

人員資通安全守則					
文件編號	XXXX-D-015	機密等級	限閱	版次	1.0

- 1 目的：為落實 XXXX 學校（以下簡稱本校）資訊通訊安全作業，維護資訊及處理設備之機密性、完整性及可用性，特訂定此守則。
- 2 範圍：本守則適用於正職人員與約聘（僱）人員。
- 3 作業守則
 - 3.1 電腦應設定密碼確實保密。
 - 3.2 電腦應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 10 分鐘以內。
 - 3.3 電腦之作業系統漏洞應即時更新修補。
 - 3.4 電腦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、或公佈欄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）以上資訊之紙本文件若不再使用時，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 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。
 - 3.12 當有跡象顯示系統可能中毒時，應儘速通知相關人員。
 - 3.13 禁止濫用系統及網路資源，複製與下載非法軟體。
 - 3.14 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 密碼使用原則
 - 4.1 應保護通行密碼，維持通行密碼的機密性；資訊系統之系統管理者應至少每 6 個月更換密碼一次，一般資訊系統之使用者應至少每年更換密碼，並禁止重複使用相同的密碼。
 - 4.2 應避免將通行密碼記錄在書面上，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通行密碼可能遭破解時，應立即更改密碼。
 - 4.4 通行密碼的長度最少應有 8 位長度，且應符合密碼設置原則。

人員資通安全守則					
文件編號	XXXX-D-015	機密等級	限閱	版次	1.0

4.5 密碼設置原則，應儘量避免使用易猜測或公開資訊為設定：

4.5.1 個人姓名、出生年月日、身分證字號。

4.5.2 機關或單位名稱識別代碼或是其他相關事項。

4.5.3 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

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 英文或是其他外文字典的字彙。

4.5.7 專有名詞。

4.5.8 空白。

5 電腦軟體版權之使用與管理

5.1 禁止使用未經授權之電腦軟體，遵守智慧財產權相關規定。

5.2 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。

5.3 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

6.1 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 本守則由本校資訊安全委員會通過後公告實施，修訂時亦同。

7.2 本校員工若未遵守上述規定或資訊安全政策及程序者，得依相關懲戒程序處置違紀人員。

簽署人：_____

中 華 民 國 年 月 日