目　　錄

1　目的 1
2　適用範圍 1
3　定義 1
4　本校資訊安全政策 2
5　管理目標 2
6　資訊安全組織 5
7　資訊資產分類、等級及評鑑原則 7
8　不可接受風險等級 7
9　有效性量測 7
10　適用性聲明書 8
11　審查 8
12　實施 8
13　附件 8

環球科技大學

文件名稱	資訊安全管理政策	版本	5.1
文件編號	ISMS-01-001	發行日期	2016/11/23
		頁次	1 / 8

1 目的

為強化資訊安全管理，確保所屬之資訊資產(含資料庫中具有個人資料的資料庫)的機密性、完整性及可用性，以提供本校各業務持續運作環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

2 適用範圍

資訊安全涵蓋 14 項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資訊不當使用、洩漏、竄改、破壞等情事發生，對本校帶來各種可能之風險及危害。管理事項如下：

2.1 資訊安全政策訂定與評估。
2.2 資訊安全組織。
2.3 人力資源安全。
2.4 資產管理。
2.5 存取控制。
2.6 密碼學(加密控制)。
2.7 實體及環境安全。
2.8 運作安全。
2.9 通訊安全。
2.10 系統獲取、開發及維護。
2.11 供應者關係。
2.12 資訊安全事故管理。
2.13 營運持續管理之資訊安全層面。
2.14 遵循性。

3 定義

所謂資訊安全係將管理程序及安全防護技術應用於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體及經由列表機所列印之各式報表，以確保資訊蒐集、處理、傳送、儲存及流通之安全。

4 本校資訊安全政策

本校資訊安全政策為：

A：易用適用的功能(Available / Availability)

重要系統更新/上線前經測試。

重要系統開發或變更時應更新系統文件。

R：穩定可靠的品質(Reliable / Reliability)

定期監控網路重要伺服器執行作業之系統容量及網路資源使用率。

進行網路線路適當維護，避免網路斷線影響工時。

M：易修改易維護與易擴增的(Maintainable / Maintainability)

建立系統需求申請及修改之作業程序。

於系統建立時需考量未來使用狀況之容量可滿足要求。

S：安全可靠的服務(Service/Security)

