**年度金融機構透過財團法人金融聯合徵信中心介接使用公務機關資料查核報告工作底稿(範本)-109年2月**修訂(編號:聯徵1)

**(會員機構名稱)：**

本單位查詢方式為：（可複選）□晶片卡 □伺服器連線(STS) □檔案傳輸(FTP)

查核基準日： 查核範圍： 查核期間： 查核人：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 查核項目 | 工作底稿編號 | 查核結果 | 處理意見 | 查核參考資料 |
| 調閱文件/ 查核方法 | 會員易致之疏漏 |
| 1. 公務機關資料蒐集與使用：

1)查調公務機關資料前，是否已取得當事人之書面授權或電子授權？2)是否符合辦理授信業務目的(不含信用卡)？3)公務機關資料使用單位透過網際網路連線取得客戶電子授權作業，是否以加密檔案傳輸傳送自然人憑證簽章之授權書？同時確保電子授權之不可否認性？4)如以電子授權，系統是否留存記錄(如日期、來源IP或電話號碼、授權書內容或版本、身分驗證結果等)？且其內容是否可完整呈現並可於日後取出供查驗？5)取得當事人授權書時，是否確實審核當事人之查調目的及身分，並確認授權書之驗證結果及授權書之真實性？6)查詢後，當事人之書面或電子授權相關資料、檔案及紀錄是否至少保管至授信期間終止後5年或自拒絕日起保存5年？ | 聯徵2聯徵2聯徵2聯徵2 |  |  | 1依據「金融機構透過財團法人金融聯合徵信中心介接使用公務機關資料管理規範」、機構訂定之信用資訊查詢作業控管要點及金管會108年7月30日以金管銀國字第10801097940號函示本中心轉知會員機構，內容略以：「有關本案管理規範所列使用單位自行查核機制，係為安全使用介接資料之最低標準，金融機構除須遵循本案管理規範，亦應依照各自所訂內部控制及內部稽核制度之規定，以風險為基礎方法之原則定期檢討對於資料使用者權限及查詢紀錄之自行查核頻率及筆數，以強化使用單位查詢介接政府資料之安全。」2.調閱聯徵中心之「介接公務機關資料發查紀錄資訊(含期間查詢)」（查詢代號 Z52），該表提供查詢日起算最近12個月內各會員機構發查紀錄，由該表進一步瞭解查詢之依據。3.「查詢條件限制」規定之查核，非常重要。進行查詢前請確認是否有合法之依據，即已取得當事人之書面授權或電子授權，及符合授信業務目的(不含信用卡)。4.請調閱印出之公務機關資料表，檢視是否簽章、控管機制及電子浮水印。 | 1.本項查詢資格要件常為查詢人及查核人忽略，請特別注意。2.查調前查詢人員應先確定查詢之合法性，以免違反相關法令規定。 3.系統未完整留存軌跡紀錄。4.未核貸之案件未留存相關資料或紀錄至少5年。5.公務機關資料表未有查詢人員簽章。6.公務機關資料表未有使用單位機構代號浮水印。7.公務機關資料表簽章者非為主管指定之查詢人員。8.未核貸或作廢之公務機關資料表任意丟棄，或由外部人員清理，易致資料外流。 |
| 7)查詢人員是否於列印之公務機關資料表簽章，以明責任並供查證？印出後不使用(含未承作案件)之公務機關資料表，是否予以控管或銷毀？產生之公務機關資料表是否確實印有使用單位機構代號之電子浮水印標識？8)使用財稅資料之業務系統是否標註「財稅資料係為課稅目的蒐集，僅供金融徵信案件之參考；若有資料內容疑問時，應向資料主管機關洽詢」等提示文字？ |  |  |  | 5.不使用(含未承作案件)之公務機關資料表之銷毀紀錄(應設有銷毀登記簿)。 |  |
| 1. 資料使用者之指定與登記：

