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。
二、機敏資料，指下列事項、業務及資料： （一）依法規明定之國家機密事項、一般公務機密事項。 （二）各級主管指示應保密之敏感性業務。 （三）承辦單位或人員就辦理業務考量，認為需保密之重要資料。		一、本點新增。 二、明定機敏資料之範圍。
三、實體隔離作業須知 （一）處理機敏資料時，應使用專屬實體隔離電腦設備處理及列印。 （二）儲存機敏資料之可攜式儲存媒體應上鎖保管，並僅限於實體隔離電腦讀取、繕打及列印。 （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。 （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，應先將文	二、實體隔離作業須知 （一）處理密級以上或各單位認定需保護之敏感性（以下簡稱機敏資料）資料時，須使用專屬實體隔離電腦設備處理及列印。 （二）儲存機敏資料之可攜式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。 （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。 （四）實體隔離電腦製妥之文件如需網	一、點次變更。 二、配合實務狀況第一款、第二款及第四款酌作文字修正。 三、第三款未修正。

件複製至可攜式儲存媒體，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、後應格式化刪除所有檔案。	路傳輸或從連網電腦下載文件複製至隔離電腦使用時，須先將文件複製至可攜式儲存媒體，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。	
四、資料保護須知 （一）機敏資料及依法規應保護之資料應做適當之保護；以電子通信工具傳遞機密資料者，應以加裝政府權責主管機關核發或認可之通信、資訊保密裝備或加密技術傳遞。 （二）使用可攜式儲存媒體存放資料時，機敏資料及一般資料應分開儲存，不得混用並妥善保管。 （三）禁止在家中、公共場合等辦公室以外場所使用連網電腦處理機敏公務。 （四）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。	三、資料保護須知 （一）機敏資料須加密，且不可存放於連網電腦。 （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。 （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。 （四）公務個人電腦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。 （五）使用可攜式儲存媒體存放資料時，機敏資料及一般資料應分開儲存，不得混用並妥善保管。 （六）禁止在家中、公共場合等辦公室以外場所使用連	一、點次變更。 二、現行第一款至第三款整併為第一款並配合實務狀況酌作修正。 三、現行第四款移列修正規定第六點第一款。 四、現行第五款至第七款移列第二款至第四款。

	網電腦處理機敏公務。 （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。	
五、網際網路使用須知 （一）連網電腦禁止瀏覽非法或本部所限制之網站。 （二）禁止於辦公室內私裝電腦及網路通訊等相關設備。 （三）因業務特性須上網瀏覽大陸網站者，須經單位主管核可後，向本部資訊處提出申請後使用。 （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。	四、網際網路使用須知 （一）連網電腦禁止瀏覽非法或本部所限制之網站。 （二）禁止於辦公室內私裝電腦及網路通訊等相關設備。 （三）因業務特性須上網瀏覽大陸網站者，須經單位主管核可後，向本部資訊處提出申請後使用。 （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。	點次變更，內容未修正。
六、電腦使用須知 （一）公務個人電腦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。 （二）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。 （三）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。	五、電腦使用須知 （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。 （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。 （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）。 （四）禁止私自安裝未	一、點次變更 。 二、第一款規定由現行第三點第四款移列。 三、現行第一款至第六款移列第二款至第七款，並配合實務調整第四款系統名稱。 四、配合本部資訊安全管理系統文件規範新增第八款至第十款。 五、現行第七款及第八款移列第十一款及第十二款。

（四）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（如部內入口網、電子郵件系統、自然人憑證等）。 （五）禁止私自安裝未經合法授權軟體。 （六）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。 （七）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。 （八）不得使用公務電子信箱帳號登記做為非公務網站之帳號，如社群網站、電商服務等。 （九）不得使用非公務電子郵件傳送或討論公務訊息。 （十）帳號密碼必須妥善保存，如有外洩疑慮，除儘速更換密碼外，並應通知本部熱線服務窗口。 （十一）下班時應關閉電腦及螢幕電源。 （十二）如發現資安問題，請主動向本部熱線服務通報。	經合法授權軟體。 （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。 （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。 （七）下班時應關閉電腦及螢幕電源。 （八）如發現資安問題，請主動向本部熱線服務通報。	
七、具上網功能行動裝置使用須知	六、具上網功能行動裝置使用須知	點次變更，內容未修正。

（一）行動裝置必須使用專用電源，不得接觸公務個人電腦USB接口。 （二）公務個人電腦不得透過行動裝置連網。 （三）不得修改或破解公務配發行動裝置之安全措施。 （四）公務配發行動裝置，須安裝防毒軟體。 （五）行動裝置透過本部網路連網前，須向本部資訊處提出申請。	（一）行動裝置必須使用專用電源，不得接觸公務個人電腦USB接口。 （二）公務個人電腦不得透過行動裝置連網。 （三）不得修改或破解公務配發行動裝置之安全措施。 （四）公務配發行動裝置，須安裝防毒軟體。 （五）行動裝置透過本部網路連網前，須向本部資訊處提出申請。	
八、生成式AI使用須知 （一）使用原則 1、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及人格權之可能性，業務委外辦理時亦同。 2、使用生成式AI時，應避免造成民眾生命、身體、自由或財產安全、社會秩序、生態環境之損害，或出現利益衝突、偏差、歧視、廣告不實、資訊誤導或造假等問題。 （二）資訊輸入注意事項 1、涉及公務機密、個人資料		一、本點新增。 二、增訂生成式AI使用須知。

或未經同意公開之資訊，切勿上傳至生成式AI，亦不得詢問涉及機密業務或個人資料之問題。 2、使用生成式AI時，所有互動資料皆可能為該服務提供者得以應用之資源，應避免資訊不當揭露之風險。 （三）應用資訊注意事項 1、使用生成式AI時應查證其產出之資訊真偽，不得僅依賴AI作為公務決策依據。 2、使用生成式AI時應判斷其生成資訊之正確性，未經查證，不宜引用或轉述。 3、使用生成式AI作為業務輔助工具時，應做適當資訊揭露或標記。 （四）禁止事項 1、機密文書必須由人員親自撰寫，不得使用生成式AI代勞。 2、公務上不得使用大陸地區之生成式AI工具，如百度、阿里巴巴等。 （五）其他 1、行動裝置安裝		

生成式AI相關APP 前，須確認其真偽。 2、使用自建地端之生成式AI模型，應建立資安防護措施，防範安全威脅及攻擊，確保其系統之穩健性及安全性。		