

機密等級： ☐ 一般 ☒ 限閱 ☐ 密 ☐ 機密	文件編號：ISMS-D-018	保存年限：3 年
日期：114 年 1 月 24 日	紀錄編號：2025-001	版本：1.3

國立高雄科技大學

人員資訊安全守則

- 1 目的：為落實國立高雄科技大學（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 電腦應設定密碼確實保密。
- 4 電腦應設定螢幕保護程式（10 分鐘）並設定密碼保護。
- 5 電腦之作業系統漏洞應即時更新修補。
- 6 電腦應安裝防毒軟體並即時更新病毒碼。
- 7 應定期將重要資料備份存放。
- 8 使用通行密碼應注意下列要點：
 - 8.1 應保護通行密碼，維持通行密碼的機密性；
 - 8.1.1 資訊系統之管理者應至少每 3 個月更換通行密碼一次，並禁止重複使用相同的密碼。
 - 8.1.2 系統一般使用者應至少每 6 個月更換通行密碼一次，並禁止重複使用相同的密碼。
 - 8.2 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。
 - 8.3 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。

機密等級： ☐ 一般 ☒ 限閱 ☐ 密 ☐ 機密	文件編號：ISMS-D-018	保存年限：3 年
日期：114 年 1 月 24 日	紀錄編號：2025-001	版本：1.3

8.4 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。

8.5 通行密碼設置原則，應儘量避免使用易猜測或公開資訊為設定：

8.5.1 個人姓名、出生年月日、身分證字號。

8.5.2 機關或單位名稱識別代碼或是其他相關事項。

8.5.3 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。

8.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

8.5.5 電話號碼。

8.5.6 英文或是其他外文字典的字彙。

8.5.7 專有名詞。

8.5.8 空白。

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

10 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。

11 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。

12 限閱等級（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。

13 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。

14 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。

機密等級： ☐ 一般 ☒ 限閱 ☐ 密 ☐ 機密	文件編號：ISMS-D-018	保存年限：3 年
日期：114 年 1 月 24 日	紀錄編號：2025-001	版本：1.3

- 15 當有跡象顯示系統可能中毒或遭到惡意攻擊時，應儘速通知本校電算中心。
- 16 禁止濫用系統及網路資源，複製與下載非法軟體。
- 17 本校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授權之電腦軟體。
- 18 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。
- 19 保密協定：

本校人員若於業務上有接觸「密」級以上之資料者，應簽署「保密切結書」，並克盡保密之責，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。
- 20 為防止資訊安全事件發生或擴大，本校電算中心得限制或撤銷違反本守則人員之資訊資源使用權利。
- 21 人員如違反本守則，將由電算中心通知其單位，建請依本校獎懲相關規定議處；情節重大者，則由本校相關單位依據「公務機關所屬人員資通安全事項獎懲辦法」第四條及第五條規定辦理。

本守則由資訊安全委員會核准後公告實施，修訂時亦同。