

人員資訊安全守則					
文件編號	YUNTECH-ISMS-D-018	機密等級	一般	版次	1.6

紀錄編號：_____

填表日期： 年 月 日

1. 目的：為落實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：本守則適用於本校人員、約聘(僱)人員與委外人員(以下簡稱本校人員)。
3. 公務電腦與**公務伺服器**使用與管理
 - 3.1 應設定螢幕保護程式及密碼。
 - 3.2 **應即時更新修補作業系統漏洞。**
 - 3.3 應安裝防毒軟體並即時更新病毒碼。
 - 3.4 **應關閉可攜式儲存媒體之自動執行功能。**
 - 3.5 **對外提供網路服務，應於上線前通過弱點掃描檢測，並由專人負責資通安全維護作業。**
4. 使用通行密碼應注意下列要點：
 - 4.1 應保護通行密碼，維持通行密碼的機密性；一般資訊系統之使用者應至少每 6 個月更換通行密碼一次。
 - 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，必要時通知資安與個資窗口。
 - 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。
 - 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。
 - 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。

人員資訊安全守則					
文件編號	YUNTECH-ISMS-D-018	機密等級	一般	版次	1.6

4.5.8 空白。

5. 公務資料及文件儲存之管理

- 5.1 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。
- 5.2 應定期將重要資料備份存放。
- 5.3 含有敏感等級（含）以上資訊之紙本文件不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。
- 5.4 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。

6. 公務資料傳遞及電子郵件使用與管理

- 6.1 傳送公務資訊應有適當保護，例如加密傳送。
- 6.2 公務資料傳遞及聯繫必須使用公務電子郵件帳號，不得使用非公務電子郵件傳送或討論公務訊息。
- 6.3 在開啟來路不明之電子郵件及其附件應謹慎小心，以防電腦中毒。
- 6.4 不得使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。
- 6.5 即時通訊軟體使用應注意不得傳送公務敏感資料。

7. 網路通信與作業管理

- 7.1 辦公環境內必須使用機關提供之資訊設備、網路，及規定之軟體，不得使用個人私有設備及危害國家資通安全產品(例如:大陸廠牌資通訊設備)，公務設備亦不得連結個人私有手機上網。
- 7.2 禁止濫用系統及網路資源，複製與下載非法軟體。
- 7.3 上班期間不應連結非公務需要之網站，並避免連結惡意網站或釣魚網站，如發現異常連線，請通知資安窗口。

8. 所有人員應留意各相關資訊資產對應之機密等級，防止資訊不當外洩

9. 有資安疑慮或異常時，應即時通報資安窗口及相關人員。

10. 電腦軟體版權之使用與管理

- 10.1 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。
- 10.2 本校人員若有安裝機房伺服器軟體需求時，需經權責主管以上核准後，始得執行安裝。

人員資訊安全守則					
文件編號	YUNTECH-ISMS-D-018	機密等級	一般	版次	1.6

11. 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。
12. 請勿任意拆卸或架設資通訊設備，或擅自更改系統環境設定；應定期進行資通訊設備硬體與軟體之安全性檢查。
13. 應依「資通安全責任等級分級辦法」接受資通安全教育訓練。
14. 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。
15. 應遵守「個人資料保護法」及「個人資料保護法施行細則」規範，保護個人資料使用之合法性及機密性；應遵守「資通安全管理法」，嚴守工作保密規定與國家相關法令對業務機密負完全保密之責。
16. 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。
17. 主動通報資安事件或可能資安風險者，依規定獎勵。
18. 本校人員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，未遵守機關資安規定，初次予以告誡，若持續發生或勸導不聽者，依規定懲處；若因而發生資安事件，加重處分。
19. 資通安全與個資保護管理專區網址：<https://ismssys.yuntech.edu.tw/>
20. 資安窗口：

單 位:圖書資訊處網路資安組
電 話:05-5342601#2655
電子郵件:pdp@yuntech.edu.tw

我已閱讀並接受上述守則內容 _____ (請親簽)

中 華 民 國 _____ 年 _____ 月 _____ 日