# 公務出國（含大陸地區、香港及澳門）資通訊設備管理須知

| 規定 | 說明 |
| --- | --- |
| 一、為推動資通安全管理法第六條第一項所定資通安全整體防護事宜，強化中央與地方機關（構）人員公務出國（含大陸地區、香港及澳門）期間資通訊設備及儲存媒體管理，防止公務機密資料遭竊取、竄改、毀損、滅失或洩漏，影響其機密性、完整性及可用性，訂定本須知。 | 明定本須知訂定目的，係為推動資通安全管理法第六條第一項所定資通安全整體防護事宜，強化公務出國人員資通訊設備及儲存媒體管理，以保護公務機密資料。 |
| 二、名詞定義<br>(一)資通訊設備：電腦、平板、手機、穿戴裝置等設備；惟不含已落實實體隔離且配有保密裝備之設備。<br>(二)儲存媒體：隨身碟、硬碟、記憶卡等儲存裝置。<br>(三)一般人員：因公務出國之中央及地方機關（構）人員，不含公立學校之教職員及駐外館處長期派駐人員；但駐外館處長期派駐人員若因臨時、短期公務需求，需離開駐在國並派赴他國者，仍適用之。<br>(四)重要人員：政務人員及其秘書人員、國家機密保護法第二十六條第一項所列涉及國家機密人員、涉及國家安全或重大利益公務人員特殊查核辦法第二條第一項所稱涉及國家安全或重大利益公務人員，及其他經機關認定攜有高度機敏性資料或具備機敏資料存取權限之人員。<br>(五)高資安風險地區：指反滲透法第二條第一款所定義之境外敵對勢力所管地區。 | 一、就本須知各相關重要名詞，予以定義及限縮適用範圍。<br>二、考量部分機關因其業務具高度保密性質，已對公務出國人員資通訊設備施以實體隔離及保密裝備等措施，業具備充分防護且無法適用本須知管理措施，爰於第一款將前揭設備排除本須知適用。<br>三、 本須知係針對短期間公務出國人員資通訊設備及儲存媒體之管理，爰於第三款排除駐外館處長期派駐人員；惟派駐人員因公派赴駐在國以外之他國時，仍適用本須知規定。 |
| 三、本須知管理措施分為二級，適用時機如下：<br>(一)一般管理措施：一般人員及重 | 說明本須知管理措施分級方式及適用時機，分為兩級，公務出國人員無論一般人員或重要人員均適用一般管理措施； |

| | |
|---|---|
| 要人員公務出國，均適用一般管理措施。<br>(二)進階管理措施：重要人員前往高資安風險地區，除一般管理措施外，尚須適用進階管理措施。 | 重要人員前往高資安風險地區，另適用進階管理措施，詳細內容分列於第四及第五點。 |
| 四、一般管理措施<br>公務出國人員攜帶機關配發提供平時公務使用（以下簡稱公務配發）之資通訊設備及儲存媒體，或攜帶存有公務資料、用於公務聯絡之自有資通訊設備及儲存媒體者，均應採行下列管理措施，並依附件一資通安全檢核表檢核一般管理措施之項目；攜帶自有資通訊設備及儲存媒體，無法自行完成檢測者，應簽署附件二資通安全檢測同意書，由機關設備管理人員協助完成檢測：<br>(一)出國前<br>1.公務配發資通訊設備僅安裝公務需用且為官方合法授權之穩定版本軟體；且不得下載、安裝或使用危害國家資通安全產品。<br>2.公務配發資通訊設備應確實套用政府組態基準（Government Configuration Baseline, GCB）或機關自訂之組態基準，並記錄例外項目。<br>3.公務配發資通訊設備應安裝防毒軟體並確認病毒碼更新至最新版，並執行全機掃描；確認資通訊設備之作業系統及各項軟體更新至最新穩定版本，勿使用已停止更新版本。<br>4.自有或公務配發資通訊設備應預設以純文字瀏覽電子郵件，並關閉自動預覽、讀取窗格及自動下載圖片等有潛在風險之功能。<br>5.公務配發資通訊設備建議安裝機關提供之虛擬私人網路（VPN）及虛擬桌面基礎設施 | 一、訂定一般管理措施，依出國前、出國期間及返國後分為三個時間區間，便於公務出國人員參照辦理。<br>二、考量各機關公務出國人員因經費考量常須使用自有設備辦理公務，惟個人自有設備之資安保護措施程度不一，易成資安防護弱點，爰請須以自有設備處理公務，且無法自行完成檢測，需機關設備管理人員協助檢測之公務出國人員簽署安全檢測同意書後，由機關設備管理人員協助公務出國人員施予部分資安管理措施。 |

