

財政部及所屬機關(構)**資通安全**基本認知

一、宗旨

為維護本部及所屬機關(構)**資通安全**，特收錄每位同仁皆應注意之重點**資通安全**行政規定，彙整為本基本認知，以利同仁遵循。

二、**資通安全**政策

本部**資通安全**政策為「**資通安全**人人有責」，同仁應熟悉並遵循**資通安全**認知、**資通安全**法規，落實**資通設備**及系統之安全防護，以確保機關(構)**資通安全**。

三、**資通安全**目標

- (一)各機關(構)**資通安全**事件，應依規定時間完成通報、應變，及損害控制或復原作業。
- (二)每人每年應接受三小時以上**資通安全**教育訓練。

四、**資通設備**使用管理

- (一)公務配發之可攜式設備(筆記型電腦、行動裝置等)及儲存媒體(行動硬碟、隨身碟等)應妥適保管，非因公務需要不得攜出辦公處所。
- (二)公務配發之可攜式設備不得透過公開(無需認證)之無線網路傳輸敏感性資料，若有連結外部網路或設備之情形，該設備於攜回或連結機關資訊作業環境前，應進行掃毒或系統還原。
- (三)私人之**資通設備**不得連結機關**資通作業環境及處理機密或敏感性公務資料**。
- (四)使用者離開電腦時，應關閉螢幕電源或啟動電腦鎖定功能；電腦應設定超過十五分鐘未使用，進入螢幕密碼保護或強制登出。
- (五)辦公環境內必須使用機關提供之**資通設備**、網路，及規定之軟體，不得使用個人私有設備及中國廠牌產品，公務設備亦不得連結個人私有手機上網。若有業務上的需求，必須經資安長同意後，列冊管理並定期檢討。

五、電腦軟體使用管理

- (一)**資通設備**所需軟體，安裝前應確認已取得合法授權。
- (二)未經機關首長或其授權人核准，不得使用私有、免費或共享軟體；經核准使用之軟體已逾授權期限者，應立即刪除。

六、資料管理

- (一)保管機密或敏感性之電腦資料或檔案者，應將檔案加密或置於設有加密**保護之資料夾**。
- (二)機密或敏感性之資料及記載電腦檔案相關資訊等文件，不得隨意放置，下班時應上鎖或以其他方式妥為收存。
- (三)定期備份重要資料及檔案。

(四)因業務需要於公務電腦建立之個人資料檔案，應每年至少一次檢視有無保留之必要。

(五)即時通訊軟體使用應注意不得傳送公務敏感資料。

七、網路使用管理

(一)未經機關首長或其授權人核准，不得自行更改公務電腦 IP 位址、名稱及網路卡設定。

(二)公務電腦(含筆記型電腦)及伺服器不得安裝數據機或架設無線網路等相關對外連線設備，若有特殊需求應規劃防護措施並專案簽陳機關首長核准。

(三)未經機關首長核准，不得私自架設網站。

(四)不得使用點對點 (Peer-to-Peer, P2P) 分享軟體，但因公務需要且經機關首長或其授權人核准者，不在此限。

(五)機密性檔案不得於網路上傳輸；敏感性檔案傳輸前應先加密。

八、帳號及密碼管理

(一)密碼應設定八碼以上，且至少自英文大寫、英文小寫、數字及特殊符號，擇取三類依複雜性原則組成，並避免設定與使用者相關資料（生日、身分證字號、單位簡稱、電話號碼、車牌等）。

(二)密碼應至少每九十天更換一次。

(三)使用者識別碼及密碼應妥善保管，不得張貼於公務電腦、螢幕或其他容易洩密之場所。

(四)系統或瀏覽器應取消密碼自動記憶功能，避免密碼遭擷取或竊用，並遵守機關規定，如有外洩疑慮，除儘速更換密碼外，並應通知資安窗口。

九、病毒及駭客防範

(一)防毒軟體之病毒碼應為最新版本（日期最長不得超過一週，如有問題立即聯絡資訊人員）。

(二)不得開啟及下載來路不明之連結或檔案，以避免遭受木馬或病毒軟體植入。

(三)使用儲存媒體前，應先執行病毒掃描檢查，以防駭客藉由儲存媒體植入後門程式。

(四)公務電腦(含筆記型電腦)及伺服器應關閉 USB 儲存裝置自動執行設定 (AutoRun)，以防駭客藉由 USB 儲存裝置植入後門程式。

(五)上班期間不應連結非公務需要之網站，並避免連結惡意網站或釣魚網站，如發現異常連線，請通知資安窗口。

十、電子郵件管理

(一)同仁收發公務所需資訊應使用公務電子信箱(網域為 **ntbna.gov.tw**)，不得使用非公務信箱。

(二)公務名片所載電子信箱聯絡資訊，應以公務信箱為準。

(三)非因業務需要不得設定自動傳送電子郵件讀取回條。

(四)收取電子郵件規定如下：

1. 來路不明郵件勿任意開啟，應逕行刪除。
2. 關閉自動預覽再開啟郵件閱讀。
3. 以純文字讀取模式開啟郵件。
4. 傳送敏感性資料，應確認是否啟動加密機制。
5. 收信時應先確認發信者電子郵件帳號是否遭偽冒，必要時應直接聯繫發信者確認。
6. 不得使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。

十一、事件通報

- (一)發現或察覺可疑資安事故、異常事件或安全弱點等情事，應立即向機關資安窗口通報。
- (二)主動通報資安事件或可能資安風險者，依規定獎勵。
- (三)未遵守機關資安規定，初次予以告誡，若持續發生或勸導不聽者，依規定懲處；若因而發生資安事件，加重處分。

十二、應遵守個人資料保護法及資通安全管理法。

十三、資安訊息網址：

- (一)財稅內網-資源管理-電子書管理系統(YIM)-電子書模組-電子書閱讀(YIM410W)-財稅中心共通資安文件(SEcurity)及北區專用資安文件(ISMS)。
- (二)財稅內網右下角-資通安全宣導。
- (三)新竹分局資安窗口：

姓名：

電話:03-5336060#321



本人已詳閱**資通安全**基本認知

簽名：_____

日期：_____

宣導人簽名：_____