

經濟部國際貿易署員工資通安全作業規定修正對照表

修正規定	現行規定	說明
一、經濟部國際貿易署（以下簡稱本署）為健全資通安全環境，強化本署人員資通安全程度及認知，防止人為疏失、蓄意破壞或機密資料外洩等情事發生，確保本署電腦設備、資料、系統及網路安全，特訂定本規定。	一、經濟部國際貿易署（以下簡稱本署）為健全資通安全環境，強化本署人員資通安全程度及認知，防止人為疏失、蓄意破壞或機密資料外洩等情事發生，確保本署電腦設備、資料、系統及網路安全，特訂定本規定。	本點未修正。
二、本規定主要為規範本署公務作業相關資通安全責任，俾落實執行。	二、本規定主要為規範本署公務作業相關資通安全責任，俾落實執行。	本點未修正。
三、辦公環境安全規定 （一）重要文件及其儲存媒體（紙張、隨身碟、磁片、光碟片等）應適當保管。 （二）不用之紙張文件或報表應採取適當之程序加以銷毀或廢棄。 （三）資訊設備於無人看管或下班時採取適當之防護措施。	三、辦公環境安全規定 （一）重要文件及其儲存媒體（紙張、隨身碟、磁片、光碟片等）應適當保管。 （二）不用之紙張文件或報表應採取適當的程序加以銷毀或廢棄。 （三）資訊設備於無人看管或下班時採取適當之防護措施。	一、序文、第一款及第三款未修正。 二、酌作第二款文字修正。
四、密碼管理規定 （一）密碼長度至少十二碼，採英文字母、數字、特殊符號混合使用之原則，並應妥善保管，不得外洩。 （二）密碼應至少每九十天更換一次，且三代不得重覆。 （三）啟用螢幕保護功能，時間至少十五分鐘，並設定密碼。 （四）署內之連網電腦需登入網域（DMBOFT），統一套用密碼規定；其他電腦需自行設定Windows密碼，並符合上述密碼規定。 （五）網際網路瀏覽器不得啟用自動記憶帳號及密碼之功能。	四、密碼管理規定 （一）密碼長度至少十二碼，採英文字母、數字、特殊符號混合使用之原則，並應妥善保管，不得外洩。 （二）密碼應至少每九十天更換一次，且三代不得重覆。 （三）啟用螢幕保護功能，時間至少十五分鐘，並設定密碼。 （四）署內之連網電腦需登入網域（DMBOFT），統一套用密碼規定；其他電腦需自行設定Windows密碼，並符合上述密碼規定。 （五）網際網路瀏覽器不得啟用自動記憶帳號及密碼之功能。	本點未修正。
五、網際網路管理規定	五、網際網路管理規定	一、序文、第二款至第八款及