| | |
|---|---|
| （VDI）等強化連線安全之軟體。<br>6. 公務配發資通訊設備及儲存媒體應備份其所儲存之資料於安全之儲存設備及場所。<br>(二)出國期間<br>1. 倘有連網需求，應使用漫遊上網；當地無提供漫遊服務者，應使用來源可信任之 SIM 卡或 eSIM 服務，且不得連線任何公共場所（包含會議場地及洽公場所）提供之有線及無線網路。<br>2. 於確保可安全連網時，應即時更新各項軟體及防毒軟體病毒碼。<br>3. 公務配發資通訊設備連線公務資通系統及公務雲端資通服務，建議使用 VDI、VPN 或其他適宜之防護措施。<br>4. 與機關進行資料傳遞宜用公務電子郵件傳輸，並應加密機敏資料（如使用壓縮軟體加密或其他適當方式），另以其他安全管道傳遞密碼。<br>5. 避免將公務資料存放於自有儲存媒體、非公務機關配置之雲端儲存空間或未限制存取權限之網路共用資料夾。<br>6. 資通訊設備如有遭駭疑慮，應即關閉設備或關閉對外網路通訊，並通知機關及留存紀錄；若帳密疑似外洩，應立即變更密碼。<br>7. 公務配發資通訊設備及儲存媒體應限於公務使用，並妥善保管；如有遺失或遭竊，應立即通知機關，並記錄遺失或遭竊時間、所遺失或遭竊資通訊設備及儲存媒體、所儲存之資料清單，另評估能否使用端點管理功能清除所遺失資通訊設備上儲存資料。<br>(三)返國後 | |

| | |
|---|---|
| 1. 公務配發資通訊設備及儲存媒體應交予設備管理人員完成資通安全檢測，檢查是否有連線惡意中繼站紀錄或存在惡意程式，並確認連線行為留有稽核軌跡等。<br>2. 公務配發資通訊設備及儲存媒體如發現連線惡意中繼站紀錄或存在惡意程式，設備管理人員應完成稽核紀錄備份，並應保留日誌至少六個月，以備日後事件查察所需，並評估透過格式化或恢復原廠設定等方式清除設備上之所有資料。 | |
| 五、進階管理措施<br>重要人員前往高資安風險地區，有儲存公務資料或用於公務聯絡之需要時，應攜帶機關配發臨時使用且恢復原廠設定（以下簡稱臨時配發）之資通訊設備及儲存媒體；不得攜帶公務配發之資通訊設備及儲存媒體，或存有公務資料，用於公務聯絡之自有資通訊設備及儲存媒體。機關就臨時配發之資通訊設備及儲存媒體，應依前點管理措施辦理且採行下列管理措施，並依附件一檢核一般管理措施及進階管理措施之項目：<br>(一)出國前<br>1. 臨時配發資通訊設備建議安裝端點管理或啟用相關服務。<br>2. 臨時配發資通訊設備應例外開放使用網頁瀏覽無痕模式或其他不儲存瀏覽紀錄、網站資料及表單輸入之模式。<br>3. 行前設立臨時電子郵件及點對點加密功能之通訊軟體（如Signal、Juiker 及 WhatsApp等）帳號，並於公務完成返國後刪除。<br>4. 機敏業務資料應於出境前完成備份並加密儲存（如使用保密設備或利用壓縮軟體加密）。<br>(二)出國期間 | 一、訂定進階管理措施，依出國前、出國期間及返國後分為三個時間區間，訂定進階管理措施，便於重要人員前往高資安風險地區時併同一般管理措施參照辦理。<br>二、進階管理措施係針對攜有高度機敏性資料或具備機敏資料存取權限人員前往高資安風險地區，具高度資安風險，應由機關提供臨時配發設備，且公務出國人員不得攜帶自有或公務配發設備。 |