1)單位主管是否指定專人辦理公務機關資料之查詢？有無未經指定者擅自查詢？【使用檔案傳輸批次／伺服器連線（以下簡稱FTP/STS）系統查詢之使用單位，其授權程序及異動管理，是否依據各使用單位作業流程自行訂定？是否留存「授權異動明細紀錄表」及「信用資訊查詢人員授權表」？】2)查詢人員其姓名、職稱、擔任期間、持用之晶片卡號碼或使用者帳號等是否設簿（請將貴機構所訂登記簿名稱填入）登記，並經單位主管核定？ 前項登記簿是否妥善保存五年？【使用FTP/STS系統查詢之使用單位，是否由系統紀錄授權異動情形並自動產生信用資訊查詢人員授權表取代登記簿？該授權表是否妥善保存最近五年之授權紀錄？】 3)單位主管對於執行查詢、覆核查詢紀錄，及保管晶片卡與密碼等人員之指定，是否符合內部控制原則？ | 聯徵4聯徵4 |  |  | 查核時可調閱下列資料：1.查詢作業相關人員授權登記簿。 2.會員自設之登記簿，如：「查詢設備保管登記簿」、「查詢信用資訊申請登記簿」、「晶片卡借用登記簿」等。3.聯徵中心之「介接公務機關資料發查紀錄資訊(含期間查詢)」（Z52）。4.請評估查詢作業流程及人員授權內部牽制是否足夠及有效。 | 1.單位主管未指定專責查詢人員。2.由未經指定者擅自查詢。3.有設簿但未確實登記。4.授權主管未核章。5.平時未依規進行事後勾稽，僅於稽核時才由查核人員抽核，內控不足。6.僅有查詢人員自行勾稽，不符內控原則。 |
| 1. 使用者帳號密碼：

1)使用FTP/STS系統查詢之使用單位，查詢人員之密碼是否保密及遵守使用聯徵中心查詢系統的設備密碼設定規定，並設定密碼複雜度（數字、英文字大小寫及特殊符號混合）要求，密碼每90天強制更新一次，至少不可以與前三次使用過之密碼相同？2)每位查詢人員是否各自配予一組獨立帳號密碼？查詢人員是否有使用用他人帳號密碼或將帳號密碼借予他人使用？3)使用單位帳號管理人員是否每年至少進行二次帳號及權限審查？4)晶片卡查詢密碼，由聯徵中心以掛號密件寄交，是否由單位主管親收，再密交密碼保管人員？5)晶片卡與查詢密碼是否由不同人員保管？ 6)晶片卡查詢人員異動或業務需要時，是否更換密碼？7)查詢人員離(調)職，帳號管理人員是否應至遲於離(調)職生效日移除/停用相關系統帳號與權限？ | 聯徵4聯徵4聯徵4 |  |  | 查核時可調閱下列資料：1.請調閱帳號及權限盤點表。2.請調閱查詢作業相關人員授權登記簿。3.會員自設之登記簿，如：「查詢設備保管登記簿」、「查詢信用資訊申請登記簿」、「晶片卡借用登記簿」等。4.晶片卡與密碼應由專人且非同一人妥善保管。 | 1.查詢人員異動/離職未向聯徵中心申請人員異動。2.密碼保密措施欠妥(如貼於電腦邊)。3.密碼設定未符合複雜度規定。4.查詢人員異動時，未變更密碼。5.帳號及權限未一年審查二次。6.查詢人員離(調)職，未能於離(調)職生效日前移除/停用相關系統帳號與權限。7.查詢後不使用未登出或查詢完畢未將晶片卡拔出歸還。8..晶片卡查詢人員異動未更換密碼。 |
| 1. 公務機關資料保密、保護義務：