<p>(一)不得使用 P2P (Peer-to-Peer) 檔案分享程式、抓檔軟體、續傳軟體等或利用電子郵件服務進行任何可能對網路正常傳輸造成不利影響之行為。</p> <p>(二)連網電腦禁止瀏覽非法或本署所限制之網站，例如：社交網站、色情網站、線上遊戲網站、賭博網站、直播網站及拍賣網。</p> <p>(三)機密資料及文件須以權責主管機關認可之加密機制加密後始得在網際網路上傳送。機密資料及文件以外之敏感性或個人隱私資料，應予以加密，始得傳送。</p> <p>(四)個人私用之電子郵件不得傳送公文或作為公務連絡。</p> <p>(五)郵件瀏覽器須關閉郵件預覽之功能。</p> <p>(六)不隨意回覆或打開不明郵件。</p> <p>(七)在署辦公者，電腦應避免二十四小時開機，不使用時即關機或離線。居家辦公者仍應注意電腦使用情況，暫時離開時應登出電腦，長期不使用時應關機。</p> <p>(八)本署員工（含臨時人員）、委外駐點人員非經核准，一律禁止攜入非本署之個人電腦、筆記型電腦、網路設備及其他具備連線本署區域網路能力之設備。</p> <p>(九)外賓携入之電腦不得連接本署有線區域網路。<u>如有使用本署無線網路需要時，應向無線網路管理人員取</u></p>	<p>(一)不得使用 P2P (Peer-to-Peer) 檔案分享程式、抓檔軟體、續傳軟體等或利用電子郵件服務進行任何可能對網路正常傳輸造成不利影響之行為。</p> <p>(二)連網電腦禁止瀏覽非法或本署所限制之網站，例如：社交網站、色情網站、線上遊戲網站、賭博網站、直播網站及拍賣網。</p> <p>(三)機密資料及文件須以權責主管機關認可之加密機制加密後始得在網際網路上傳送。機密資料及文件以外之敏感性或個人隱私資料，應予以加密，始得傳送。</p> <p>(四)個人私用之電子郵件不得傳送公文或作為公務連絡。</p> <p>(五)郵件瀏覽器須關閉郵件預覽之功能。</p> <p>(六)不隨意回覆或打開不明郵件。</p> <p>(七)在署辦公者，電腦應避免二十四小時開機，不使用時即關機或離線。居家辦公者仍應注意電腦使用情況，暫時離開時應登出電腦，長期不使用時應關機。</p> <p>(八)本署員工（含臨時人員）、委外駐點人員非經核准，一律禁止攜入非本署之個人電腦、筆記型電腦、網路設備及其他具備連線本署區域網路能力之設備。</p> <p>(九)外賓携入之電腦不得連接本署有線區域網路，但得使用本署無線網路。使用無線網路前須填寫「無線網</p>	<p>第十款至第十四款未修正。</p> <p>二、酌作第一款文字修正。</p> <p>三、第九款修正。配合實務，修正本署外賓無線網路使用規定。</p>
---	--	---

<p>得帳號及密碼後始得登入使用。</p> <p>(十)禁止在本署區域網路內任何電腦上使用行動網路及任何無線網路。</p> <p>(十一)為執行職務(如負責為民服務事項)或瞭解民意、推動政策等需要，上網連結本署所限制之網站(如 Facebook、PTT、YouTube)或使用雲端硬碟，及安裝 Juiker 以外之即時通訊軟體，應提出申請，經單位主管同意，始得使用。</p> <p>(十二)為執行公務需要，限科長級以上主管，始得使用全署群組帳號發送電子郵件予全署同仁。</p> <p>(十三)使用本署區域網路以公務需求為原則，並應遵守上述相關規定；非上班時間更應提高警覺，以避免資安事件發生。</p> <p>(十四)公務之電子郵件不得用來註冊電商網站、社交軟(媒)體等非公務用之帳號。</p>	<p>路使用登記表」，並經本署承辦人簽名後，取得使用帳號和密碼。</p> <p>(十)禁止在本署區域網路內任何電腦上使用行動網路及任何無線網路。</p> <p>(十一)為執行職務(如負責為民服務事項)或瞭解民意、推動政策等需要，上網連結本署所限制之網站(如 Facebook、PTT、YouTube)或使用雲端硬碟，及安裝 Juiker 以外之即時通訊軟體，應提出申請，經單位主管同意，始得使用。</p> <p>(十二)為執行公務需要，限科長級以上主管，始得使用全署群組帳號發送電子郵件予全署同仁。</p> <p>(十三)使用本署區域網路以公務需求為原則，並應遵守上述相關規定；非上班時間更應提高警覺，以避免資安事件發生。</p> <p>(十四)公務之電子郵件不得用來註冊電商網站、社交軟(媒)體等非公務用之帳號。</p>	
<p>六、實體隔離規定</p> <p>(一)隔離電腦指非連接任何網路之電腦(單機使用)，應張貼明顯之識別標籤；連網電腦指連接網際網路，供上網瀏覽資訊或收發電子郵件之電腦，兩者不得混用。</p> <p>(二)隔離印表機指連接於隔離電腦或隔離電腦</p>	<p>六、實體隔離規定</p> <p>(一)隔離電腦指非連接任何網路之電腦(單機使用)，應張貼明顯之識別標籤；連網電腦指連接網際網路，供上網瀏覽資訊或收發電子郵件之電腦，兩者不得混用。</p> <p>(二)隔離印表機指連接於隔離電腦或隔離電腦</p>	<p>本點未修正。</p>

