臺北城市科技大學

資通安全政策

機密等級：公開使用

文件編號：IS-A-001

版　　次：4.0

發行日期：112 年 12 月 21 日

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	98 年 4 月 20 日	N/A	呂育霖	初版
2.0	99 年 12 月 7 日	1、2	呂育霖	二版
2.1	101 年 2 月 21 日	N/A、1	林育泉	更改校名
3.0	104 年 2 月 9 日	2	林育泉	因應 ISO 27001:2013 新版標準進行調整
4.0	112 年 12 月 1 日	1、2	林育泉	配合 ISO 27001：2022 資通安全管理系統更版，實施修訂。

資通安全政策					
文件編號	IS-A-001	機密等級	公開使用	版次	4.0

目錄

資通安全政策					
文件編號	IS-A-001	機密等級	公開使用	版次	4.0

1 總則

1.1 為保護臺北城市科技大學（以下簡稱「本校」）所管理之資訊資產安全，免於因內部或外部、蓄意或意外之各種威脅與破壞，致使業務無法正常運作或資訊遭受竄改、揭露、破壞或遺失等風險，特制訂本政策。

1.2 本政策適用之範圍係含本校所有資通訊作業。

1.3 本校全體教職員、委外廠商及相關資訊業務之第三方人員均應遵守本政策。

2 目標

2.1 本校之資通安全政策包含下列目標：

2.1.1確保本校所保管校務資料之機密性、完整性與可用性，防止非法使用校務資料。

2.1.2確保本校所提供資通服務之完整性與可用性，提供全校師生便利和穩定的資通服務。

2.1.3確保本校所提供軟硬體資源之可用性，均能被合法及正確地使用。

3 資通安全準則

3.1 本校全體教職員工於日常作業中確實遵守「資通安全管理法」等資通安全相關法令規範。

3.2 本校全體教職員工遵守本校相關資通安全規定，確保適當使用本校資源。

3.3 視實際需要辦理資通安全教育訓練及宣導，提高所有人員資通安全意識並熟悉工作中之資通安全職責。

3.4 對於資通安全事件須有完整的通報及應變措施，以確保資通系統及重要業務的持續運作。

3.5 違反本政策與本校之資通安全相關規範，依相關法規或本校懲戒規定辦

理。

4 責任

4.1 為能有效確保本校之資通安全，應針對各資通安全領域訂定資通安全規範。

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

4.3 高階主管應積極參與資通安全管理活動，提供對資通安全之支持及承諾。

4.4 所有相關同仁皆應遵循本校資安事件通報機制，通報所發現之資通安全事件或資通安全弱點。

4.5 應建立資訊資產風險評鑑機制，每年至少進行一次風險評鑑，並訂定可接受風險值。

4.6 每年應至少進行一次業務永續經營計畫及資安事件通報程序之演練、測試、檢討。

4.7 每年應依據行政院訂頒「資通安全責任等級分級辦法」之規定，規劃並提供本校人員資通安全訓練課程，以提昇人員資通安全認知。

4.8 所有委外廠商皆須簽署保密協議書，並遵循本政策以及相關程序之規定，不得未經授權使用或濫用本校之各類資訊資產。

4.9 與本校業務相關之專案，無論其類型均應將資通安全要求納入專案管理考量，以落實資通安全目標。

5 審查與實施

5.1 本政策應每年定期審議，或因組織、業務、法令或環境等因素之變迭時，予以適當修訂。

5.2 本政策初次由行政會議審議通過，爾後修正呈請　資通安全長核定後公布施行。