國立臺北藝術大學

電子計算機中心

資訊安全政策

機密等級：**D**

文件編號：**ISMS-01-001**

版　　次：**2.1**

發行日期：**2015.11.27**

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	2010.09.01			初版發行
1.1	2010.11.05	P2	邱意勳	修改3政策 維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料安全
1.2	2013.12.11	P1	李政達	修訂目的範圍
2.0	2014.10.14	P1,P2	李政達	依據 ISO27001:2013 修正
2.1	2015.11.27	P1,P2	李政達	修訂資安目標

資訊安全政策					
文件編號	ISMS-01-001	機密等級	D	版本	2.1

目錄

資訊安全政策					
文件編號	ISMS-01-001	機密等級	D	版本	2.1

1 目的

確保國立臺北藝術大學電子計算機中心（以下簡稱本中心）電腦機房及校園資訊入口網 EIP 及單一帳號登入 SSO 與 NAS 資料庫維運所屬之資訊資產機密性、完整性及可用性，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。

2 適用範圍

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：

一、 資訊安全政策制定及評估

二、 組織的資訊安全與分工

三、 人力資源的安全

四、 資產管理

五、 存取控制

六、 密碼學

七、 實體及環境安全

八、 運作安全

九、 通訊安全

十、 系統獲取、開發及維護

十一、 供應者關係

十二、 資訊安全事故管理

十三、 營運持續管理之資訊安全層面

十四、 遵循性

3 政策

「維護本校重要資訊系統之機密性、完整性與可用性，
並保障使用者資料安全。」

4 目標

本中心執行資訊安全管理制度需達以下目標：

- 系統異常而影響業務運作次數每年不得超過三次。
- 電腦病毒造成系統或網路癱瘓事件次數每年不得超過三次。
- 無 NAS 重大資訊安全事件發生。
- 社交工程演練郵件開啟率低於 10%。
- 社交工程演練附件連結點閱率低於 6%

5 責任

- 本中心的管理階層建立及審查此政策。
- 資訊安全管理者透過適當的標準和程序以實施此政策。
- 所有人員和合約供應商均須依照程序以維護資訊安全政策。
- 所有人員有責任報告安全事件，和任何已鑑別出的弱點。
- 任何蓄意去危及資訊安全的行為將受到相關懲罰或法律行動。

6 審查

本政策應至少每年評估一次，以反映利害關係方之關注、政府法令、技術及業務等最新發展現況，以確保對於維持營運的能力。

7 實施

本政策經本中心主任核准，於公告日施行，並以書面、電子或其他方式通知員工及與本中心連線作業之有關機關（構）、廠商，修正亦同。