東方設計大學

資訊安全政策

機密等級：一般

文件編號：ISMS-A-001

版　　次：2.0

發行日期：107.1.15

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日期	修訂頁次	修訂者	說　　明
1.0			資訊安全小組	初稿
2.0	106.12	封面、P3	資訊安全小組	變更校名

本程序書由資訊安全小組負責維護。

目錄：

1 目的

1.1 東方設計大學 (以下簡稱本校) 為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本校之資訊業務持續運作之資訊環境，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 範圍

2.1 資訊安全管理涵蓋 14 項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、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：

2.1.1 資訊安全政策訂定與評估。

2.1.2 資訊安全組織。

2.1.3 人力資源安全。

2.1.4 資產管理。

2.1.5 存取控制安全。

2.1.6 密碼安全。

2.1.7 實體與環境安全。

2.1.8 作業安全。

2.1.9 通訊安全。

2.1.10 系統獲取、開發與維護之安全。

2.1.11 供應者關係管理。

2.1.12 資訊安全事件之反應及處理。

2.1.13 營運持續運作管理。

2.1.14 相關法規與施行單位政策之符合性。

本校之內部人員、委外服務廠商與訪客皆應遵守本政策。

3 定義

3.1 資訊資產：係指為維持本校資訊業務正常運作之硬體、軟體、服務、文件及人員。

3.2 營運持續運作之資訊環境 : 係指為維持本校各項業務正常運作所需之電腦作業環境。

4 目標

4.1 透由利害關係者及與議題等要求事項，達成下列目標：

4.1.1 全景與範圍對應其重要業務流程之要求與維運持續。

4.1.2 執行資訊安全管理制度需達以下目標(資訊安全工作目標與計畫)：

4.1.2.1 維運之系統可用率每年達 95%。

4.1.2.2 電腦病毒造成系統、網路癱瘓無法作業與機密資訊外洩、破

壞、竄改之零事件。

4.1.2.3 發生3級以上重大資訊安全事件之次數,每年不得超過一次。

4.1.3 達成與資安政策一致之預期。

4.1.4 透過可量測的規範進行風險管理過程。

4.1.5 本校之業務活動執行須符合相關法令或法規之要求如下表;

內部議題	外部議題	利害相關者	利害相關者要求
組織政策、目標	主管機關要求	主管機關	各項法令、法規
	政府單位要求	政府單位	各項法令、法規
組織文化	N/A	內部人員	組織內部規範
相關資源需求（包括：人力、技術、預算等）	N/A	內部人員	訓練
		高階主管	績效（KPI）
	資訊安全事件 資訊技術	客戶	合約內容（SLA）
		供應商	合約內容
	ISO 國際標準	ISO 國際組織	ISO 27001
		第三方稽核單位	

4.2 組織欲達成目標需決定相關要點：

4.2.1 執行事項。

4.2.2 所需資源。

4.2.3 負責人員。

4.2.4 完成時間。

4.2.5 成果評估方式。

4.2.6 各項量測指標(目標與計畫)、所需資源、負責人員、達成時間及成果評估方式等資訊，請詳閱「ISMS 營運量測指標」。

5 責任

5.1 本校的管理階層建立及審查此政策。

5.2 透過適當的標準和程序以實施此政策。

5.3 所有人員和委外服務廠商均須依照相關安全管理程序以維護資訊安全政策。

5.4 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。

5.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行懲處。

6 審查

6.1 本政策應至少每年審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本校營運持續運作及提供學術網路服務之能力。

7 實施

7.1 資訊安全推動暨維運組，每年召開資訊安全管理及審查會議，進行資訊安全政策審核。

7.2 本政策經「資訊安全推動暨維運組」核定後實施，修訂時亦同。