

經濟部資通安全須知修正對照表

修 正 規 定	現 行 規 定	說 明
一、為健全本部資通安全環境，強化人員（含駐點外包人員）資通安全認知，防止因人為疏失而導致機敏資料外洩等情事發生，以確保各單位電腦、資料、系統及網路安全，特訂定本須知。	一、為健全本部資通安全環境，強化人員（含駐點外包人員）資通安全認知，防止因人為疏失而導致機敏資料外洩等情事發生，以確保各單位電腦、資料、系統及網路安全，特訂定本須知。	本點未修正。
<p>二、實體隔離作業須知</p> <p>（一）處理密級以上或各單位認定需保護之敏感性資料（以下簡稱機敏資料）時，須使用專屬實體隔離電腦設備處理及列印。</p> <p>（二）儲存機敏資料之<u>可攜式</u>儲存媒體須上鎖保管，並僅限於實體隔離電腦讀取、繕打及列印。</p> <p>（三）實體隔離電腦不得私自連接網路並不得與上網電腦共用印表機。</p> <p>（四）實體隔離電腦製妥之文件如需網路傳輸或從連網電腦下載文件複製至隔離電腦使用時，須先將文件複製至<u>可攜式</u>儲存媒體，再移至目的電腦。此等儲存媒體僅當作兩部電腦間檔案傳送之「載具」，使用前、後應以格式化方式刪除所有檔案。</p>	<p>二、實體隔離作業須知</p> <p>（一）處理密級以上或各單位認定需保護之敏感性資料（以下簡稱機敏資料）時，須使用專屬實體隔離電腦設備處理及列印。</p> <p>（二）儲存機敏資料之<u>專屬隨身碟、磁片等</u>儲存媒體須上鎖保管，並僅限於實體隔離電腦讀取、繕打及列印。</p> <p>（三）實體隔離電腦不得私自連接網路並不得與上網電腦共用印表機。</p> <p>（四）實體隔離電腦製妥之文件如需網路傳輸或從連網電腦下載文件複製至隔離電腦使用時，須先將文件複製至<u>隨身碟、磁片等</u>儲存媒體，再移至目的電腦。此等儲存媒體僅當作兩部電腦間檔案傳送之「載具」，使用前、後應以格式化方式刪除所有檔案。</p>	因實務上使用之儲存媒體類別多元，不限於特定儲存媒體，爰修正第二款及第四款儲存媒體類型。
<p>三、資料保護須知</p> <p>（一）機敏資料須加密，</p>	<p>三、資料保護須知</p> <p>（一）機敏資料須加密<u>後</u></p>	一、第一款規範重點在於機敏資料不

<p><u>且</u>不可存放於連網電腦。</p> <p>(二) 密級以上資料須以國安單位認可之加密機制於實體隔離電腦加密後，方可透過網路傳送。</p> <p>(三) 敏感性資料須於實體隔離電腦設定密碼保護功能或加密後，方可透過網路傳送。</p> <p>(四) <u>公務個人電腦</u>密碼長度至少須十二碼（採文數字、特殊符號混合使用原則）且不得採用電腦自動記憶方式、明文書寫、張貼或交予他人使用。</p> <p>(五) 使用<u>可攜式儲存媒體</u>存放資料時，機敏資料及一般資料應分開儲存，不得混用並妥善保管。</p> <p>(六) 禁止在家中、<u>公共場合</u>等辦公室以外場所使用連網電腦處理機敏公務。</p> <p>(七) 各項重要業務資料均應妥善定期備份，並經檢視以確保備份資料之可用性。</p>	<p><u>儲存於實體隔離電腦、隨身碟或磁片等</u>，不可存放於連網電腦。</p> <p>(二) 密級以上資料須以國安單位認可之加密機制於實體隔離電腦加密後，方可透過網路傳送。</p> <p>(三) 敏感性資料須於實體隔離電腦<u>啟動其編輯軟體</u>設定密碼保護功能或加密後，方可透過網路傳送。</p> <p>(四) 密碼長度至少須十二碼（採文數字、特殊符號混合使用原則）且不得採用電腦自動記憶方式、明文書寫、張貼或交予他人使用。</p> <p>(五) 使用<u>隨身碟或磁片等</u>存放資料時，機敏資料及一般資料應分開儲存，不得混用並妥善保管。</p> <p>(六) 禁止在家中等辦公室以外場所使用連網電腦處理機敏公務。</p> <p>(七) 各項重要業務資料均應妥善定期備份，並經檢視以確保備份資料之可用性。</p>	<p>可存放於連網電腦，且儲存媒體類別多元，爰刪除相關描述。</p> <p>二、設定密碼方式多元，不局限於單一形式，爰刪除第三款相關描述。</p> <p>三、密碼規範主要用於公務個人電腦，爰修正第四款。</p> <p>四、因實務上使用之儲存媒體類別多元，不限於特定儲存媒體，爰修正第五款儲存媒體類型。</p> <p>五、因辦公室以外場所不限於住家，爰於第六款增列公共場合。</p>
<p>四、網際網路使用須知</p> <p>(一) 連網電腦禁止<u>瀏覽非法或本部所限制</u>之網站。</p> <p>(二) 禁止於辦公室內私裝電腦及網路通訊等相關設備。</p> <p>(三) 因業務特性須上網瀏覽大陸網站者，須經單位主管核可</p>	<p>四、網際網路使用須知</p> <p>(一) 連網電腦禁止<u>覽瀏</u>非法或<u>不當</u>之網站。</p> <p>(二) 禁止於辦公室內私裝電腦及網路通訊等相關設備。</p> <p>(三) 因業務特性須上網瀏覽大陸網站者，須經單位主管核可</p>	<p>一、不當之網站用語較不明確，爰修正第一款部分文字。</p> <p>二、配合本部組織改造，修正第三款幕僚單位名稱。</p>

