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

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 □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 □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 □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 □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 □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 □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 □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 □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 □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 □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 □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 □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、VPN 或其他適宜之防護措施。	□是 □否		
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	□是 □否		

		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。			
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 □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 □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 □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 □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紀錄、網站資料及表單輸入之模式。	□是 □否		

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 □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 □否		
22	資料	所攜機敏業務資料無使用需求後即刪除。	□是 □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 □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 □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 □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	□是 □否		

		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。			

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。