1)查詢所得公務機關資料是否嚴限內部業務參考使用，不得跨境或國際傳輸及不得對外公開或移轉他人？ 2)資料查調及存放場所，是否嚴禁相關人員進入或停留，並應有門禁或監控措施？3)使用公務機關資料之連線電腦設備是否設定螢幕保護密碼，及每日下班前是否關機？ |  |  |  | 1.查核時請確認下列事項：1)在被核准存取自聯徵中心查詢所得資訊或資訊系統前，是否正確地向其簡要說明資訊安全角色與責任。2)FTP/STS系統設備是否設置於安全區域。3)對於自聯徵中心查詢所得資訊存取是否有限制特定人員。4)自聯徵中心查詢所得資訊不宜複製至非安全區域。 | 1.相關人員未能充分認知資訊安全的威脅與關切事項、其基本責任與強制責任等。2.提供公務機關資料予非相關業務人員或機關。3.公務機關資料做跨境傳輸。4.資料查調及存放場所未管制人員進出或有監控措施。5.使用公務機關資料之連線電腦每日人員下班前未關機離開。 |
| 4)使用FTP/STS系統查詢之公務機關資料使用單位，對於存放自公務機關查得資訊之相關資料庫，是否建立資料庫存取軌跡紀錄，並建立資訊安全管理控制措施及規範，包含人力資源安全、實體及環境安全、資訊交換、通訊與作業管理、存取控制等？5)資料庫主機是否使用網管設備阻檔非必要連結，禁止直接存取網際網路，並關閉USB與序列埠等介面裝置？6)主機作業系統、設備實體及網路之相關主機是否置於電腦機房，維持良好運作維護管理，並建置防毒或防火牆等防護設備？7)若屬「資通安全責任等級分級辦法」適用對象而使用公務機關資料之系統，是否完成資訊系統分級與資安防護基準作業及辦理安全性檢測？8)晶片卡查詢設備是否妥善保管，並限於營業或辦公處所使用？9)晶片卡如有毀損或停用，是否具函退還聯徵中心？如有遺失或滅失時，是否具函聯徵中心掛失？10)查詢公務機關資料前（即傳授權書前），是否填寫或輸入日期、人員、案號及事由，並依分層負責之規定，取得授權核定層級人員之核准？採紙本申請單者是否裝夾留存？ 11)系統是否記錄查詢者帳號、查詢者IP、查詢日期、時間、查詢作業代號、查詢條件、案號及事由等查詢日誌，並留存五年？ | 聯徵3聯徵3 |  |  | 5)對於FTP/STS系統或相關程式變更是否有受控管。6)存放公務機關資料之資料庫是否有防火牆管制，連線設定為最小必要化，並無直接存取網際網路。7)存放公務機關資料之資料庫是否關閉非必要或無使用之USB或序列埠。8)使用公務機關資料之相關主機是否置於電腦機房並定期修補安全性漏洞。9)使用公務機關資料之相關主機是否有安裝防毒軟體並定期更新病毒碼與完整掃描。10)「資通安全責任等級分級辦法」適用對象而使用公務機關資料之系統是否完依資訊系統分級完成資安防護基準作業及定期辦理安全性檢測。2.清點聯徵中心晶片卡。3.會員留存之聯徵中心「IC晶片卡簽收單」、「晶片卡異動申請書」、「晶片卡查詢工作站移機、重新安裝申請書」(影本)。4.請調閱公務機關資料查詢申請單與查詢記錄單。 | 6.公務機關資料的存取權限管理未落實、稽核日誌未盡完備等。7.公務機關資料複製至非安全區域如測試系統環境或個人電腦等。8.公務機關資料存放之資料庫，未有網路設備管制連結，或有網路設備管制但未最小必要化連線設定。9.資料庫主機未關閉USB或序列埠。10.查詢記錄單未送經分層負責授權核定層級人員之核可。 |
| 12)每週是否產出查詢紀錄單，送查詢人員核章確認及分層負責授權核定層級人員之核可，並留存三年？13)公務機關資料是否提僅供予業務相關人員閱覽、使用，且不得任意複製？ |  |  |  |  |  |
| 1. 安全控管、查核與稽核：

1)聯徵中心定期通知之晶片卡使用情形，單位主管是否派人切實核對？對於晶片卡異常使用或遭鎖卡者是否追蹤原因？2)單位主管有否指定專人抽核聯徵中心之「介接公務機關資料發查紀錄資訊(含期間查詢)」（Z52），抽核比率是否每月至少為2%，且筆數不得少於10筆（查詢記錄總筆數少於10筆者，是否全數查核）？【使用FTP/STS系統查詢之單位，是否增加核對其系統自動產生之「查詢紀錄」，查詢記錄至少保留5年？】3)使用單位是否將使用公務機關資料管理規範執行情形列入內部自行查核，且每年至少查核1次？查核報告（副本）是否依規定時間由總機構指定單位(本查核項目內請註明此單位名稱）彙總送聯徵中心？4)使用單位是否將使用公務機關資料管理規範執行情形列入內部稽核項目，且內部稽核單位每半年至少查核1次，稽核記錄是否保留3年?？5)使用單位若發生公務機關資料外洩或相關資安事件，是否立即通知本中心及提供該資料之公務機關？ |  |  |  | 查核時可調閱下列資料：1.清點聯徵中心晶片卡。2.聯徵中心之「介接公務機關資料發查紀錄資訊(含期間查詢)」（Z52）。3.查詢公務機關資料相關之作業控管規定。4.查核報告書。5.資訊安全相關事件單。 | 1.晶片卡相關設備未指定專人保管，致生設備遺失或非指定人員查詢等情事。2.晶片卡(與密碼)之交付及收回未依規定登記，影響職責之認定。3.Z52抽核比例偏低。4.未依規執行內部自行查核或稽核單位查核。5.查核流於形式。6.經由分支單位查核，總行未將查核情形予以彙總，查核發現缺失未改善。 |