<p>串接區域之印表機，不得同時連接於網路。</p> <p>(三)隔離電腦與連網電腦不得共用印表機。</p> <p>(四)機密公文及敏感性資料須於隔離電腦、隔離印表機製作或列印；發文作業則依文書處理作業規定辦理。</p> <p>(五)隔離電腦變更用途為連網電腦或連網電腦變更用途為隔離電腦時，須填具資訊作業需求單，由資訊室將電腦重新格式化、重新安裝作業系統。</p> <p>(六)禁止將行動裝置連接於本署電腦充電。</p>	<p>串接區域之印表機，不得同時連接於網路。</p> <p>(三)隔離電腦與連網電腦不得共用印表機。</p> <p>(四)機密公文及敏感性資料須於隔離電腦、隔離印表機製作或列印；發文作業則依文書處理作業規定辦理。</p> <p>(五)隔離電腦變更用途為連網電腦或連網電腦變更用途為隔離電腦時，須填具資訊作業需求單，由資訊室將電腦重新格式化、重新安裝作業系統。</p> <p>(六)禁止將行動裝置連接於本署電腦充電。</p>	
<p>七、筆記型電腦安全性規定</p> <p>(一)公務用筆記型電腦每月須送回資訊室進行安全性檢查。</p> <p>(二)公務用筆記型電腦如曾連接署外網路，於連接本署有線區域網路前，須送回資訊室檢查。</p> <p>(三)公務用筆記型電腦有中毒疑慮或受其他資訊安全威脅時，應將電腦送回資訊室處理。</p> <p>(四)公務相關資料勿存放於筆記型電腦，應備份於其它儲存媒體。</p> <p>(五)使用筆記型電腦應符合密碼管理規定。</p>	<p>七、筆記型電腦安全性規定</p> <p>(一)公務用筆記型電腦每月須送回資訊室進行安全性檢查。</p> <p>(二)公務用筆記型電腦如曾連接署外網路，於連接本署有線區域網路前，須送回資訊室檢查。</p> <p>(三)公務用筆記型電腦有中毒疑慮或受其他資訊安全威脅時，應將電腦送回資訊室處理。</p> <p>(四)公務相關資料勿存放於筆記型電腦，應備份於其它儲存媒體。</p> <p>(五)使用筆記型電腦應符合密碼管理規定。</p>	<p>本點未修正。</p>
<p>八、公務用隨身碟使用及管理規定</p> <p>(一)公務用隨身碟分類</p> <ol style="list-style-type: none"> 1. 加密隨身碟：貼有黃色標籤，有安裝加密機制，設定密碼保護。 2. 一般隨身碟：貼有白色標籤，得使用於連網電腦，或作為連網電腦與隔離 		<p>一、<u>本點新增</u>。</p> <p>二、依本署一百十二年資通安全管理委員會會議決議辦理。</p>

<p>電腦資料（病毒碼、網路下載參考資料等）交換用。</p> <p>(二)使用及管理</p> <ol style="list-style-type: none"> 1. 加密隨身碟禁止使用於連網電腦。 2. 隨身碟若需連接本署設備或網路時，應先進行電腦病毒掃描，確認無問題後始可使用。 3. 隨身碟如為機關內共同使用，使用者應在使用完畢後將所有之資料文件移除，以免資料遭他人誤用。 4. 非公務需求不得將載有機密、敏感性資料之加密隨身碟攜出辦公場所。 5. 含機密、敏感性資料之加密隨身碟遞送，應以密件及密封袋方式傳送。 6. 隨身碟超過使用年限應繳回並由資訊室辦理銷毀，含機敏性資料之儲存媒體應消磁或格式化，必要時採取實體破壞。 7. 本署人員如有單位異動、離職等情形，應向所在單位之窗口繳回隨身碟，並由窗口人員隨時更新各單位公務用隨身碟清冊。 8. 本署公務隨身碟領用、繳回、庫存量控制、窗口維護等資料，應納入物品領用系統。 		
<p><u>九</u>、軟體使用規定</p> <p>(一)授權軟體是指具合法版權，且經主管同意使用於公務之軟體；其餘均為非授權軟體</p>	<p>八、軟體使用規定</p> <p>(一)授權軟體是指具合法版權，且經主管同意使用於公務之軟體；其餘均為非授權軟體</p>	<p>一、點次變更。</p> <p>二、序文、第一款、第三款及第四款未修正。</p> <p>三、酌作第二款及第五款文字修正。</p>

