資訊安全稽核查檢表

|  |  |  |  |
| --- | --- | --- | --- |
| **受稽單位/人員** |  | **填表日期** |  |
| **稽核人員** |  | **稽核日期** |  |

**工作底稿填寫說明：**

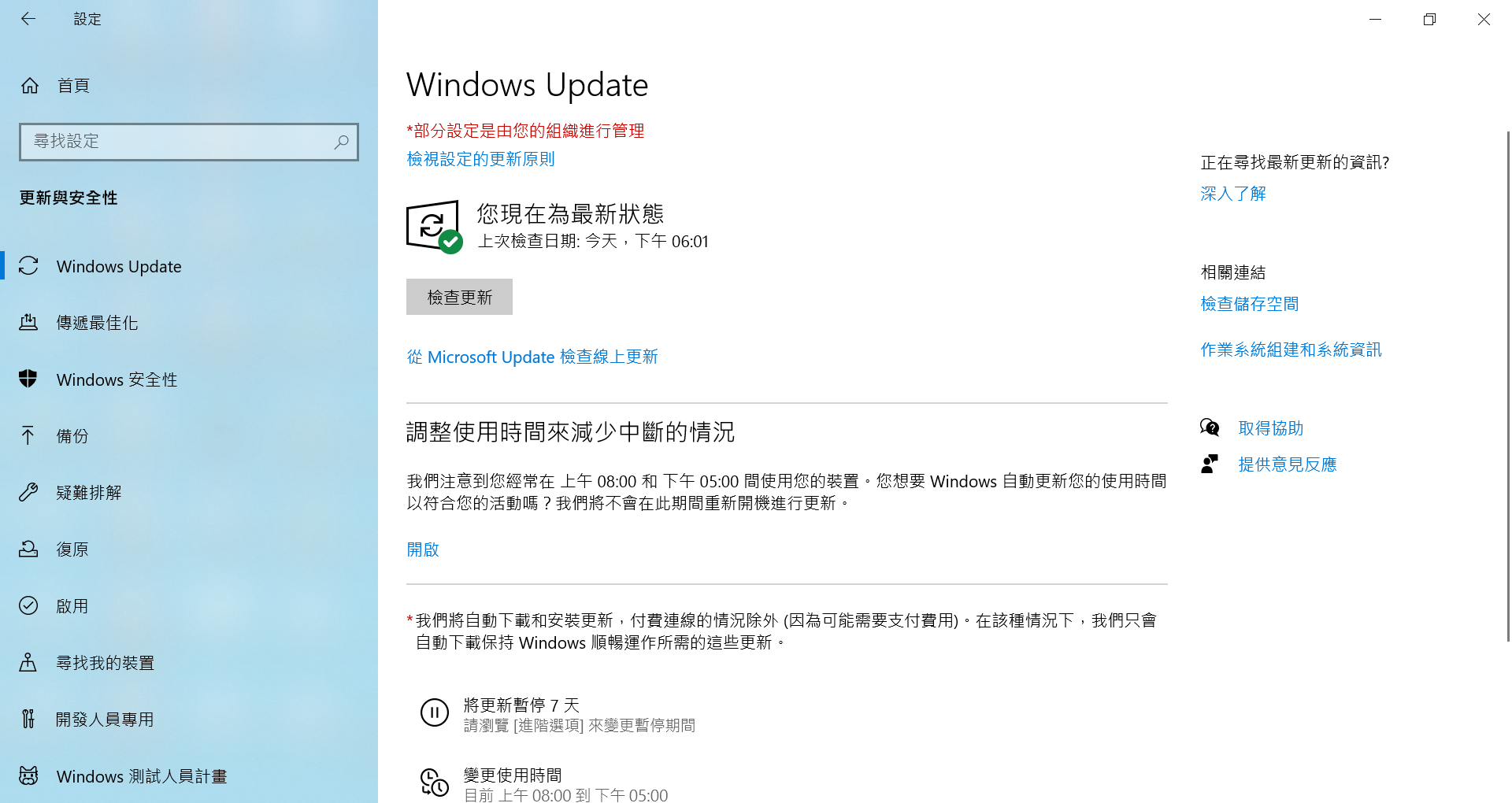
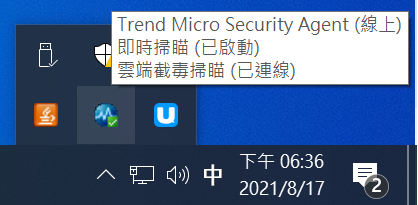
1. 判定結果請當場確認並填寫以利稽核結果說明及報告彙整。
2. 若為「不適用」項目請於「稽核結果」欄位註記說明。
3. 「稽核結果」欄位可考慮以下幾種方式陳述：
   1. 經與OO單位OOO訪談發現表示，目前…。
   2. 經抽檢…（文件、紀錄）發現，於第OO頁（第OO章節、編號OOO紀錄）…不符合事項。
   3. 經於OO單位實地訪查時發現…。
4. 稽核結果判定原則：
   1. 若稽核項目要求之作業程序均確實執行或相關文件紀錄完整且無缺失，則判定為「符合」。對於「符合」項目，可以提供建議事項。對於提供建議事項之稽核項目，請於「備註」欄位中註明。
   2. 若受稽核單位無執行稽核項目要求之作業程序，或相關文件紀錄缺漏甚多(為明顯之漏填或並未執行)，或違反作業程序之規定，則判定為「不符合」事項記扣。
   3. 若稽核項目要求之作業程序均已確實執行且留存相關紀錄，惟仍有少部分遺漏處，則判定為「觀察」事項記扣。
5. 一般同仁查檢表