| | |
|---|---|
| 1.於入境海關期間保持手機關機或啟用飛航模式，以免國際行動用戶識別碼（IMSI）資訊遭竊；各項資通訊產品任何時候都應隨身攜帶，並採用通過安全檢驗之充電裝置，避免以通用序列匯流排（USB）連接任何來路不明資通訊設備或資料儲存媒體，或將連接手機之傳輸線接至不可信任之設備進行充電或檔案移轉。<br>2.臨時配發資通訊設備瀏覽網站時，應使用網頁瀏覽無痕模式或其他不儲存瀏覽紀錄、網站資料及表單輸入之模式。<br>3.與國內支援單位通聯時，宜使用支援點對點加密功能之通訊軟體，且勿使用真實姓名聯繫，並應檢查有無異常登入手機、電子郵件或通訊軟體等情形。<br>4.臨時配發手機應僅儲存當次行程所必要之人員通訊錄。<br>5.所攜機敏業務資料無使用需求後即刪除。<br>6.臨時配發資通訊設備如有遺失或遭竊時，評估能否使用端點管理功能清除所遺失資通訊設備之資料，並將設備恢復原廠設定。<br>(三)返國後：臨時配發之資通訊設備及儲存媒體交由各機關設備管理人員檢測後，除發現連線惡意中繼站紀錄或存在惡意程式情形，須留存證據及保留日誌之情形外，應還原至出廠設定後，重設臨時配發密碼，方可移至他用。 | |
| 六、機關為防護行動裝置相關之資安威脅，對行動裝置之規劃、部署、維運、控制及監督機制導入，可參考國家資通安全研究院發布之「行動裝置資安防護資安參考指引」。 | 說明機關如需參考了解行動裝置之控管機制導入細節，可參考國家資通安全研究院發布之「行動裝置資安防護資安參考指引」。 |

# 第四點、第五點附件一

## 公務出國（含大陸地區、香港及澳門）
## 資通訊設備資通安全檢核表
## （範本）

設備名稱(列舉)：_____

出國期間： 年 月 日至 年 月 日

| 項次 | 分類 | 項目 | 檢核結果 | 例外備註 | 檢核人簽名/檢核日期 |
|---|---|---|---|---|---|
| 出國前 | | | | | |
| 一般管理措施（一般人員及重要人員公務出國） | | | | | |
| 1 | 設備 | 公務配發資通訊設備僅安裝公務需用且為官方合法授權之穩定版本軟體；且不得下載、安裝或使用危害國家資通安全產品。 | □ 是<br>□否 | | |
| 2 | 設備 | 公務配發資通訊設備應確實套用政府組態基準（Government Configuration Baseline, GCB）或機關自訂之組態基準，並記錄例外項目。 | □ 是<br>□否 | | |
| 3 | 設備 | 公務配發資通訊設備應安裝防毒軟體並確認病毒碼更新至最新版，並執行全機掃描；確認資通訊設備之作業系統及各項軟體更新至最新穩定版本，勿使用已停止更新版本。 | □ 是<br>□否 | | |
| 4 | 設備 | 自有或公務配發資通訊設備應預設以純文字瀏覽電子郵件，並關閉自動預覽、讀取窗格及自動下載圖片等有潛在風險之功能。 | □ 是<br>□否 | | |

| | | | | | |
|---|---|---|---|---|---|
| 5 | 設備 | 公務配發資通訊設備建議安裝機關提供之虛擬私人網路（VPN）及虛擬桌面基礎設施（VDI）等強化連線安全之軟體。 | □ 是<br>□否 | | |
| 6 | 資料 | 公務配發資通訊設備及儲存媒體應備份其所儲存之資料於安全之儲存設備及場所。 | □ 是<br>□否 | | |
| 進階管理措施（重要人員前往高資安風險地區） | | | | | |
| 7 | 設備 | 臨時配發資通訊設備建議安裝端點管理或啟用相關服務。 | □ 是<br>□否 | | |
| 8 | 設備 | 臨時配發資通訊設備應例外開放使用網頁瀏覽無痕模式或其他不儲存瀏覽紀錄、網站資料及表單輸入之模式。 | □ 是<br>□否 | | |
| 9 | 資料 | 行前設立臨時電子郵件及點對點加密功能之通訊軟體（如 Signal、Juiker 及 WhatsApp 等）帳號，並於公務完成返國後刪除。 | □ 是<br>□否 | | |
| 10 | 資料 | 機敏業務資料應於出境前完成備份並加密儲存（如使用保密設備或利用壓縮軟體加密）。 | □ 是<br>□否 | | |
| 出國期間 | | | | | |
| 一般管理措施（一般人員及重要人員公務出國） | | | | | |
| 11 | 通訊 | 倘有連網需求，應使用漫遊上網；當地無提供漫遊服務者，應使用來源可信任之 SIM 卡或 eSIM 服務，且不得連線任何公共場所（包含會議場地及洽公場所）提供之有線及無線網路。 | □ 是<br>□否 | | |
| 12 | 設備 | 於確保可安全連網時，應即時更新各項軟體及防毒軟體病毒碼。 | □ 是<br>□否 | | |
| 13 | 通訊 | 公務配發資通訊設備連線公務資通系統及公務雲端資通服務，建議使用 VDI、 | □ 是<br>□否 | | |