<p>後，向本部資訊<u>處</u>提出申請後使用。</p> <p>(四) 機敏場所如非業務需要，禁止安裝網路攝影機等視訊會議設備。</p>	<p>後，向本部資訊<u>中心</u>提出申請後使用。</p> <p>(四) 機敏場所如非業務需要，禁止安裝網路攝影機等視訊會議設備。</p>	
<p>五、電腦使用須知</p> <p>(一) 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。</p> <p>(二) 電腦若疑似受駭時，應立即拔除網路線，停止連網行為並向本部熱線服務通報。</p> <p>(三) 受駭電腦重整後，應立即變更曾於該受駭電腦登入之所有系統密碼（如部內服務網、電子郵件系統、自然人憑證等）。</p> <p>(四) 禁止私自安裝未經合法授權軟體。</p> <p>(五) 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。</p> <p>(六) 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。</p> <p>(七) 下班時應關閉電腦及螢幕電源。</p> <p>(八) 如發現資安問題，請主動向本部熱線服務通報。</p>	<p>五、電腦使用須知</p> <p>(一) 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。</p> <p>(二) 電腦若疑似受駭時，應立即拔除網路線，停止連網行為並向本部熱線服務通報。</p> <p>(三) 受駭電腦重整後，應立即變更曾於該受駭電腦登入之所有系統密碼（如部內服務網、電子郵件系統、自然人憑證等）。</p> <p>(四) 禁止私自安裝<u>點對點檔案分享軟體</u>（Peer-to-Peer，簡稱 P2P）及未經合法授權軟體。</p> <p>(五) 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。</p> <p>(六) 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。</p> <p>(七) 下班時應關閉電腦及螢幕電源。</p> <p>(八) 如發現資安問題，請主動向本部熱線</p>	<p>未授權軟體不限於點對點檔案分享軟體，爰刪除第四款相關描述。</p>

	服務通報。	
<p>六、具上網功能行動裝置使用須知</p> <p>(一) 行動裝置必須使用專用電源，不得接觸公務<u>個人</u>電腦USB接口。</p> <p>(二) 公務<u>個人</u>電腦不得透過行動裝置連網。</p> <p>(三) 不得修改或破解公務<u>配發</u>行動裝置之安全措施。</p> <p>(四) 公務<u>配發</u>行動裝置，須安裝防毒軟體。</p> <p>(五) 行動裝置透過本部網路連網前，須向本部資訊<u>處</u>提出申請。</p>	<p>六、具上網功能行動裝置使用須知</p> <p>(一) 行動裝置必須使用專用電源，不得接觸公務電腦USB接口。</p> <p>(二) 公務電腦不得透過行動裝置連網。</p> <p>(三) 不得修改或破解公務<u>用</u>行動裝置之安全措施。</p> <p>(四) 公務<u>用之</u>行動裝置，須安裝防毒軟體。</p> <p>(五) <u>公務用</u>行動裝置透過本部網路連網前，須向本部資訊<u>中心</u>提出申請。</p>	<p>一、第一款至第四款現行部分用語較不明確，爰酌作文字修正。</p> <p>二、無論是否為公務配發行動裝置，均需向資訊處提出申請，爰第五款刪除部分文字。</p> <p>三、配合本部組織改造，修正第五款幕僚單位名稱。</p>