| 序號 | 編  號 | 稽核項目 | 自我評審 | | | 稽核評量 | | | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 是 | 否 | 不適用 | 符合 | 不符合 | 觀察 | 不適用 | 備註 |
| GC 1 | | 資通安全政策及組織 | | | | | | | | |
|  | GC1.1 | 是否知悉本局或上級機關資通安全政策，且以書面、電子或其他方式被告知？(可以請受稽人說明放置位置) | V |  |  |  |  |  |  | 員工入口網\文件管理\資通安全專區\ISMS專區 |
| 2 | GC1.2 | 是否知悉本局成立跨部門資通安全組織，且有高階主管負責推動、協調監督及審查資訊安全管理事項？(本局資訊安全組織名稱?資通安全長是誰?) | V |  |  |  |  |  |  | 資通安全長:楊副分局長  組織名稱為:資訊安全暨個資保護小組。 |
| 3 | GC1.3 | 是否依職務層級參加單位或上級機關辦理之資訊安全講習，且時數達3小時以上？(請單位窗口提供單位訓練人員名冊)ISMS專區有放全局受訓練表 | V |  |  |  |  |  |  | 於8/23進行第一場資訊安全講習。 |
| GC 2 | | 實體與環境安全 | | | | | | | | |
| 4 | GC2.1 | 是否將智慧型手機連接個人公務電腦USB進行充電？(有看到要記點) |  | V |  |  |  |  |  | 檢查USB線有無接至電腦  行動裝置不允許連接電腦 |
| 5 | GC2.2 | 個人公務電腦是否擅自加裝週邊設備？（USB或智慧型手機）(有看到要記點) |  | V |  |  |  |  |  | 檢查USB孔有無其他設備  未經授權的隨身碟 usb |
| 6 | GC2.3 | 是否將所保管之可攜式電腦或媒體，使用嚴謹的保護措施（如設定硬體開機通行碼、檔案加密、送修前清除檔案等作業，使用後應將檔案刪掉）？ | V |  | V |  |  |  |  | 不適用。(無保管可攜式電腦及平板、手機、行動硬碟。)  是。(筆電確認開機密碼、Windows版本、行動硬碟確認檔案處理 ) |
| GC 3 | | 作業管理與存取控制 | | | | | | | | |
| 7 | GC 3.1 | 是否將個人公務電腦儲存之機密敏感檔案加密保護？ | V |  | V |  |  |  |  | 是(詢問加密方式)  **不適用** |
| 8 | GC 3.2 | 是否有自架設無線網路基地台連接機關網路、個人公務電腦上自行介接行動網路上網（如3/4G手機或3.5/4G網卡）(有看到要記點) |  | V |  |  |  |  |  | **否。** |
| 9 | GC 3.3 | 是否有擅自變更網路管理單位授與之電腦網路環境參數或移除內定軟體（如網路IP或防毒、弱掃、資安偵測等軟體）？(請確認防毒元件版本、防毒是否斷開) |  | V |  |  |  |  |  | **否。(檢查下方防毒軟體Trend Micro Security Agent\本機雲端病毒碼、更新時間、APEX ONE伺服器位置。)**  **內部IP有無被擅自更改** |
| 10 | GC 3.4 | 是否有在個人公務電腦使用P2P軟體，或是下載、複製非法或未經授權軟體（程式）？ |  | V |  |  |  |  |  | **否(檢查設定\應用程式\程式和功能。)**  **常見無授權:嘸蝦米、編輯PDF軟體、WinRAR。**  **用搜尋的方式** |
| 11 | GC 3.5 | 是否依規定安裝防毒軟體並更新最新病毒碼？且定期對電腦系統及資料儲存媒體進行病毒掃描？ | V |  |  |  |  |  |  |  |
| 12 | GC 3.5 | 是否有依規定更新個人公務電腦作業系統，或定期進行系統漏洞修補及檢視，並以手動同意執行Adobe Reader/ Acrobat/ Flash Player及Java Update等程式更新？(請確認Adobe Reader/ Acrobat/ Flash Player及Java Update版本) | V |  |  |  |  |  |  | **是。** Adobe Acrobat Reader為:21版以上。  Flash Player請移除。  Java為8版以上，如不用請刪除 |
| 13 | GC 3.6 | 是否有違反以下網路使用規定：   * 利用機關網路從事與公務無關或私人商業營利之行為。 * 以電子郵件大量傳送廣告信件或未經證實之信息；或以灌爆信箱、掠奪資源等方式，影響系統之正常運作。(請確認防毒元件版本、防毒是否斷開) |  | V |  |  |  |  |  | **否** |
| 14 | GC 3.8 | 是否符合以下相關安全設定：   * 公務電腦應啟動螢幕保護程式，設定啟動時間符合螢幕淨空政策之規定 * 密碼長度應為8碼以上 * 定期變更密碼（至少3個月執行1次變更） | V |  |  |  |  |  |  |  |
| 15 | GC 3.7 | * 是否避免將通行碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所？(有看到要記點) | V |  |  |  |  |  |  | **是。(詢問密碼張貼處或目視座位)** |
| 16 | GC 3.8 | 是否注意電子郵件使用之安全：   * 人員使用之電子郵件是否已關閉預覽功能？(有看到要記點) * 傳送機密性、敏感性資料及文件，是否符合保密安全規定？(詢問?看個人業務，有加密要嘉獎) | V |  |  |  |  |  |  | **是。(檢查Outlook)**  1.主畫面\檢視\讀取窗格\關閉  2.檔案\選項\信任中心\信任中心設定項目之  　　附件處理：關閉附件預覽 　　電子郵件安全性：以純文字讀取所有標準郵件。  3.傳送跟個資有關是否有加密處理 符合保密安全規定 |

