國立陽明交通大學

資通安全暨個資保護政策

機密等級：一般

文件編號：ISMS-A-02-000

版　　次：1.3

發行日期：112.12.15

修 訂 紀 錄				
版次	**發行日期**	**修訂頁次**	**修訂者**	**修訂內容摘要**
1.0	110.07.01	All	陳俐君	初版
1.1	111.04.01	3	楊麗娟	將量測指標原 4.7 有關資安事件統計的部分依據教育部稽核建議刪除
1.2	112.10.02	3,5,7	楊麗娟	1. 修訂 4.7 內容、4.12 增加服務可用時間說明。 2. 修訂 6.4 內外部議題之內容。
1.3	112.12.15	3	楊麗娟	刪除 4.6 每年因實體安全控制不足導致機房資訊資產損毀或遺失件數， 1 件(含)以下。

目錄

國立陽明交通大學

文件編號	ISMS-A-02-000	文 件 名 稱	版　　本	1.3
制定單位	資訊中心	資通安全暨個資保護政策	機密等級	一般

1 目的

為落實國立陽明交通大學（以下簡稱本校）資通安全與個人資料之保護及管理，確保各項核心資通業務所屬之資訊資產的機密性、完整性及可用性符合「個人資料保護法」、「個人資料保護法施行細則」、「資通安全管理法」與「資通安全管理法施行細則」等相關法令法規之要求，強化本校資訊安全管理暨個資保護管理，保護校內資訊資產及個人資料免於遭受內、外部蓄意或意外之威脅，維護資料、系統、設備及網路之安全，提供可靠之資訊服務，訂定本政策。

2 適用範圍

本校資訊安全暨個資保護管理涵蓋 14 項管理事項領域，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 資通安全暨個資保護政策訂定與評估。

2.2 資通安全暨個資保護組織。

2.3 資訊資產管理。

2.4 風險評鑑管理。

2.5 人員安全管理與教育訓練。

2.6 供應商管理。

2.7 實體與環境安全。

2.8 通訊與作業安全管理。

2.9 存取控制安全。

2.10系統開發與維護之安全。

2.11資訊安全事故管理。

2.12業務永續運作管理。

2.13遵循性。

2.14資訊安全稽核矯正管理。

本校之內部人員、供應商與訪客皆應遵守本政策。

3 目標與宣言

維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

3.1 保護本校核心業務及核心資通系統服務之安全，避免未經授權的存取，以確保其機密性。

3.2 保護本校核心業務及核心資通系統服務之安全，避免未經授權的修改，確保其正確完整。

3.3 建立資訊業務永續運作計畫，確保本校核心業務及核心資通系統活動之持續運作。

3.4 本校核心業務及核心資通系統活動執行須符合相關法令或法規之要求。

4 確保績效之量測指標

4.1 每年至少辦理一次全校資通系統分級及防護基準，並檢視資通系統分級妥適性。

4.2 每年辦理一次內部資通安全稽核。

4.3 每年辦理一次資安治理成熟度評估。

4.4 每二年辦理一次資通安全健診。

4.5 每年電子郵件社交工程演練對象惡意郵件開啟率≤10%，惡意郵件點擊率≤6%。

4.6 每年依教育體系資安分級，開辦資安教育訓練(含資安相關法令宣導)達成率(實際開班時數/規定開班時數) 100%，並統計全校各單位教職同仁(含主管)資安教育訓練的達成率。

4.7 本校各同仁須遵守外來文件一覽表，資安法、個資法、著作權法等相關法規，不得發生違反法規事件。

4.8 全部核心資通系統每年辦理一次業務持續運作演練。

4.9 全部核心資通系統每年辦理一次網站安全弱點檢測。

4.10全部核心資通系統每二年辦理一次系統滲透測試。

4.11全部核心業務及核心資通系統服務每年可用率維持在 99 %以上。

4.11.1　本校核心資通業務範圍包含

4.11.1.1 資訊機房維運服務

4.11.1.2 校園骨幹網路服務

4.11.1.3 無線網路服務

4.11.1.4 學籍成績系統服務

4.11.1.5 電子郵件系統服務

4.11.1.6 雲端虛擬平台服務

4.11.1.7 校園單一入口服務

4.11.1.8 學雜費系統服務

4.11.1.9 電子公文資訊服務

4.11.1.10　LDAP 認證系統

4.11.1.11　DNS 網域名稱系統

4.11.1.12　E3 數位學習平台

4.11.1.13　課務系統

4.11.1.14　全人教育系統/學務資訊系統

4.11.1.15　人事差勤系統

4.11.1.16　資訊服務追蹤系統(InspireOZ)

※上述可用率計算方式：[(服務可用時間-因資訊安全事故造成中斷時間)/ 服務可用時間]x100%，其中服務可用時間為上班日(週一至週五) 08:00-22:00，統計中斷時間為非預期的中斷，若為公告之停機時間不列入中斷時數計算。

5 責任

5.1 本校的管理階層建立及審查此政策，並成立資訊安全暨個人資料保護組織統籌資訊安全及個資保護事項推動。

5.2 管理階層應積極參與及支持資訊安全管理制度，並授權資訊安全暨個人資料保護組織透過適當的標準和程序以實施本政策。

5.3 本校之內部人員、供應商與訪客等皆應遵守相關安全管理程序以維護本政策。

5.4 本校之內部人員、供應商與訪客等均有責任透過適當通報機制，通報資訊安全事件或弱點。

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，以確保本校永續運作及提供學術網路服務之能力。

6.2 依據 ISMS 有效性量測表，定期審查資訊安全管理制度之有效性。

6.3 應考量內、外部議題及其關注方之要求，定訂適當之資訊安全管理制度驗證範圍，經由管理階層審核，確認後實行。

6.4 資訊安全管理制度驗證範圍應定期或不定期視內、外部環境之變更或執行狀況，如：法令法規之要求、組織異動、資安事件發生、管理制度落實狀況等因素，於管理審查會議進行檢視調整。

內部議題	外部議題	利害相關者	利害相關者要求	備註
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		
外部環境之變化	疫情嚴峻	教職員生	教學模式改變 上班模式改變	
	台海局勢緊張(網路攻擊)	教職員生 主管機關	提升資安防護能力	

7 實施

7.1 資訊安全政策配合管理審查會議進行資訊安全政策審核。

7.2 本政策經「資通安全暨個人資料保護推動委員會」核定後實施，修訂時亦同。

8 相關文件

8.1 ISMS-D-01-A02 ISMS 有效性量測表