| | | | | | |
|---|---|---|---|---|---|
| | | VPN 或其他適宜之防護措施。 | | | |
| 14 | 通訊 | 與機關進行資料傳遞宜用公務電子郵件傳輸，並應加密機敏資料（如使用壓縮軟體加密或其他適當方式），另以其他安全管道傳遞密碼。 | □ 是<br>□否 | | |
| 15 | 資料 | 避免將公務資料存放於自有儲存媒體、非公務機關配置之雲端儲存空間或未限制存取權限之網路共用資料夾。 | □ 是<br>□否 | | |
| 16 | 通訊 | 資通訊設備如有遭駭疑慮，應即關閉設備或關閉對外網路通訊，並通知機關及留存紀錄；若帳密疑似外洩，應立即變更密碼。 | □ 是<br>□否 | | |
| 17 | 資料 | 公務配發資通訊設備及儲存媒體應限於公務使用，並妥善保管；如有遺失或遭竊，應立即通知機關，並記錄遺失或遭竊時間、所遺失或遭竊資通訊設備及儲存媒體、所儲存之資料清單，另評估能否使用端點管理功能清除所遺失資通訊設備上儲存資料。 | □ 是<br>□否 | | |
| 進階管理措施（重要人員前往高資安風險地區） | | | | | |
| 18 | 使用 | 於入境海關期間保持手機關機或啟用飛航模式，以免國際行動用戶識別碼（IMSI）資訊遭竊；各項資通訊產品任何時候都應隨身攜帶，並採用通過安全檢驗之充電裝置，避免以通用序列匯流排（USB）連接任何來路不明資通訊設備或資料儲存媒體，或將連接手機之傳輸線接至不可信任之設備進行充電或檔案移轉。 | □ 是<br>□否 | | |
| 19 | 使用 | 臨時配發資通訊設備瀏覽網站時，應使用網頁瀏覽無痕模式或其他不儲存瀏覽 | □ 是<br>□否 | | |

| | | | | | |
|---|---|---|---|---|---|
| | | 紀錄、網站資料及表單輸入之模式。 | | | |
| 20 | 通訊 | 與國內支援單位通聯時，宜使用支援點對點加密功能之通訊軟體，並勿使用真實姓名聯繫；及檢查有無異常登入手機、電子郵件或通訊軟體等情形。 | □ 是<br>□否 | | |
| 21 | 資料 | 臨時配發手機應僅儲存當次行程所必要之人員通訊錄。 | □ 是<br>□否 | | |
| 22 | 資料 | 所攜機敏業務資料無使用需求後即刪除。 | □ 是<br>□否 | | |
| 23 | 資料 | 臨時配發資通訊設備如有遺失或遭竊時，評估能否使用端點管理功能清除所遺失資通訊設備之資料，並將設備恢復原廠設定。 | □ 是<br>□否 | | |
| 返國後 | | | | | |
| 一般管理措施（一般人員及重要人員公務出國） | | | | | |
| 24 | 檢測 | 公務配發資通訊設備及儲存媒體應交予設備管理人員完成資通安全檢測，檢查是否有連線惡意中繼站紀錄或存在惡意程式，並確認連線行為留有稽核軌跡等。 | □ 是<br>□否 | | |
| 25 | 檢測 | 公務配發資通訊設備及儲存媒體如發現連線惡意中繼站紀錄或存在惡意程式，設備管理人員應完成稽核紀錄備份，並應保留日誌至少六個月，以備日後事件查察所需，並評估透過格式化或恢復原廠設定等方式清除設備上之所有資料。 | □ 是<br>□否 | | |
| 進階管理措施（重要人員前往高資安風險地區） | | | | | |
| 26 | 還原 | 臨時配發之資通訊設備及儲存媒體交由各機關設備管理人員檢測後，除發現連線惡意中繼站紀錄或存在惡意程式情形，需留存證據及保留日誌之情形外， | □ 是<br>□否 | | |

