敏實科技大學

資訊安全手冊

機密等級：D

文件編號：ISMS-A-002

版　　次：1.1

發行日期：112.11.21

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	109.07.14			依據 ISO27001:2013 初版發行
1.1	112.11.21	全頁	劉得瑨	適用性範圍變更為全校

目錄

壹、 目的

確保敏實科技大學（以下簡稱本校）之校園系統開發、網路及教學支援等資訊業務運作符合資訊安全管理系統及法規之要求，並滿足相關於資訊安全之適用要求事項的承諾及持續改善資訊安全管理系統之承諾。

貳、 業務活動與關注各方之需求及期望

一、 本校主要業務活動：

為培育科技人才、推動研發創新、產學合作與社會服務。

二、 內、外部議題分析與管理

(一) 應決定與本校目標相關，並會影響達成資訊安全管理系統預定成果的外部與內部議題。

(二) 宜透過會議或問卷方式分析內、外部議題，並將分析結果以「會議紀錄」方式呈現，可探討之議題如下：

1. 外部議題：

(1) 與學校相關的法令、法規、契約新增與異動。

(2) 日常所接觸的資訊服務/系統（關鍵業務流程相關），是否有哪些問題。

(3) 可供學校借鑒之任何資訊安全事項。

(4) 與外部關注者之感知與價值有關聯。

2. 內部議題：

(1) 治理、組織結構、角色和責任。

(2) 政策、目標、及在不同階層實現這些目標的策略。能力、資源和知識方面的理解（如資金，時間，人員，流程，系統和技術）。

(3) 內部關注者、組織的文化、觀念和價值的關係。

(4) 資訊系統，資訊流和決策過程（包括正式和非正式的）。

(5) 被組織所採用的標準、指引和模型。

(6) 契約關係的形式和範圍。

3. 關注者分析與管理

(1) 組織應分析檢討與組織資訊安全相關的關注各方，作為要求與期望分析及內、外部議題討論時之參與對象，分析方式如下：

- 依據組織業務流程衝擊分析組織關鍵業務流程。
- 針對所分析之關鍵業務流程，分析其內、外部關注者。

(2) 組織應於每年組織全景分析作業時，邀請關注各方參與討論會議，不克參加者則以填寫議題問卷代之，以了解其對於本校資訊安全的要求與期望（包括法律、契約....等）以及內、外部之議題探討。

(3) 依據會議決議，作為組織擬定資訊安全範圍及後續風險與機會

評鑑之依據。

4. 擬定組織資訊安全範圍

(1) 活動間的介面及相依性分析

- 組織應於每年定期組織全景分析作業時，分析組織的各項活動，針對與其他組織相關的活動，分析該活動在組織內部與其他組織活動之間的介面及相依性，以作為組織擬定資訊安全範圍之依據。
- 組織應依據內、外部議題分析討論、關注者需求與期望討論會議之「會議紀錄」、及活動間的介面及相依性分析結果，分析並評估組織現有資訊安全管理範圍是否須調整，並於管理審查會議上報告分析結果，並取得管理階層之核准。

(三) 參考文件

1. 會議記錄

2. 會議簽到表

三、 確保法律與契約之遵循

為避免違反有關資訊安全之法律、法令、法規、契約義務、政策、標準或技術，以及任何安全要求本校採取：

(一) 識別適用之法律與契約的要求，加以明確界定維持最新文件化資訊

(二) 遵循與智慧財產權及專屬軟體產品使用相關法律、法令、法規或契約要求。

(三) 對合規性及營運要求之紀錄應予保護，免於遺失、毀損、偽造、未經授權存取及未經授權發佈。

(四) 對學校所有或受委託保有之個人資料應予保護以符合法令法規要求。

(五) 當有強制需求時應將機密資料以加密方式內部控制或傳輸。

(六) 對於資訊安全施行的相關要求定期審查。

四、 參考文件: 外來文件一覽表

參、 ISMS 適用範圍

一、 為確保敏實科技大學之資訊安全管理系統符合利害關係方之資訊安全期望，資訊安全實施範圍為：

適用敏實科技大學(以下簡稱本校)範圍涵蓋本校全部單位。

本校驗證範圍為綜合行政處電腦機房、所有核心資訊系統之維運。

二、 資訊安全管理系統(ISMS)提供本中心準備建立、運作、維護、改進 ISMS 的戰略決策。ISMS 的設計和措施受業務需求和目標、安全需求、應用的過程及學校的規模、結構而持續進行改善。