\*請移除:adobe acrobat pro9、 bandicam、faststone image view & potplayer、FlashPlayer、WinRAR、嘸蝦米、PDF編輯軟體必須移除

\*0906 確認windows 版本及更新

\*檢查Windows版本:本機\右鍵內容\Windows規格\版本下方(應為20H2或21H1，如小於20H2請報修至資訊室)

1. 檢查Windows更新:左下視窗\右鍵設定\更新與安全性\檢查更新，並確認顯示視窗為最新狀態
2. 檢查防毒軟體版本及更新:箭頭點開\藍色圖案Trend Micro Security Agent點開\查看本機雲端病毒碼及APEX ONE伺服器
3. 檢查安裝程式：左下設定\應用程式\右上相關設定程式和功能  
   　　檢查Adobe Acrobat Reader DC 版本號為21.005.20060或以上

　　檢查Java版本為8以上(最新為8 Update 301)，如不需要請移除

　　檢查如有疑似授權軟體，詢問使用者授權，如無法提供佐證視同無法提供授權，須**另行採購或先行移除**  
　　如有FlashPlayer請移除

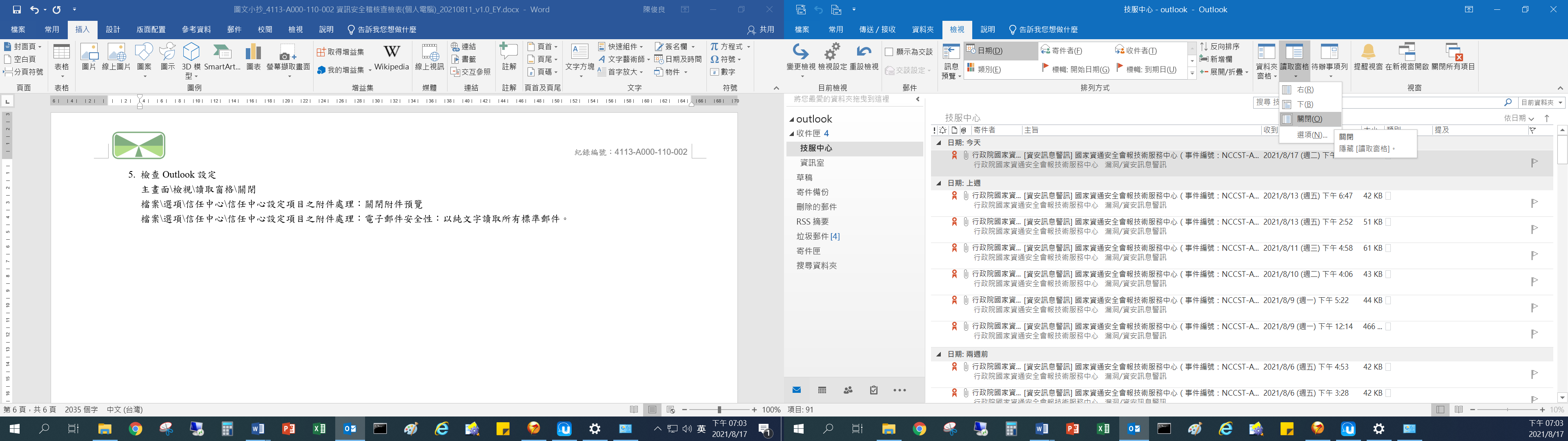
**滑鼠移至此處→**

　　常見須注意軟體：WinRAR、嘸蝦米、PDF編輯軟體

5. 檢查Outlook設定

主畫面\檢視\讀取窗格\關閉

* 每個分類資料夾需個別設定、檢查



檔案\選項\信任中心\信任中心設定\附件處理：關閉附件預覽

檔案\選項\信任中心\信任中心設定\電子郵件安全性：以純文字讀取所有標準郵件。

