

國立羅東高中 資訊網路系統安全宣導

一、資安管理

1. 資安宣導：密碼換新、程式更新、下載要當心。
2. 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中國廠牌產品，公務設備亦不得連結個人私有手機上網。若有業務上的需求，必須經資安長(校長)同意後，列冊管理並定期檢討。
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(註冊組)。
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。
5. 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. 即時通訊軟體使用應注意不得傳送公務敏感資料。
7. 傳送公務資訊應有適當保護，例如加密傳送。
8. 帳號密碼必須妥善保存，並遵守機關規定，如有外洩疑慮，除儘速更換密碼外，並應通知資安窗口(註冊組)。
9. 主動通報資安事件或可能資安風險者，依規定獎勵。
10. 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。
11. 有資安疑慮或異常時，應即時通報資安窗口(註冊組)。
12. 應遵守個人資料保護法及資通安全管理法。
13. 資安窗口：圖書館
14. 備註：參考資料來源：行政院資通安全處

二、教育訓練（使用者）：一般使用者及主管每人每年接受三小時以上之資通安全通識教育訓練

- 資安法上路！建構資通安全新時代(影片)
-

- 網路犯罪掀資安隱憂(影片)
- 談資安法要求
- 網路犯罪掀資安隱憂

三、教育訓練（資安人員）：

- 校園機房管理與安全
- 資產盤點與風險評鑑
- 校內資通安全線上教育訓練

四、密碼安全：

- 密碼包含大小寫英文字母、數字和符號，長度 6 碼以上，建議 8 碼以上。
- 資訊系統避免使用共用帳號密碼。
- 更改密碼：（建議每 6 個月更新一次）

五、防毒軟體：

- 校內電腦授權請至圖書館協助安裝。

六、遠端連線：

- 因台灣學術網路資安政策限制，校外電腦不得使用 TeamViewer 等資安高風險遠端桌面軟體連線校內電腦。

七、公務資安：

- 資安宣導口號「密碼換新、程式更新、下載要當心」
 - 作業系統更新：設定→更新與安全性→Windows Update。
-

- 安裝防毒軟體，更新病毒碼：Sophos，設定排程定期掃描。
- 電子郵件附件及下載檔案在使用前需檢查有無惡意軟體。
- 設定螢幕保護：設定→個人化→鎖定畫面→螢幕保護程式設定→15 分鐘+登入密碼。
- 非經核准，不可安裝非公務用軟體。
- 電子郵件附件及下載檔案在使用前需檢查有無惡意軟體。
- 重要資料備份：至少每月一次。
- 機密性資料妥善保存於上鎖的櫃子，下班後將經辦之機密性或敏感性資料妥善收藏。

八、社交工程：

- 使用 Outlook 收信軟體，請務必關閉郵件預覽功能。
- 陌生郵件不開附件檔！不點入連結！
- 不轉發非業務相關郵件。
- 常見的社交工程攻擊方式有哪些？應如何防範？（行政院資通安全處）
- 疾管署「最終通知」假郵件 小心遭駭！（華視新聞）

九、資安通報：

- 教育機構資安通報平台
-

資通安全事件通報流程說明



十、資安機構：

- 國家資通安全通報應變網站

- 行政院國家資通安全會報
- 行政院國家資通安全會報技術服務中心
- TACERT 台灣學術網路危機處理中心

十一、資安網站：

- 教育部全民資安素養網站
- 165 全民防騙網

十二、資安管理法規：

- 資通安全管理法
 - 資通安全管理法施行細則
 - 資通安全責任等級分級辦法
 - 資通安全事件通報及應變辦法
-