三、 ISMS 通過使用風險管理過程來保護資訊的保密性，完整性，可用性，給關注各方帶來信心並使風險得到充分管理。

肆、 政策與目標

一、 本校之資訊安全政策：

「強化人員認知、避免資料外洩
落實日常維運、確保服務可用。」

此政策之建立符合了

(一) 適合學校的目的;

(二) 為資訊安全目標提供框架;

(三) 滿足與資訊安全相關要求的承諾;

(四) ISMS 持續改進的承諾。

二、 資訊安全目標及其達成計畫

(一) 對 ISMS 相關功能和等級建立學校之資訊安全目標。

(二) 依資訊安全目標制定原則建立資訊安全目標:

1. 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
2. 保護本校業務活動資訊，避免未經授權的存取與修改，確保其正確完整。
3. 定期進行內部與不定期外部稽核，確保相關作業皆能確實落實。

4. 確保本校關鍵核心系統維持一定水準的系統可用性。

(三) 資訊安全目標及其達成計畫定期於管理審查會審查。

三、 此資訊安全政策與目標由最高管理者建立並正式宣告，除於網頁中揭櫫給關注各方外，並公告或張貼於本校明顯處，以提醒所有人員對資訊安全之警覺與責任。

四、 參考文件：資安政策

伍、 領導階層責任

一、 本校 **資訊安全長** 職務者為本中心資訊安全管理系統之最高管理者。對本管理系統負有:

(一) 有效運作與維持監督管理之責

(二) 對內及對外之溝通協調之窗口

(三) 定期向經營層報告實施成效

二、 最高管理者表現出對 ISMS 的領導階層責任：

(一) 確保資訊安全政策和資訊安全目標的制定，並與學校的策略方向相容;

(二) 確保 ISMS 的要求整合到學校的過程中;

(三) 確保 ISMS 所需要的資源;

(四) 達有效的資訊安全管理的重要性，並符合 ISMS 的要求;

(五) 確保 ISMS 達到其預期的效果;

(六) 指導和支持員工對 ISMS 作出有效的貢獻;

(七) 促進持續改進;

(八) 於相關管理角色在他們的職責範圍內全力支持以展示自己的領導力。

三、 職責與授權

最高管理者應確保與資訊安全相關角色的職責和權限的分配和溝通

。

最高管理者應指定 ISMS 組織相關人員職責與授權：

(一) 確保 ISMS 符合資訊安全要求;

(二) 將 ISMS 的績效報告給最高管理者。

四、 參考文件： 資訊安全組織程序書

陸、 文件化資訊

一、 資訊安全管理系統包括：

(一) 遵循資訊安全國際標準所需要的文件;

(二) 記錄 ISMS 有效性必要的紀錄。

二、 創建和更新

當創建和更新文件和紀錄時，應確保適當的：

(一) 識別與描述（如標題，日期，作者或參考號碼）;

(二) 格式（如語言，軟體版本，圖形）和媒體（如紙張，電子〉；

(三) 適用性和適切性的審查和批准。

三、 文件化資訊的控制

對資訊安全管理系統與 ISMS 國際標準要求的文件化資訊進行管理，以確保：

(一) 當文件化資訊被需要時是可用且適用的;

(二) 得到充分的保護（例如防止機密性喪失，不當使用或喪失完整性)。

(三) 分配，存取，檢索和使用;

