

# 公務機密維護宣導



112年10月



# 公務機關「駭不駭」怕~~~資安三件事

## 別駭人

公務機密維護到位嗎？

洩密？

我是檢舉人？

## 被駭了

網頁竄改

資料庫入侵

## 不給駭

關鍵基礎設施

資通訊設備

維護給不給力



## 駭客入侵！高雄市環保局官網高掛五星旗 市府緊急公告維護

2022-08-04 21:43 聯合報 / 記者徐如宜、林巧璉 / 高雄即時報導

# 造成公務資料外洩的原因— 人為疏忽

1. 使用私人電腦處理公務
2. 電腦知識不足
3. 使用不明軟體
4. 主要原因還是在於駭客入侵問題 上

# ▶ 為何駭客會對公務資料有興趣？

因為公務資料在資訊安全的定義中，是一種可以變賣的資產。

而資訊資產的範圍包括：

1. 資訊紀錄（資料、資料庫、資料檔、系統規劃與設計文件、使用與操作手冊、內部控制 作業要點）
2. 電腦系統（電腦作業系統、應用系統、開發工具、服務、電力服務、空調服務）
3. 人員（資訊系統開發與維護人員、系統管理人員、資訊與設備擁有者、資訊/文件製作人員）
4. 實體（工作區、員工辦公區、主機控制室、機房、機器設備、電腦、通訊設備）等，它們每一項可以用財務的角度來評估它的價值，駭客經由各種手段取得這些資產後，可以變賣獲利，這也就是為何資訊安全事件會層出不窮的原因，最後的目的就是竊取公務機密資料。

參考網址：

[HTTPS://WWW.DGPA.GOV.TW/UPLOADS/PUBLIC/ATTACHMENT/8121716442771.PDF](https://www.dgpa.gov.tw/uploads/public/attachment/8121716442771.pdf)  
從資安看如何防止 公務機密資料外洩-陳邦正 行政院人事行政局(目前為人事行政總處)資訊室主任

# “ 如何防止公務機密資料外洩 ”

要有資訊安全是大家的事的認知，不會只是資訊人員的事

- 減少接觸不當資訊管道，不隨意下載或複製不明檔案。
- 減少上網做線上交易等機密活動，不輕易在網路留下身分證號、信用卡號。
- 機密資料要審慎保護：重要資料要備份、桌面要清潔、螢幕保持淨空、機密文件上鎖、重要檔案要加密、減少檔案分享。
- 電子郵件會攜帶病毒和木馬程式等惡意程式，不要轉寄郵件、取消郵件預覽、不明人士寄的附件檔立即刪除、使用垃圾郵件篩選功能、不回應垃圾郵件、使用防毒軟體。
- 不隨便下載不明程式或在不明網站上閒逛。
- 定期檢查防毒或防火牆軟體，並且隨時更新病毒碼。

參考網址：<https://www.dgpa.gov.tw/Uploads/public/Attachment/8121716442771.pdf>  
從資安看如何防止 公務機密資料外洩-陳邦正 行政院人事行政局(目前為人事行政總處)資訊室主任

# 本府近期資訊安全重要提示



**社交工程演練期間為一個月(9  
月 18 日至 10 月 17 日)請同仁  
勿開啟與公務無關之電子郵件**

本府本(112)年度第二次電子郵件社交工程訂於9月18日~10月17日實施，請各位同仁不要開啟來路不明及與本身業務不相關之「電子郵件」。

感謝各位同仁的配合。

計畫處資訊科



# 「使用生成式AI參考指引」內容（一）

## 行政院112年8月31日通過

本參考指引（草案）共計十點如下：

一、為使行政院及所屬機關（構）（以下簡稱各機關）使用生成式AI提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險，特就各機關使用生成式AI應注意之事項，訂定本參考指引。

二、生成式AI產出之資訊，須由業務承辦人就其風險進行客觀且專業之最終判斷，不得取代業務承辦人之自主思維、創造力及人際互動。

三、製作**機密文書**應由**業務承辦人親自撰寫**，禁止使用生成式AI。前項所稱機密文書，指行政院「文書處理手冊」所定之國家機密文書及一般公務機密文書。

四、業務承辦人不得向生成式AI提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式AI詢問可能涉及機密業務或個人資料之問題。但封閉式地端部署之生成式AI模型，須確認系統環境安全性後，方得依機密等級分級使用。

五、各機關不可完全信任生成式AI產出之資訊，亦不得以未經確認之產出內容直接作成行政行為或作為公務決策之唯一依據。



# 「使用生成式AI參考指引」內容（二）

## 行政院112年8月31日通過

六、各機關使用生成式AI作為執行業務或提供服務輔助工具時，應適當揭露。

七、使用生成式AI應遵守資通安全、個人資料保護、著作權與相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。各機關得依使用生成式AI之設備及業務性質，訂定使用生成式AI之規範或內控管理措施。

八、各機關應就所辦採購事項，要求得標之法人、團體或個人注意本參考指引，並遵守各該機關依前點所訂定之規範或內控管理措施。

九、公營事業機構、公立學校、行政法人及政府捐助之財團法人使用生成式AI，得準用本參考指引。

十、行政院及所屬機關（構）以外之機關得參照本參考指引，訂定各該機關使用生成式AI之規範。

# 禁止公務部門使用生成式AI製作機密文書 以保有執行公務之機密性及專業性

- 機密文書，指行政院「文書處理手冊」所定之國家機密文書及一般公務機密文書。
- 業務承辦人不得向生成式AI提供涉及公務應保密之資訊。
- 也不得向生成式AI詢問可能涉及機密業務的問題。
- 生成式AI產出之資訊須由業務承辦人做最終判斷。

陳建仁院長在院會表示，生成式AI可取代部分腦力，相關應用的確非常重要，但帶來對國人、社會、個人及國家安全的潛在風險與衝擊，更需由科技、產業發展、人才及治理等各方面積極布局並正面因應挑戰，以回應國內、外社會挑戰及維持國家安全。

# 資料來源

1. 2022-08-04 21:43 聯合報／ 記者徐如宜、林巧璉／高雄即時報導客
2. <https://www.dgpa.gov.tw/Uploads/public/Attachment/8121716442771.pdf>  
從資安看如何防止 公務機密資料外洩-陳邦正 行政院人事行政局(目前為人事行政總處)資訊室主任





苗栗縣政府政風處 關心您

▶ 廉政專線：037-356639