<p>。</p> <p>(二)禁止下載或使用非授權軟體。各單位主管應善加督導，並視個案情形由資訊室會同政風室處理。</p> <p>(三)禁止安裝任何非法、來路不明或資安主管機關明文禁止之軟體，例如：P2P 軟體。因業務需求申請安裝之軟體，須經單位主管核准。</p> <p>(四)本署個人電腦之授權軟體由資訊室統一安裝。</p> <p>(五)登入網域之電腦即能自動更新修補 Windows、Office 漏洞及防毒程式病毒碼，其他公務用電腦應洽資訊室處理。</p>	<p>。</p> <p>(二)禁止下載或使用非授權軟體；請各單位主管善加督導，並視個案情形由資訊室會同政風室處理。</p> <p>(三)禁止安裝任何非法、來路不明或資安主管機關明文禁止之軟體，例如：P2P 軟體。因業務需求申請安裝之軟體，須經單位主管核准。</p> <p>(四)本署個人電腦之授權軟體由資訊室統一安裝。</p> <p>(五)登入網域之電腦即能自動更新修補 Windows、Office 漏洞及防毒程式病毒碼，其他公務用電腦請洽資訊室處理。</p>	
<p><u>十</u>、資料保護規定</p> <p>(一)各單位應列出機密及敏感資料要項，俾便同仁遵循。</p> <p>(二)機密性或敏感性資料，須儲存於專用之光碟、磁片、加密硬碟或隨身碟，且禁止使用於連網電腦。</p> <p>(三)本署人員離職前將電腦中之資料備份後，應將電腦交回資訊室，由資訊室將電腦格式化、重新安裝作業系統。</p> <p>(四)禁止在家中等使用連網電腦處理機密性或敏感性公務。</p> <p>(五)禁止使用網路芳鄰共享資料夾（連網之電腦已統一套用本規定）。</p> <p>(六)各項重要資料，均應做妥善之資料備份，並定期測試備份資料，以確保備份資料之可用性。</p>	<p><u>九</u>、資料保護規定</p> <p>(一)各單位應列出機密及敏感資料要項，俾便同仁遵循。</p> <p>(二)機密性或敏感性資料，須儲存於專用之光碟、磁片、加密硬碟或隨身碟，且禁止使用於連網電腦。</p> <p>(三)人員離職前須將電腦中之資料備份後，將電腦交回資訊室，由資訊室將電腦格式化、重新安裝作業系統。</p> <p>(四)禁止在家中等使用連網電腦處理機密性或敏感性公務。</p> <p>(五)禁止使用網路芳鄰共享資料夾（登入網域之電腦已統一套用本規定）。</p> <p>(六)各項重要資料，均應做妥善之資料備份，並定期測試備份資料，以確保備份資料之可用性。</p>	<p>一、點次變更。</p> <p>二、序文、第一款、第二款、第四款及第六款至第九款未修正。</p> <p>三、酌作第三款及第五款文字修正。</p>