(四) 存儲和保存，包括易讀性之保存;

(五) 控制變更（例如版本控制）;

(六) 保留和處置。

(七) 規劃和運作必要的外來文件化資訊，應被適當識別和管理。

四、 參考文件：

(一) 文件管理程序書

柒、 支持

一、 資源

學校應確定並提供 ISMS 的建立，措施，維護和持續改進所需的資源

。

二、 能力

學校應：

(一) 確定在 ISMS 管控下工作的員工，其所必備能力將影響學校的資訊安全績效；

(二) 確保這些人在適當的教育訓練或取得經驗後是能勝任的；

(三) 在適當情況下，採取行動以獲得必要的能力，並評估所採取行動的有效性；

適用的行動可能包括，例如： 提供訓練，指導，或重新分配現有雇員、主管人員的聘用或承包。

(四) 保留適當的文件化資訊作能力之證據。

三、 認知

應讓學校工作的人員應了解：

(一) 資訊安全政策；

(二) 他們對 ISMS 有效性的貢獻，包括提高資訊安全績效的收益；

(三) 不符合 ISMS 要求所帶來的影響。

四、 參考文件：

(一) 人員安全與教育訓練程序書

(二) 人員資訊安全守則

(三) 資訊安全組織章程

捌、 資訊業務之風險管理

資訊業務之風險管理業務由資安防護組執行。

學校於資訊安全風險評估過程中包含過程及結果應予以文件化並存檔保留，以保證風險評鑑之過程已依照計畫措施。

一、 規劃：風險評鑑為資訊安全管理規劃時首先須考量的議題。

(一) 處理風險和機會的行動

當規劃學校的 ISMS 時，考慮學校背景與關注各方之期望以確定需要解決的風險和機會。

(二) 資訊安全風險評鑑

資訊安全風險評鑑過程原則：

1. 建立準則:資訊安全風險評估過程須先建立和維護資訊安全風險的標準，包括風險接受準則; 決定執行的資訊安全風險評估的標準;
2. 衡量標準:確保重複使用資訊安全風險評估過程能產生一致的，有效的和可比較的結果。
3. 識別風險:包含資訊機密性，完整性和可用性的損失風險以及識別風險的所有者。

