南臺科技大學

資通安全暨個人資料保護管理政策

機密等級：一般

文件編號：STUST-ISPI-A-01

版　　次：1.0

發行日期：113 年 6 月 28 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	113 年 6 月 28 日		呂宜庭	初版

目錄

1 目的 1

2 適用範圍 1

3 資通安全暨個人資料保護管理目標 1

4 責任 1

5 管理指標 2

6 審查 5

資通安全暨個人資料保護管理政策					
文件編號	STUST-ISPI-A-01	機密等級	一般	版次	1.0

1 目的

1.1 南臺科技大學（以下簡稱本校）為確保所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，建立安全及可信賴之資訊環境，確保資料、資通系統、設備及網路安全，特訂定本政策。

1.2 為確保個人資料之蒐集、處理及利用之合理使用，本政策依據「個人資料保護法」、「個人資料保護法施行細則」及相關法令法規要求，使其免於遭受內、外部蓄意或意外之威脅，建立安全及可信賴之個人資料保護作業環境，保障本校人員之權益。

2 適用範圍

本校之教職員工、業務往來單位、委外服務廠商與訪客等。

3 資通安全暨個人資料保護管理目標

為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之安全，期藉由本校全體同仁共同努力以達成下列目標：

3.1 保護本校業務服務之安全，確保資訊須經授權人員才可存取資訊，以確保其機密性。

3.2 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

3.3 建立本校業務永續運作計畫，以確保本校業務服務之持續運作。

3.4 確保本校各項業務服務之執行須符合相關法令或法規之要求。

4 責任

4.1 本校應成立資通安全暨個人資料保護管理組織，統籌資通安全暨個人資料保護管理事項推動。

4.2 管理階層應積極參與及支持資通安全暨個人資料保護管理制度，並透過

適當的標準和程序以實施本政策。

4.3 本校全體人員、委外服務廠商與訪客等皆應遵守本政策。

4.4 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資通安全與個人資料事件或弱點。

4.5 任何危及資通安全與個人資料、機敏資料保護之行為，或人為故意、嚴重疏失致違反資通安全暨個人資料保護管理指標，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議處。

5 管理指標

為評量資通安全管理暨個人資料保護管理目標達成情形，特訂定資通安全暨個人資料保護管理指標如下：

5.1 資通安全管理定量化指標

5.1.1 確保本校核心資通系統資訊維運服務達全年上班時間 96%以上之可用性。

5.1.2 本校核心資通系統確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每季不得超過 4 次。

5.1.3 本校核心資通系統確保因資通安全事件、異常事件、其他安全事故所造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 4 工作小時。

5.1.4 核心業務系統作業單位應適當保護核心資通系統資訊資產之機密性與完整性，並每年至少須進行 1 次風險評鑑及風險管理。

5.1.5 為確保本校資通安全措施或規範符合現行法令、法規之要求，本校每年至少須辦理內部稽核 1 次。

5.1.6 核心業務系統作業單位應每年進行至少 1 次核心資通系統之業務永續運作計畫之維護及演練，以確保核心業務服務得以持續運作。

5.2 資通安全管理定性化指標

5.2.1 本校應定期審查本校資通安全組織人員執掌，以確保資通安全工作之推展。

5.2.2 各單位應遵循主管機關之要求，依教職員工職務及責任符合適當之資通安全相關訓練。

5.2.3 各單位應加強本校核心資通系統資訊機房設施之環境安全，採取適當之保護及權限控管機制。

5.2.4 各單位應確保本校核心資通系統資訊不因傳遞過程，或無意間之行為，透漏給未經授權之第三者。

5.2.5 各單位應加強存取控制，防止未經授權之不當存取，以確保本校核心資通系統資訊資產已受適當之保護。

5.2.6 核心資通系統應於開發時考量安全需求，並定期檢測安全弱點、進行弱點修補。

5.2.7 各單位應確保所有資通安全事件或可疑之安全弱點，均依循適當之通報機制向上反應，並予以適當調查及處理。

5.3 個人資料保護管理定量化指標

5.3.1 內部稽核結果符合合法蒐集、處理、利用個人資料，未有不符合情況。

5.3.2 妥善管理本校個人資料檔案，未有嚴重事件。

5.3.3 內部稽核結果依「個人資料保護法」規定保護資料當事人權益，未有不符合情況。

5.4 個人資料保護管理定性化指標

5.4.1 各單位對於個人資料的蒐集、處理、利用，除合法及合於業務作業目的之外，嚴禁一切非法或非業務作業之行為。

5.4.2 各單位僅於業務作業過程中之特定目的內蒐集個人資料。

5.4.3 各單位僅於法律規定及業務作業所須範圍蒐集最少之個人資料，並且不處理過多的個人資料。

5.4.4 各單位應提供明確之管道讓當事人知悉其個人資料將如何被使用及被誰使用的清楚資訊。

5.4.5 各單位本著合法、公平、公正、公開的合理處置原則，進行蒐集、處理、利用必要之個人資料，並建立管理制度，以合理且適切的處理所取得之個人資料。

5.4.6 各單位對於所取得之個人資料，應建立個人資料檔案清冊並適當維護相關內容。

5.4.7 為保持個人資料精確性，依作業性質及當事人之請求，予以保持最新。

5.4.8 個人資料保存期限，僅在合乎法律或規定或特定目的內進行。

5.4.9 各單位應尊重當事人權利，建立相關處理流程。

5.4.10 為了確保個人資料的正確性和安全性，各單位應建立適當的安全維護措施。

5.4.11 各單位僅於合法及有適當保護的狀況下傳送個人資料至其他國家或地區。

5.4.12 各單位應嚴格遵守個人資料保護相關法規，包含其他法規豁免例外應用。

5.4.13 各單位適當鑑別並諮詢利害關係人，以增加利害關係人的參與程度。

5.4.14 本校持續發展及實施個人資料保護管理工作，以確保政策得以落實。

5.4.15 各單位確認相關人員在個人資料保護管理制度內之職掌及責任。

5.4.16 當需要處理兒童個人資料時，各單位應有監護人同意機制，但關

於提供專業諮詢與預防性服務之情況除外。

5.4.17各單位應妥善維護及保存個人資料處理紀錄。

6 審查

本校應每年至少審查本政策 1 次，以反映政府法令、技術及業務等最新發展現況，以確保本校業務永續運作暨個人資料保護之能力。