 針對新的資訊處理設施，應適當制定管理授權程序。
     4. 為解決資訊安全的各種問題，應適當的詢問本校資訊安全委員會或其他專家，用以提昇本校內部人員資安之相關知識，達到最高的效率及最好的效果。
     5. 針對安全事件發生時，應迅速採取行動並應與執法機關、主管機關及往來廠商取得適當的聯絡管道，以保障本校之權益。
     6. 為確保本單位業務運作符合安全政策的要求，應適當對資訊安全政策的落實情況進行獨立審查。
     7. 為避免未經授權的存取資訊處理設備和資訊資產，應建立適當的存取控制程序。
     8. 為確保符合本校資訊安全政策，應與相關單位簽署適當的正式合約。
     9. 為確保符合本校之資訊安全政策，要嚴格控制第三方（委外支援廠商）對本校資訊處理設備的使用。
  2. 溝通程序

宣達本校資訊安全政策，組織目標及相關規定或校內涉及資訊安全需求，適時參與校內各項溝通會議。

* + 1. 內部溝通管道
       1. 參加人員

本校各單位主管、各業務承辦人員或相關同仁。

* + - 1. 溝通時機與頻率

透由校內舉辦之行政會議、校務會議、資訊委員會。如透由管理審查會議與視情況召開之資安會議，過程內容則須產出會議紀錄並經資安長審視後存查。

* + - 1. 溝通事項

涉及資訊安全之網路、系統、本校校務行政業務流程相關活動議題。

* + 1. 外部溝通管道
       1. 參加人員

與本校業務相關之主管機關、委外(維護)廠商，與本校業務關係或交流互動、具高度關聯或影響之對象。

* + - 1. 溝通時機與頻率

非迫切或法令法規要求事項，均由相關人員進行溝通，如需要時另合宜安排會議進行溝通。

* + - 1. 溝通事項

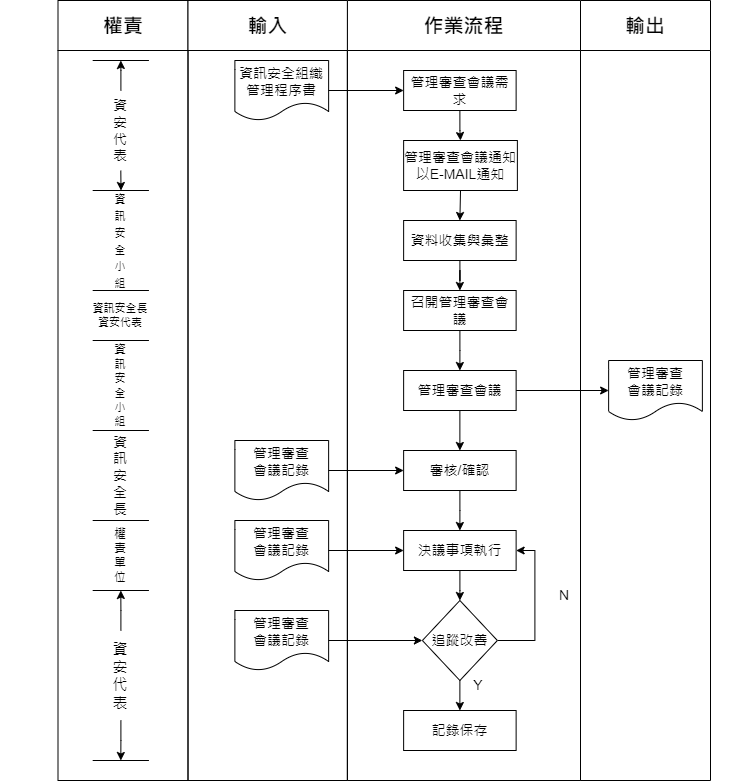
涉及資訊安全之網路、系統、本校校務行政業務流程相關活動議題。

* + 1. 內／外部溝通或傳達一覽表

|  |  |  |  |
| --- | --- | --- | --- |
| **溝通事項** | **溝通時機與頻率** | **參加人員** | **說明** |
| 資訊安全政策 | 每年 | 校內單位  校外單位  (含教育部)  委外廠商 | 1. 公開「資訊安全政策」於本校全球資訊網提供閱覽。 2. 舉辦「資訊安全及資安教育訓練」，於課程內容增加政策推廣並說明資訊安全管理系統之重要性與人員違反之可能後果。 |
| 資訊安全目標 | 每年 | 校內單位 | 報告「維運績效衡量統計表」，於管理審查會議檢討資安目標適切度及達成度。 |
| 資訊安全事故 | 每年 | 校內單位 | 於管理審查會議增加資安事故通報程序並說明「異常事件處理記錄單」。 |
| 理解組織及其環境 | 每年 | 校內單位  校外單位  (含教育部)  委外廠商 | 討論「資訊安全全景與範圍程序書」，於環境分析之適切性並記錄於「利害相關者與議題一覽表」。 |

* 1. 管理審查

為確保本單位矯正預防措施之有效運作，應落實管理審查機制，一年至少舉行一次管理審查會議，並確實討論下列議題：

* + 1. 管理審查會議應包括：
       1. 資訊安全政策。
       2. 風險評鑑及防護報告。
       3. 營運持續計畫及演練報告。
       4. 適用性聲明(SOA)。
       5. 資安事件處理報告。
       6. 稽核報告。
       7. 資源需求。
       8. 相關程序或活動執行紀錄。
    2. 管理審查會議討論項目：
       1. 過往管理審查之議案的處理狀態。
       2. 與ISMS有關之內部及外部議題的變更。
       3. 與資訊安全管理系統相關之關注方需求與期望的變化。
       4. 資訊安全績效之回饋。
       5. 關注方之回饋。
       6. 風險評鑑結果及風險處理計畫之狀態。
       7. 持續改善之機會。
    3. 管理審查會議結論應含括下列內容：
       1. 與持續改善機會有關之決策。
       2. 任何對ISMS變更之需要。
    4. 管理審查作業流程

1. 相關文件
   1. 會議通知單（表單編號：AS-04-013）
   2. 會議記錄（表單編號：AS-04-014）
   3. 資訊安全組織任務編組名單（表單編號：AS-04-032）