4. 分析風險：分析風險實現後潛在的後果、實現的可能性、確定風險等級。

5. 評估風險：比較風險分析結果與風險準則，並建立風險處理的優先順序。

(三) 資訊安全風險處理

資訊安全風險處理過程原則：

1. 考慮風險評估的結果，選擇適當的資訊安全風險處理方法；

2. 確定所選擇處理資訊安全風險的控制措施是必要的；

3. 確認適用性聲明書中的控制項，已包含所有必要的控制項；

4. 適用性聲明已包含適用及不適用之理由；

5. 制定資訊安全風險處置計畫；

6. 風險處置方案和殘餘風險得到風險所有人的批准。

二、 運行：風險管理為資訊安全管理運行時隨時依據實行現況予以變更

(一) 運行計畫及控制

1. 於規畫、實施與控制其過程需求以達成資訊安全要求，並且實施風險評鑑以及風險處理採行的計畫，以實現資訊安全目標。

2. 應控制計畫變更，同時審查非計畫的變更，並採取適當措施以減輕任何不良影響。

3. 確保外包過程是被確定和受控。

(二) 資訊安全風險評估

學校應於規畫的時間或發生重大變化時執行資訊安全風險評估中建立的風險評鑑的準則執行資訊風險評鑑。

(三) 資訊安全風險處理

學校應實作資訊安全風險處理計畫並保留處置結果的文件化資訊。

三、 參考文件：

(一) 風險評鑑與管理程序書

(二) 資訊安全組織程序書

(三) 資訊資產分類分級管理程序書

(四) 人員安全與教育訓練程序書

(五) 委外管理程序書

(六) 實體安全管理程序書

(七) 系統開發與維護程序書

(八) 存取控制管理程序書

(九) 網路通信管理程序書

(十) 資訊備份管理作業說明書

(十一) 安全事件管理程序書

(十二) 業務永續運作管理程序書

(十三) 適用性聲明書

玖、 績效評估

一、 監督、量測、分析與評估

(一) 學校評估資訊安全績效與 ISMS 的有效性時應確定：

1. 需要進行監督與測量，包括資訊安全過程和控制措施;
2. 監督、量測、分析與評估的方法，確保有效性的結果; 有效的方法應該可以產生可比較性和可再現性的結果。
3. 執行監督與量測時間;
4. 監督與量測的人員;
5. 監督與量測的結果進行分析和評估的時間;
6. 分析與評估這些結果的人員。

學校須保留監督和量測結果的文件化資訊作為證據。

(二) 對資訊安全的審查

1. 當發生重大變更時，獨立審查資訊安全的各項控制目標、控制措施、政策、過程及程序的作法與實作。
2. 管理人員定期審查相關責任範圍內之安全處置及程序已遵循安全政策、標準與其他的安全要求。
3. 定期對技術遵循審查以符合安全政策與標準

二、 內部稽核

內部稽核應

(一) 被規畫、建立、實作與維持一份稽核方案，其中包括

1. 頻率為二年一次，可依人力、時間安排分多梯次進行。
2. 其方法為合格稽核員採用稽核查檢表或使用資訊稽核工具執行。
3. 選擇稽核員和稽核組長以確保稽核過程的客觀性和公正;
4. 稽核員應完成稽核紀錄;稽核組長應制定稽核計畫、完成稽核報告與追蹤稽核發現的改善結果
5. 稽核程序應考慮相關過程和以往稽核結果的重要性;

(二) 定義每次稽核的章程和範圍;

(三) 確保稽核結果報告提交相關管理階層;

(四) 保留稽核程序和稽核結果相關的文件化資訊作證據。

(五) 根據稽核的結果可提供資訊安全管理資訊：

1. 遵循學校自訂的 ISMS 的要求; 或符合 ISMS 的國際標準的要求
2. 有效實作和維持。

三、 管理審查

最高管理者應一年一次審查學校的資訊安全管理系統以確保其持續的適用性、充分性和有效性。管理審查應考慮：

(一) 以往管理審查行動實施的狀態;

(二) 與 ISMS 相關的內外部問題的變化；

(三) 與 ISMS 相關關注方之需要及期望的變更。

(四) 資訊安全績效和趨勢的回饋，包括：

1. 不符合項目的矯正措施；
2. 監督和量測結果；
3. 稽核結果；
4. 資訊安全目標的實現；

(五) 關注各方的回饋；

(六) 風險評鑑的結果和風險處理的狀態；

(七) 持續改進的機會。

管理審查的輸出應包括持續改進的機會和任何 ISMS 需要變更的相關決定。

學校應保留管理審查結果的文件化資訊作為證據。

四、 參考文件：

(一) 資訊安全組織程序書

(二) 資訊安全稽核作業程序書

(三) 資訊安全管理審查會議紀錄

(四) 資訊安全政策

壹拾、 改進

一、 不符合及矯正措施

ISMS 出現不符合事項時，應採行措施並保留文件化資訊、作為證據。

(一) 對不符合事項作出反應，如適用：

1. 採取行動控制並矯正；
2. 處理結果；

(二) 評估採取措施的必要性，以消除不符合的原因，使不復發或不在其他地方發生，

1. 審查不符合；
2. 確定不符合的原因；
3. 確定是否存在類似的不符合和發生的可能；

(三) 實作所需的任何措施；

(四) 審查已採取矯正措施的有效性；

(五) 如果有必要，進行變更以改進 ISMS。

(六) 不符合的性質和後續各項行動；

(七) 各項矯正措施的結果。

一、 持續改進

應不斷提高 ISMS 的合宜性、適切性和有效性。

二、 參考文件：

矯正及預防管理程序