國立政治大學

人員資通安全守則

機密等級：一般

文件編號：NCCU-C-002

版　　次：2.0

發行日期：113/07/30

人員資通安全守則					
文件編號	NCCU-C-002	機密等級	一般	版次	2.0

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	110/09/06	All	郭紫玫	初版 (依資通安全管理法與 ISO 27001 標準要求事項修訂)
2.0	113/07/30	All	郭紫玫	彙整一般使用者應落實執行之控制項目。

人員資通安全守則					
文件編號	NCCU-C-002	機密等級	一般	版次	2.0

目錄

人員資通安全守則					
文件編號	NCCU-C-002	機密等級	一般	版次	2.0

1. 目的

為落實本校「資通安全政策」，維護資通訊及處理設備之機密性、完整性及可用性，並強化人員（含駐點外包人員）資通安全認知，防止因人為疏失而導致機敏資料外洩等情事發生，以確保各單位電腦、資料、系統及網路安全，特訂定此守則。

2. 適用範圍

本校人員、約聘（僱）人員與委外人員均適用之。

3. 電腦及資通訊設備使用規範

3.1 電腦應設定帳號、密碼，帳號持有人應妥善保管帳號與密碼。

3.2 無論系統管理者或使用者應避免共用帳號。

3.3 密碼設定最少應有 8 位長度，並取英文字母大小寫、數字與特殊符號其中 2 種要素之組合，且不得採用電腦自動記憶方式、明文書寫、張貼或交予他人使用。

3.4 密碼應至少每年更換一次，並禁止重複使用前 3 次相同的密碼。

3.5 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並以密碼保護、鎖定或登出離線等安全控制措施，且取出自然人憑證。

3.6 禁止私自安裝未經合法授權軟體。

3.7 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

3.8 下班時應關閉電腦及螢幕電源。

3.9 針對物聯網設備應採取適當管控機制，如連線控管、變更廠商預設帳密、禁止使用弱密碼、修補安全漏洞。

3.10 電腦若疑似受駭時，應立即拔除網路線，停止連網行為並向本校「資通安全事件通報窗口」通報。

3.11 受駭電腦重整後，應立即變更曾於該受駭電腦登入之所有系統密碼（如校內資通系統、電子郵件系統等）。

3.12 如發現資安問題，請主動向本校「資通安全事件通報窗口」通報。

4. 網際網路使用規範

4.1 連網電腦禁止瀏覽非法網站。

4.2 禁止於辦公室內架設私人電腦及網路通訊等相關設備。

5. 電子郵件安全管理規範

5.1 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。

5.2 辦理公務業務或核心業務時，應使用本校配發之電子信箱收發公務所需資訊，不得使用非公務信箱進行公務郵件收發等事宜。

5.3 辦理公務、及重要（或敏感）專案使用之電子郵件信箱（可規劃專用電子郵件信箱），不得轉至外部私人信箱收發公務資訊。

6. 資料保護規範

6.1 處理密級以上或各單位認定需保護之敏感性資料（以下簡稱機敏資料）時，得評估使用專屬實體隔離電腦設備處理及列印。

6.2 機敏資料應考量加密存放。

6.3 儲存機敏資料之可攜式儲存媒體須上鎖保管。

6.4 使用可攜式儲存媒體存放資料時，機敏資料及一般資料得分開儲存，避免混用並妥善保管。

6.5 機敏資料若有傳送需求，應於加密後，方可透過網路傳送。

6.6 禁止在家中、公共場合等辦公室以外場所使用連網電腦處理機敏公務。

6.7 各項重要業務資料均應妥善定期備份，並經檢視以確保備份資料之可用性。

6.8 銷毀含機敏資料之相關文件及設備，應依下列方式處理：

6.8.1 含有機敏資料之紙本，使用碎紙機將其銷毀。

6.8.2 含有機敏資料之公文，銷毀方式，須依檔案法及相關規定辦理。另委外銷毀時，應派人隨車陪同，確認公文已經安全銷毀，並拍照存證備查。

6.8.3 有機敏資料電子檔案之媒體，例如：光碟片可利用將反光層抹除，或經由碎紙機銷毀；磁帶、磁片或其他無法以軟體清除資料之硬體資訊資產，應進行實體破壞，使其無法使用，並拍照存證備查。

7. 人員管理暨保密規範

7.1 本校人員與約聘（僱）人員於服務期間皆應遵守「公務員服務法」、本資通安全守則或聘用契約書之保密條款規範要求，於業務上所獲知之機密資訊，非經主管授權不得對外透露，克盡保密之責。

7.2 本校處理核心資通系統業務等相關人員(含工讀生)，於到職時應另行簽署「保密切結書」。

7.3 本校一般使用者或主管每年應完成 3 小時以上之資安通識教育訓練；資訊人員應每 2 年完成 3 小時以上之資安專業課程訓練。

7.4 委外廠商應要求遵守「資通安全管理法」、「個人資料保護法」及本校之相關規定，並簽訂「合約商保密切結書」。

7.5 針對人員違反本守則，依情節重大程度進行議處。

8. 大陸廠牌資通訊產品管理規範

8.1 禁止使用及採購「大陸廠牌資通訊產品」

8.1.1 大陸廠牌如：杭州海康威視（Hikvision）、華為（Huawei）、深圳大疆創新科技公司（DJI）、普聯技術公司（TP-Link）、廣東歐加

控股公司／廣東行動通訊公司（OPPO）、小米集團（MI）、浙江大華技術公司（Dahua）等。

8.1.2 大陸廠牌軟體例如：微信、騰訊 QQ、360 安全衛士等。

8.2 於學校「對外出租場域契約」或「場地租借使用規定」，應明訂不得使用大陸廠牌資通訊產品。

9. 公告與實施

本守則由本校「資通安全委員會」執行秘書核准後公告實施，修訂時亦同。

10. 相關文件

10.1 資通安全政策。

10.2 個人資料保護法。

10.3 資通安全管理法。

10.4 保密切結書。

10.5 合約商保密切結書。