朝陽科技大學
資訊安全管理政策

編　修	審　　查	核　　准	發　行　日　期
林翠婷	朱鴻棋	楊文廣	113/3/14

資訊安全管理政策					
編號	ISMS-1-001-4	**等級**	一般	**發行日期**	113/3/14

文件修訂紀錄

版次	內　　容	日　期	編修者	審查者	核准者
1	新制訂	105/7/5	林翠婷	林翠婷	朱鴻棋
2	修正參考文件 6.2	109/3/4	林翠婷	朱鴻棋	楊文廣
3	修正 5.1 政策需高階管理階層核定	112/3/21	林翠婷	朱鴻棋	楊文廣
4	資安管理制度適用範圍由圖資處改為全校，修訂 2.範圍、4.5、4.6 及 5.1 文字內容	113/3/14	林翠婷	朱鴻棋	楊文廣

資訊安全管理政策					
編號	ISMS-1-001-4	等級	一般	發行日期	113/3/14

1 目的

朝陽科技大學（以下簡稱本校）為強化資訊安全管理，以確保本校所屬資訊資產免於遭受內、外部之蓄意或意外等威脅。本校所屬資訊資產多且維運繁瑣，為達成資訊安全之一致性，故制定本校資訊安全管理政策(以下簡稱本政策)，提供相關人員共同遵循。

2 範圍

本校教職員工及接觸本校業務資料之外機關人員、委外服務廠商與訪客等皆應遵守本政策。

3 定義

資訊安全之本質為確保本校資訊服務系統之機密性、完整性與可用性，以達成資訊服務持續營運之目標。

3.1 機密性(Confidentiality)：資訊不可取得或不可公開於未經授權的個體、實體或過程之特性。

3.2 完整性(Integrity)：確保各項資訊資產之完整，以期組織能正確運用該項資產。

3.3 可用性(Availability)：確保各項資訊資產能提供即時且正確的服務。

4 內容

4.1 確保本校所屬之資產之機密性、完整性、可用性及正確性，提供持續營運發展之所需，並配合主管機關資訊安全管理政策之推動，持續提升資訊安全之防護能力。

4.2 資訊安全是本校全體員工的共同責任，各級員工必須充分理解並貫徹所負職責。

4.3 資訊安全管理系統的建立和維持，完全依據法律法規的要求及合約的安全責任，並和學校的組織風險管理背景相結合。

4.4 為有效管控資訊安全風險，必須建立包括風險評估方法、資訊安全法律法規要求、接受風險的標準、及風險之可接受程度等之風險評估暨作業管理程序，並落實執行。

4.5 每年至少召開一次管理審查會議，審核本校資訊安全業務執行狀況，建立管理指標量測方式與評估管理指標量測結果。

4.6 每年應至少進行一次核心業務之營運持續計畫演練、測試及檢討。

4.7 違反本政策與本校之資訊安全相關規範，依相關法規或本校懲戒規定辦理。

5 實施

5.1 本政策經本校資訊安全暨個人資料管理委員會討論並經主任委員核定後，對本校教職員工及相關外部各方公布及傳達。

5.2 本政策應至少每年評估一次，以符合政府法令之要求，並反映資訊科技發展趨勢，確保本校資訊安全作業之有效性。

6 參考文件

6.1 朝陽科技大學個人資料保護管理要點。

6.2 教育體系資通安全暨個人資料管理規範。

7 使用表單

無。