| | | | | | |
|---|---|---|---|---|---|
| | | 應還原至出廠設定後，重設臨時配發密碼，方可移至他用。 | | | |

備註：

1、 不論使用機關提供或自有設備，有辦理公務需求之設備請依本表進行整備及使用，機關得依其業務性質或其它資安要求，增列各檢核項目。

2、 本表之檢核方式：

- 出國前：
  - ■ 公務配發及臨時配發之資通訊設備及儲存媒體：由機關設備管理人員完成資通安全檢測後，就出國前項目勾選並簽名。
  - ■ 自有資通訊設備及儲存媒體：
    (1) 公務出國人員可自行完成檢測者，由其依檢核項目完成檢測、勾選並簽名；機關設備管理人員確認後簽名。
    (2) 公務出國人員無法自行完成檢測者，於簽署「公務出國（含大陸地區、香港及澳門）自有資通訊設備及儲存媒體資通安全檢測同意書」後，由機關設備管理人員協助完成檢測，並由雙方就出國前項目勾選及簽名。
- 出國期間：由公務出國人員攜帶本表，就出國期間項目勾選並簽名。
- 返國後：由機關設備管理人員檢測公務出國人員公務配發及臨時配發之資通訊設備及儲存媒體，並還原臨時配發之資通訊設備設定後，勾選、簽名，並將本表留存於設備管理單位備查。

訂定說明：

一、為利機關設備管理人員及公務出國人員依本須知落實管理措施，依本須知第四點及第五點訂定檢核表範本，機關得依其業務性質或其他資安要求彈性增列各檢核項目，俾利貼合實務所需調整。

二、檢核表依出國前、出國期間及返國後分為三個時間區間，出國前之檢核項目，公務配發及臨時配發設備由機關設備管理人員檢測後簽名，自有設備如公務出國人員可自行完成檢測，則由公務出國人員完成檢測及簽名後，提供檢測完成證明予機關設備管理人員確認後簽名；如公務出國人員無法自行完成檢測，需機關設備管理人員協助者，由機關設備管理人員協助公務出國人員完成檢測，並由雙方簽名。出國期間之檢核項目由公務出國人員攜帶並依檢核項目，返國後由機關設備管理人員依檢核項目檢測及還原後簽名，並留存於設備管理單位備查。

三、如遇設備本身限制或其他特殊因素導致無法依檢核項目實施者，應於例外備註欄說明其緣由，並確認所述緣由之合理性。

# 第四點附件二

## 公務出國（含大陸地區、香港及澳門）自有資通訊設備及儲存媒體資通安全檢測同意書

茲緣於簽署人 ＿＿＿＿＿＿（簽署人姓名，以下稱簽署人）於＿年＿月＿日至＿年＿月＿日因公務出國，期間須攜帶存有公務資料或用於公務聯絡之自有資通訊設備及儲存媒體：＿＿＿＿＿＿（以下稱「自有設備」），為防止公務機密資料遭竊取、竄改、毀損、滅失或洩漏，影響其機密性、完整性及可用性，簽署人同意前揭自有設備依《公務出國（含大陸地區、香港及澳門）資通訊設備管理須知》檢核事項，於出國前提供機關設備管理人員檢測。

簽署人姓名及簽章：

身分證字號(末4碼免填)：＿＿＿＿＿＿○○○○

中　華　民　國　　年　　月　　日

訂定說明：依國家機密保護法、文書處理手冊、公務員服務法第 5 條第 1 項及刑法第 132 條，公務員對政府機關（構）之機密，負有保密義務；惟公務出國人員為公務攜帶存有公務資料、用於公務聯絡之自有資通訊設備及儲存媒體，屬該員之私有財產，為兼顧公務機密資料保護與公務出國人員財產權利，爰增列當事人同意之要件，於公務出國人員簽署本同意書後方得依本須知管理措施檢核自有資通訊設備及儲存媒體。