<p>(七)落實印表管制，一般公文或報表資料應於各單位之印表機、無法對外連線之影印機或封閉傳真功能且無法對外連線之多功能事務機列印，特殊情況得將資料交資訊室列印。</p> <p>(八)機密及敏感資料載具（光碟、磁片、外接式硬碟等）之銷毀，須填具資訊作業需求單，由申請人會同資訊室、政風室、秘書室等有關人員共同銷毀。</p> <p>(九)資訊室每年定期以軟體工具清查同仁連網電腦疑似個人資料檔案，同仁應於Intranet查詢該等檔案之檔案名稱及儲存路徑；單位主管應負責督導同仁，將含有個人資料之檔案移除或加密。</p>	<p>(七)落實印表管制，一般公文或報表資料應於各單位之印表機、無法對外連線之影印機或封閉傳真功能且無法對外連線之多功能事務機列印，特殊情況得將資料交資訊室列印。</p> <p>(八)機密及敏感資料載具（光碟、磁片、外接式硬碟等）之銷毀，須填具資訊作業需求單，由申請人會同資訊室、政風室、秘書室等有關人員共同銷毀。</p> <p>(九)資訊室每年定期以軟體工具清查同仁連網電腦疑似個人資料檔案，同仁應於Intranet查詢該等檔案之檔案名稱及儲存路徑；單位主管應負責督導同仁，將含有個人資料之檔案移除或加密。</p>	
<p><u>十一</u>、社交工程防範規定</p> <p>(一)接獲非經常往來長官、朋友或廠商之電子郵件，宜謹慎處理。</p> <p>(二)非職務必要，應避免回應外部人員有關公務之任何詢問。</p> <p>(三)遭遇恐嚇、脅迫或任何疑似詐騙之行為時，應保持冷靜，不任意接受妥協，並儘速通報相關單位</p> <p>(四)不可將密碼隨意抄錄放置，在任何情況下不可將密碼告知他人，包括長官及資訊室人員。</p> <p>(五)本署或其他上級機關電子郵件社交工</p>	<p>十、社交工程防範規定</p> <p>(一)接獲非經常往來長官、朋友或廠商之電子郵件，宜謹慎處理。</p> <p>(二)非職務必要，應避免回應外部人員有關公務之任何詢問。</p> <p>(三)遭遇恐嚇、脅迫或任何疑似詐騙之行為時，應保持冷靜，不任意接受妥協，並儘速通報相關單位</p> <p>(四)不可將密碼隨意抄錄放置，在任何情況下不可將密碼告知他人，包括長官及資訊室人員。</p> <p>(五)本署或其他上級機關電子郵件社交工程演練結果不合格者，由資訊室簽陳署長後公布於Intranet。</p>	<p>點次變更，內容未修正。</p>

<p>程演練結果不合格者，由資訊室簽陳署長後公布於 Intranet。</p> <p>(六)開啟或點閱真實社交惡意電子郵件，且造成資訊安全事件者，由資訊室簽陳署長後公布於 Intranet。</p> <p>(七)前二款發生次數每年累計超過三次以上之同仁名單將送人事室提交年度考績委員會參考。</p>	<p>(六)開啟或點閱真實社交惡意電子郵件，且造成資訊安全事件者，由資訊室簽陳署長後公布於 Intranet。</p> <p>(七)前二款發生次數每年累計超過三次以上之同仁名單將送人事室提交年度考績委員會參考。</p>	
<p><u>十二</u>、帳號管理規範、人員訓練</p> <p>(一)使用本署區域網路資源（含個人電腦），須填具申請單，經核可後取得「一般使用者」帳號授權。如為公務特殊需用，得經核准調整授權；離職時須依規定辦理離職手續，立即取消授權帳號。</p> <p>(二)使用本署網路資源之人員，均須遵守本規定。</p> <p>(三)本署<u>人員</u>每年應接受至少三小時之資安通識教育訓練課程。</p>	<p>十一、帳號管理規範、人員訓練</p> <p>(一)使用本署區域網路資源（含個人電腦），須填具申請單，經核可後取得「一般使用者」帳號授權。如為公務特殊需用，得經核准調整授權；離職時須依規定辦理離職手續，立即取消授權帳號。</p> <p>(二)使用本署網路資源之人員，均須遵守本規定。</p> <p>(三)本署同仁每年應接受至少三小時的資安通識教育訓練課程。</p>	<p>一、點次變更。</p> <p>二、序文、第一款及第二款未修正。</p> <p>三、酌作第三款文字修正。</p>
<p><u>十三</u>、資通安全使用管理稽核</p> <p>(一)依據資通安全管理法、相關法令及本署資通安全稽核計畫辦理。</p> <p>(二)由政風室會同資訊室及相關單位進行定期或不定期資訊安全稽核作業，如有違反規定者，依相關規定辦理。</p>	<p>十二、資通安全使用管理稽核</p> <p>(一)依據資通安全管理法、相關法令及本署資通安全稽核計畫辦理。</p> <p>(二)由政風室會同資訊室及相關單位進行定期或不定期資訊安全稽核作業，如有違反規定者，依相關規定辦理。</p>	<p>點次變更，內容未修正。</p>