**本範本提供參考，各會員機構請依各自作業環境及內控制度訂定合宜之工作底稿。**

 **年度金融機構透過財團法人金融聯合徵信中心介接使用公務機關資料查核報告工作底稿(範本)**-**109年 02 月**修訂(編號:聯徵2)

**(會員機構名稱)：**

 查核基準日： 查核範圍： 查核期間： 查核人：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 查詢日期 | 被查詢當事人 | 查詢人員 | 使用者代碼 | 授權辦理事項 | 查詢資格依據(查詢條件限制) | 查詢結果 | 查核結果 | 處理意見 |
| 統一編號/身分證號 名 稱 | 姓名 | 有否被授權辦理查詢1 | 當事人之書面授權書(含電子授權資料) | 有無合法查詢依據2 | 有無紙本申請單或系統查詢日誌 | 公務機關資料表查詢人有無簽章 | 是否僅供內部使用不對外公開或移轉他人使用 | 不使用(含未承作案件)之公務機關資料表是否妥善處理 | 公務機關資料表是否列有電子浮水印標識 |
| 是否保存5年 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1 查詢人員有否被授權辦理查詢請調閱查詢人員登記簿(聯徵4) 。

2 「合法查詢」係指符合法定特定目的並取得當事人之書面授權書始得向聯徵中心查調相關資訊。有關規定請參閱「金融機構透過財團法人金融聯合徵信中心介接使用公務機關資料管理規範」相關條文。

|  |
| --- |
|  **年度金融機構透過財團法人金融聯合徵信中心介接使用公務機關資料晶片卡查詢設備使用情形查核報告工作底稿(範本)-109年02月**修訂(編號:聯徵3)**(會員機構名稱)：** 查核基準日： 查核範圍： 查核期間： 查核人：  |
| 晶片卡查詢設備 | 保管人員 | 設備使用及管理情形 | 查詢密碼3 | 晶片卡與查詢密碼保管情形 | 查核結果 | 處理意見 | 備註 |
| 名稱 | 序號 | 姓名 | 是否經主管授權辦理[[1]](#footnote-1) | 保管是否妥善 | 毀損、停用、遺失時，是否具函聯徵中心辦理 | 晶片卡使用情形[[2]](#footnote-2) | 啟用日期 | 是否由單位主管親收後密交密碼保管人員 | 密碼保管人 | 查詢人員異動或業務需要時，是否即向聯徵中心申請更換 | 晶片卡與查詢密碼是否由不同人員保管 |
| 是否派人切實 核對 | 對於使用異常或遭鎖卡者是否追蹤原因，以防範弊端發生 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |
| --- |
|   **年度金融機構透過財團法人金融聯合徵信中心介接使用公務機關資料查詢作業相關人員授權登****記****簿**[[3]](#footnote-3)1**(範本)**-**109年02月**修訂(編號:聯徵4)**(會員機構名稱)：** |
| 中文姓名 | 職稱 | 授權查詢方式[[4]](#footnote-4)2 | 授權辦理事項[[5]](#footnote-5)3 | 使用者代碼[[6]](#footnote-6)4 | 授權起日[[7]](#footnote-7) |  主管簽章 |  授權迄日[[8]](#footnote-8) |  主管簽章 | 備註 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

1. 1 晶片卡保管人員有否被授權辦理查詢請調閱查詢人員授權登記簿(聯徵4)。

2 晶片卡使用情形可參閱由聯徵中心提供之「介接公務機關資料發查紀錄資訊(含期間查詢)（查詢代號Z52）或聯徵中心定期通知（或各單位自設之登記資料）。

3 會員透過專屬網路進行信用資訊查詢須使用晶片卡及兩道密碼：第一道為使用者帳號密碼，第二道為晶片卡密碼，前者為使用者由專屬網路進入聯徵中心會員查詢專區之密碼；後者供認證晶片卡之合法性；均由聯徵中心製作提供，以掛號寄交單位主管親收，如查詢人員異動請向聯徵中心申請人員異動，亦請自行變更密碼(無須向聯徵中心申請)。 [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. 1 凡與查詢作業有關之授權事宜，如：主管指定之辦理查詢、覆核查詢紀錄等作業人員，均應設簿登記，以利事後管理。本登記簿應保存五年，備供查核。授權內容若為設備保管人員請於備註欄記載。 [↑](#footnote-ref-3)
4. 2 填報金融聯合徵信中心信用資訊查詢方式，可以「N」代表晶片卡查詢、「B」代表加密檔案傳輸查詢、「Q」代表伺服器連線查詢。 [↑](#footnote-ref-4)
5. 3 授權辦理事項如：查詢信用資訊，保管晶片卡(卡號)、覆核查詢紀錄….等。 [↑](#footnote-ref-5)
6. 4 足資辨別受指定辦理查詢人員之使用者帳號。 [↑](#footnote-ref-6)
7. YYYMMDD(民國)，填報查詢人員被授權查詢權限起日。 [↑](#footnote-ref-7)
8. YYYMMDD(民國)，填報查詢人員被授權查詢權限截止迄日。 [↑](#footnote-ref-8)