資訊安全管理制度（ISMS）

資訊安全政策

文件編號：NTPU-ISMS-A-001

機密等級：公開使用

版　　次：2.0

制訂單位：資通安全委員會

撰 寫 人：政策規劃暨推廣小組(撰稿)

單位主管：政策規劃暨推廣小組組長(審查)＿＿＿＿＿＿＿＿核章

管理代表：資通安全管理代表＿＿＿＿＿＿(核定)＿＿＿＿＿＿核章

最新版本發行日期：107 年 06 月 29 日

本文件由國立臺北大學「資通安全委員會」簽准頒行，使用者對本文件之各項內容存有疑義者，可逕洽政策規劃暨推廣小組詮釋。對本文件之內容有任何建議，可填寫「文件修訂建議表」並經相關人員審核後，擲送「政策規劃暨推廣小組」做為修正依據。

修 訂 紀 錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
2.0	107 年 06 月 29 日	更新	政策規劃暨推廣小組	2.0 版

本文件由國立臺北大學「資通安全委員會」簽准頒行，使用者對本文件之各項內容存有疑義者，可逕洽政策規劃暨推廣小組詮釋。對本文件之內容有任何建議，可填寫「文件修訂建議表」並經相關人員審核後，擲送「政策規劃暨推廣小組」做為修正依據。

`目　錄

壹、政策緣由

為遵循相關法令並保護國立臺北大學（以下簡稱本校）資訊資產(包括資料、軟體、硬體設備等)，免於因外在之威脅，或內部人員不當之管理與使用，致遭受竄改、揭露、破壞或遺失等風險，特制訂資訊安全政策以做為遵循依據。

貳、依據

本資訊安全政策（以下簡稱本政策）係依據本校之任務目標與「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」及「教育體系資通安全暨個人資料管理規範」等相關法令與規定而訂定。

參、政策說明

一、 資訊安全本質

(一)資訊安全之本質分為以下四類：

1. 可用性：
   確保經授權的人員在需要時，均能在可接受的時間內取得相關資訊及設備。

2. 完整性：
   維持資訊或系統之正確與完整。

3. 機密性：
   確保只有經授權的人員才能存取相關資訊。

4. 適法性：
   確保資訊與處理方式過程，須遵守法律、規定、合約義務或組織內部政策、章程之規範要求。

(二)本校資訊安全即為確保本校資訊資產之完整性、可用性、機密性與適法性。

二、 政策目的與說明

為達成本校之任務目標及最高管理階層對資訊安全之期許與要求，確保本校資訊資產之安全，本校之資訊安全政策訂為：確保本校相關業務資訊之機密性、完整性、可用性與適法性，以正確執行本校作業與各項業務。

肆、目標

為達成上述目的，將相關目標分為定量與定性二類，說明如下：

一、 定量化目標

(一) 確保相關資訊安全措施或規範符合政策與現行法令之要求，每年至少進行一次查核。

(二) 每年至少進行一次業務持續計畫之測試及檢核。

二、 定性化目標

(一) 確保資訊資產受適當之保護，防止未經授權或因作業疏忽對資產所造成之損害。

(二) 確保所有資訊安全事件或可疑之安全弱點，皆依適當通報程序反映，並予以適當調查及處理。

(三) 符合政府資訊安全相關政策、規定以及相關法令要求。

(四) 定期實施資訊安全教育。

三、 本校於完成目標時考量下列項目：

(一) 所需配置之人員、預算、設備技術與程序表單等資源。

(二) 活動或事項負責人員。

(三) 活動或事項預計完成時間。

(四) 管理目標是否達成之評估方式。

伍、適用範圍

本政策適用於本校資訊中心內部人員與委外廠商。

陸、責任劃分

為使資訊安全管理系統有效運行，各單位之權責劃分如下：

一、 為確保管理階層實際支持各項資訊安全措施，本校高階主管應宣示落實資訊安全之決心，並責成相關單位與人員成立資通安全委員會，以配置資訊安全責任與進行有效之資源管理。

二、 資通安全委員會之召集人因故無法參與各項資訊安全活動時由管理代表代理之。

三、 適用範圍內各單位應透過適當程序落實本政策之要求。

四、 適用範圍內所有人員、各連線使用單位及委外廠商都應遵循本政策。

五、 適用範圍內所有人員皆負有通報所發現之資訊安全事件或資訊安全弱點之責任。

柒、其他規定

一、 適用範圍內所有人員違反本政策，或發生其他任何危及本校資訊安全之行為，都將訴諸適當之處置程序或法律行動。

二、 適用範圍內所有人員應瞭解於工作期間所有取得之資訊皆為本校之資產，未經允許，禁止做任何其他未授權之使用。

三、 與委外服務廠商簽訂相關合約時應遵循本政策之規定與相關要求。

捌、修訂

本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。