國立臺南大學

人員資通安全守則

機密等級：一般

文件編號：NUTN-ISMS-C001

版　　次：1.4

發行日期：110 年 03 月 23 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	100/01/13		林雅雯	初版
1.1	100/12/20	1-2	張育傑	3.7 不得在...論壇、或公佈欄中透露... 修改為: 3.7 不得在...論壇、公佈欄、**網誌、社交網頁..等**中透露... 新增 4.5.9 全英文或全數字。
1.2	105/10/31	1	王元良	一、1 目的 國立臺南大學（**以下簡稱本校**）電子計算機中心（以下簡稱本中心）資訊通訊安全政策...可用性**及符合相關法規之要求**，特訂定此守則。 二、統一 C001、C002 及 C006 密碼設置原則： 4.5 密碼設置原則，應儘量避免使用如下等易猜測或公開資訊為設定： 4.5.1 年、月、日等時間資訊。 4.5.2 個人姓名、出生日或身分證字號。 4.5.3 機關、單位名稱、識別代碼或是其他相關事項。 4.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。 4.5.5 電話號碼。 4.5.6 使用者識別碼、使用者姓名、群組名稱或是其他系統識別碼。 4.5.7 重複出現兩個字以上的識別字碼。 4.5.8 以全部數字或是全部字母組成密碼。 4.5.9 英文或是其他外文的常用字彙。 4.5.10 常用專有名詞。 4.5.11 地方名稱。
1.3	107/02/27	1-2	王元良	配合資通安全管理法及相關子法用語，修正本說明書相關內容： 一、「人員資訊安全守則」名稱修正為「人員資通安全守則」。

				二、 內文「資訊安全」文字全部修正為「資通安全」。 三、 1 目的「為落實國立臺南大學（以下簡稱本校）電子計算機中心（以下簡稱本中心）資訊通訊安全政策...」修正為「為落實國立臺南大學（以下簡稱本校）資通安全管理政策...」。 四、 2 適用範圍「本全體中心同仁與委外廠商。」修正為「本校全體同仁與委外廠商。」。 五、 「3.7 不得在...有關本中心資訊細節」修正為「3.7 不得在...有關本校資訊細節」。 六、 「3.8 在丟棄任何曾經儲存本中心資訊...」修正為「3.8 在丟棄任何曾經儲存本校資訊...」。 七、 「5.1 本中心資訊機房...」修正為「5.1 本校電子計算機中心(以下簡稱本中心)資訊機房...」。 八、 8 相關文件增列 8.6 資通安全管理法及 8.7 資通安全管理法施行細則。
1.4	110/03/23	2	王元良	修訂條文： 一、版次頁「電子計算機中心」文字刪除。 二、修正 5.1 本校~~電子計算機中心(以下簡稱本中心)~~資訊機房伺服器所使用之電腦軟體均須具有合法版權... 三、條文內容「本中心」文字均修正為「本校」。

人員資通安全守則					
文件編號	NUTN-ISMS-C001	機密等級	**一般**	版次	1.4

1 目的

為落實國立臺南大學（以下簡稱本校）資通安全管理政策，維護資訊及處理設備之機密性、完整性、可用性及符合相關法規之要求，特訂定此守則。

2 適用範圍

本校全體同仁與委外廠商。

3 作業守則

3.1 電腦應設定密碼確實保密。

3.2 電腦應設定螢幕保護程式並設定密碼保護，若該作業系統無類似功能，離開電腦前應隨手鎖定螢幕或登出。

3.3 作業系統漏洞應即時更新修補。

3.4 視窗作業系統應安裝防毒軟體並即時更新病毒碼。

3.5 應定期將重要資料備份存放。

3.6 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。

3.7 不得在任何公開的新聞群組、論壇、公佈欄、網誌、社交網頁..等中透露任何有關本校資訊細節。

3.8 在丟棄任何曾經儲存本校資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀至無法解讀之程度。

3.9 敏感等級（含）以上之文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。

3.10 重要機密文件或合約，應妥善保存；若為電子檔案應考慮設定保護密碼。

3.11 應依「資訊資產管理程序書」規定之資產之分級制度流通資訊，防止資訊不當外洩。

3.12 開啟來路不明之電子郵件及其附件時應謹慎小心，以防電腦中毒。

3.13 當有跡象顯示系統可能中毒時，應儘速通知相關人員。

3.14 禁止濫用系統及網路資源，複製與下載非法軟體。

3.15 應遵守「個人資料保護法」規範，保護個人資料使用之合法性及機密性。

4 密碼使用要點

4.1 應保護密碼，維持密碼的機密性，使用者應至少每 6 個月更換密碼一次，並禁止重複使用相同的密碼。

4.2 應避免將密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

4.3 當有跡象顯示系統及密碼可能遭破解時，應立即更改密碼。

4.4 密碼的長度最少應有 8 位長度，且應符合密碼設置原則。

4.5 密碼設置原則，應儘量避免使用如下等易猜測或公開資訊為設定：

4.5.1 年、月、日等時間資訊。

4.5.2 個人姓名、出生日或身分證字號。

4.5.3 機關、單位名稱、識別代碼或是其他相關事項。

4.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

4.5.5 電話號碼。

4.5.6 使用者識別碼、使用者姓名、群組名稱或是其他系統識別碼。

4.5.7 重複出現兩個字以上的識別字碼。

4.5.8 以全部數字或是全部字母組成密碼。

4.5.9 英文或是其他外文的常用字彙。

4.5.10 常用專有名詞。

4.5.11 地方名稱。

5 電腦軟體版權之使用與管理

5.1 本校資訊機房伺服器所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。

5.2 本校人員若有安裝機房伺服器軟體需求時，需填寫「資訊服務申請表」，經權責主管以上核准後，始得執行安裝。

6 保密協定

本校人員應填具「保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密，非經主管授權不得對外透露或加以濫用。

7 公告與實施

7.1 本守則由本校管理代表核准後公告實施，修訂時亦同。

7.2 本校員工若未遵守上述規定或「資通安全管理政策」及程序者，得依相關懲戒程序處置違紀人員。

8 相關文件

8.1 資通安全管理政策

8.2 資訊資產管理程序書

8.3 資訊服務申請表

8.4 保密切結書

8.5 個人資料保護法

8.6 資通安全管理法

8.7 資通安全管理法施行細則