惡意程式/行動碼適當管理與監控，避免影響學校正常運作。

帳號處理及密碼控制管理。

5 管理目標

維護本校資訊資產(含資料庫中具有個人資料的資料庫)之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

5.1 資訊安全管理政策：

5.1.1 資訊安全政策宣導次數。

5.1.2 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。

5.1.3 實施資訊安全內部稽核制度，每年至少稽核 1 或 2 次，確保資訊安全管理系統之落實執行。

5.2 標準制度管理組織：

5.2.1 員工確實簽署保密協議。

5.2.2 第三方確實簽署保密協議。

5.3 資訊資產安全管理：

5.3.1 資訊資產清冊定期、不定期更新。

5.3.2 資訊資產清冊符合分級與標示規定。

5.4 人力資源安全管理：

5.4.1 資訊安全受訓時數。

5.4.2 離職/異動/退休人員帳號確實變更/刪除。

5.4.3 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。

5.5 實體與環境安全管理：

5.5.1 遵守機房門禁規定。

5.5.2 消防器材與UPS 定期保養。

5.6 通訊與運作管理：

5.6.1 定期監控網路重要伺服器執行作業之系統容量（例如：CPU、RAM、硬碟）。

5.6.2 定期監控網路之網路資源使用率（例：如連外頻寬）。

5.6.3 惡意程式/行動碼適當管理與監控，避免影響學校正常運作。

5.6.4 暫存於公共區的電子資料，需於使用完畢後立即刪除。

5.6.5 辦公區域內禁止使用行動儲存媒體及燒錄光碟（除公用區及特定電腦外）。

5.6.6 進行網路線路適當維護，避免網路斷線影響工時。

5.6.7 定期檢查重要系統的鐘訊同步情況。

5.6.8 檢查防火牆設定是否與 Server 伺服主機服務開放申請表資料相符。

5.6.9 定期備份重要資料。

5.6.10 矯正措施於規定時間內改善完成。

5.6.11 系統公用程式應做好區隔，並移除所有不必要的公用程式和系統軟體。

5.6.12 重要核心系統設備應採複式配置，提高可用性。

5.6.13 資訊系統主機皆需經過適當的使用者登錄介面才可進入操作系統。

5.6.14 相關系統主機於連線時，應設定在閒置一段時間後，必須重新登入認證。

5.7 存取及密碼控制管理：

5.7.1 定期審查重要系統存取權限。

5.7.2 未經授權存取重要資料及機密性資料之次數。

5.7.3 保護本校業務活動資訊，避免未經授權的存取。

5.8 資訊系統取得、開發及維護安全管理：

5.8.1 重要系統更新/上線前經測試。

5.8.2 重要系統開發或變更時應更新系統文件。

5.8.3 重要系統、伺服器當機頻率。

5.8.4 進行資訊系統分類分級及鑑別作業。

5.9 供應商安全管理：

5.9.1 委外服務執行管理。

5.9.2 簽署保密協議。

5.9.3 針對供應商進行評鑑作業。

5.10 資訊安全事件管理：

5.10.1 發生資安事件影響工時。

5.10.2 資訊安全通報系統建立。

5.10.3 資訊安全事件紀錄的有效維持，透過資訊安全事件，來進行員工的機會教育。

5.11 資訊安全業務持續營運管理：

5.11.1 檢討營運持續計畫演練執行情形。

5.11.2 執行風險評鑑與營運衝擊分析。

5.11.3 保護本校業務活動資訊，避免未經授權的修改，確保其正確完整。

5.11.4 建立跨部門之資訊安全組織，制訂、推動、實施及評估改進資訊安全管理事項，確保本校具備可供業務持續運作之資訊環境。

5.12 相關法規遵循性：

5.12.1 本校之業務活動執行須符合相關法令或法規之要求。

5.12.2 合法軟體之安裝。

6 資訊安全組織

6.1 ISMS 專案小組由副校長擔任資安長、圖書資訊處圖資長擔任執行秘書，其下小組成員指派圖書資訊處同仁兼任之，負責資安各標準制度之建置、實施與維持，以統籌圖書資訊處之管理制度、資源調度等事項之協調及研議。

6.2 ISMS 專案小組下設有內部稽核組及相關任務小組，任務分配如下：

6.2.1 資安長負責事項：

- 召開與主持管理審查會議。
- 各管理制度之政策建置、修訂。
- 各系統之目標的核准與確保審查框架的建立。
- 各管理制度相關事務之資源取得、分配、協調與督導。

6.2.2 執行秘書負責事項：

- 執行秘書本身具有一切與資訊安全管理運作的監督權責，當資訊安全管理系統運作發生異常時賦有向高階管理階層直接提報權力，不受行政系統與外部影響。
- 協助召開管理審查會議、資訊安全會議。
- 依照本校資訊安全管理需求之規定，負責要求建立、執行、維護符合資訊安全管理活動的書面化程序。
- 督導資訊安全事務之分配與協調，包含資訊安全管理認證單位之聯繫窗口。
- 協助高階管理階層提升全校教職員對本校資訊安全要求、法令法規的認知。
- 透過內部稽核活動成果，負責將資訊安全管理實施成效，向管理階層報告，以作為系統改善依據。

6.2.3 內部稽核組負責事項：

- 資安稽核員：由執行秘書指派具有資訊安全稽核資格之人員，負責資訊安全稽核計畫規劃與執行之相關工作。
- 資訊安全管理系統每年至少需進行一次內部稽核工作，稽核員需報告稽核結果並追蹤改善事項。
  - 資安稽核的年度計畫
  - 資安稽核的當次計畫
  - 資安稽核的執行（稽核檢查表的製作）
  - 資安稽核報告的整理
  - 資安稽核缺失的改善確認追溯

6.2.4 制度規範組負責事項：

- 負責資訊安全管理制度相關程序文件之建立、實施及維持。
- 相關法令、法規遵循之界定與更新。
- 負責資訊安全之適用性聲明書之修訂。

6.2.5 文管中心：

- 由執行秘書指派專職人員負責圖書資訊處內 ISMS 文件之控管、維護及紀錄。

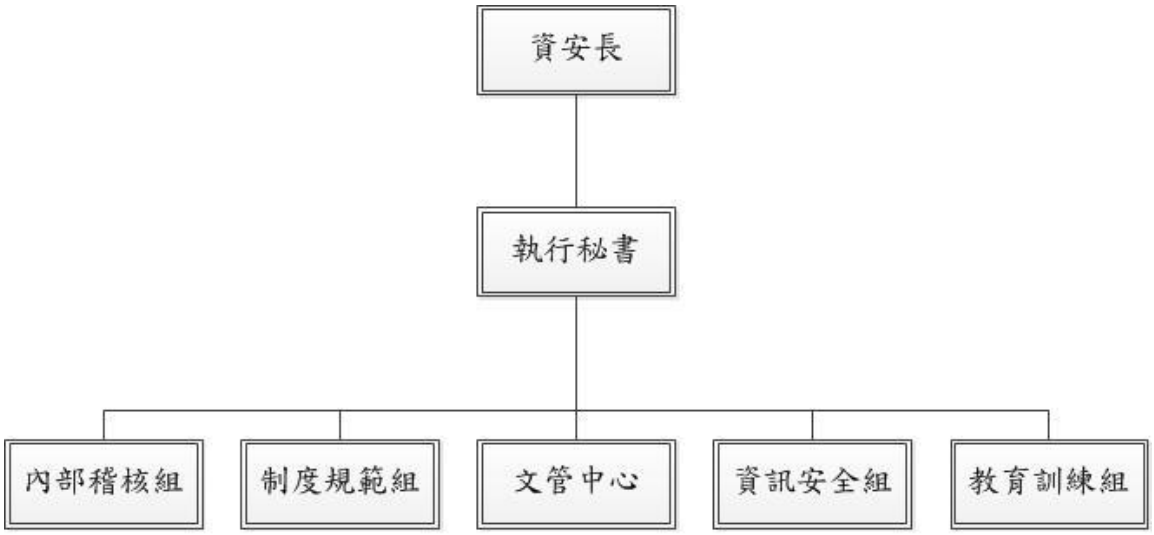
6.2.6 資訊安全組負責事項：

- 落實資訊安全管理系統於組織中各個階層。
- 負責資訊資產盤點/修訂、風險評估、風險處置、殘餘風險處理的策劃之全過程。
- 落實風險處置措施，確保風險處置措施的資源。
- 緊急應變通報、災害復原系統的規劃。
- 負責資訊與個資安全事件之通報與事故緊急應變處理事宜。
- 負責資訊與個資安全事故之持續改進、矯正措施事宜。
- 負責營運持續計畫之制定、修訂與維護。
- 負責緊急應變及災害復原計畫之執行與維護。
- 網路、網站、機房及其他影響業務運作之資訊安全事件管理。

6.2.7 教育訓練組負責事項：

- 安排有關訓練計畫與本校具有的員工訓練計畫相結合
- 本校教育/訓練的事前安排
- 訓練需求的識別與整理
- 教育訓練行政作業的辦理
- 講師、學員的聯繫
- 教育訓練成效的確認
- 教育訓練的簽到與同仁的訓練履歷歸檔整理
- 教育成果的表現
- 特殊資格的管理

6.3 資訊安全組織圖：



7 資訊資產分類、等級及評鑑原則

7.1 分類

依據各項作業內容特性，將資產分為人員、資訊、軟／硬體、基礎設施及服務等 4 大類。

7.2 等級

依照各類資產所具有之機密性、完整性及可用性評估該資產反應出之價值。

7.3 評鑑

根據風險識別與分析，針對資訊資產本身之脆弱性、威脅及衝擊，評鑑其風險等級。經分級與評鑑後，依其所具備之價值，施以適當程度之安全控管。

8 不可接受風險等級

執行風險評鑑後，將資產區分為不同風險等級，其中屬於「不可接受風險」之資產，應訂定『風險控制計畫』據以監督控管，並落實執行追蹤控制。

9 有效性量測

ISMS 專案小組需制定及彙整資訊安全管理目標於「ISMS 有效性量測表」中，已確認資訊安全系統運作之有效性及符合性，並於每年管理審查前，審查及檢討其達成狀況，針對未達規劃之項目，由資訊安全組開立「矯正措施處理單」交權責單位執行矯正活動，並將 ISMS 有效性量測結果及改善作業提報於資訊安全管理審查會議作審查。

10 適用性聲明書

依據「教育體系資通安全暨個人資料管理規範」要求產出適用性聲明書，以書面方式列舉資訊資產是否適用其標準所列之控制措施，及其不適用之原因。當組織架構、人員、設備、實體環境等變動時，ISMS 專案小組應重新定義控制措施之適用性。

11 審查

本政策應每學年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保圖書資訊處營運持續及資訊安全實務作業與個資安全保護能力。

12 實施

12.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

12.2 本政策經資安長核定後實施，修訂時亦同。

13 附件

13.1 有效性量測表 (ISMS-04-049)

13.2 適用性聲明書 (ISMS-04-052)