金融機構透過財團法人金融聯合徵信中心介接使用勞動部勞工保險局業務資料計畫

一、使用勞動部勞工保險局資訊之重大政策依據

- (一) 依總統府 106 年 5 月 1 日「經濟策略會議-金融業」會議總統、院長裁示事項：「關於為推動金融科技，而增加政府統計數據及保管資料公開，請本會針對金融業者需求先洽相關單位，分析可行性及適宜作法，提出構想後，再由行政院協助處理。」
- (二) 國家發展委員會及本會邀集內政部、財政部、交通部、勞動部及經濟部，於 106 年 11 月 2 日召開「金融科技發展所需政府資料交換運用研商會議」決議，針對金融機構所需客戶職業投保資料，在符合法規及取得客戶授權同意下，研議由本會透過電子化政府服務平臺介接勞動部資料，並指定財團法人金融聯合徵信中心(以下簡稱聯徵中心)辦理介接事宜。上開介接機制及本會「金融機構透過聯徵中心使用公務機關資料管理規範」分別經勞動部 107 年 12 月 11 日勞局企字第 10701800641 號函及勞動部勞工保險局(下稱勞保局)108 年 5 月 24 日保企管字 10860008071 號函復同意。

二、計畫目標、預期效益、實施期程、使用目的及應用範圍

(一) 計畫目標及預期效益

本會為推動數位金融發展，協助民眾以更便捷方式，取得申辦貸款所需職業投保資料，以提升資料之真實性及金融機構之徵審效率，並強化金融機構授信風險控管。

- (二) 實施期程：自本會向勞保局提出申請並經審核同意後開始實施，至連結作業終止。

(三) 使用資料目的及應用範圍

為促進金融科技發展，健全金融機構風險控管，使用單位於辦理授信業務目的，於取得當事人書面或電子授權同意下，始可透過聯徵中心查調勞保局職業投保資料。聯徵中心受本會指定負責介接公務機關資料，即受本會委託蒐集、處理及利用個人資料之受託者，視同委託機關(本會)，須依資通安全管理法、個人資料保護法等相關規定辦理，並依「金融監督管理委員會使用勞動部勞工保險局資料管理規定」受本會稽核督導。

三、資料最小化原則

使用勞保局資料內容為當事人職業投保資料，包含被保險人姓名、身分證號、生日、投保單位名稱、異動日期、投保薪資等職業投保資料，使用單位於辦理授信業務目的，取得當事人書面或電子授權同意始得進行職業投保資料查

調，取得資料作為授信徵審等授信業務目的之用。

四、資料安全管制作業

(一) 權責分工

1. 申請機關暨監督機關：本會。
2. 管理機構暨介接資料單位：聯徵中心。
3. 資料使用單位：聯徵中心會員金融機構。

(二) 資料自申請、持有、查詢、使用、保管與銷毀等管理及審查機制

1. 申請

- (1) 本會依據勞保局「各機關使用勞動部勞工保險局業務資料管理規定」，檢附相關文件向勞保局提出申請介接查調服務。
- (2) 使用單位辦理授信目的有必要查調當事人之職業投保資料時，應先取得當事人書面或電子授權，同意監督機關及管理機構與使用單位蒐集、處理及使用其資料，並應清楚告知授權書之內容以及個人資料保護法、消費者保護法及金融管理法令規定之應告知事項。取得授權後須將授權資訊傳送至管理機構，獲管理機構審核通過後，始得申請查調該當事人之職業投保資料。

2. 持有

使用單位取得當事人授權同意後，透過聯徵中心介接取得職業投保資料。而聯徵中心在確認使用單位授權及查調資訊後，透過電子化政府服務平臺介接取得勞保局職業投保資料，資料自取得後於聯徵中心暫存 3 天即刪除。

3. 查詢

- (1) 使用單位應依本管理規定進行資料使用者之指定與登記及使用者帳號密碼管理。
- (2) 使用單位辦理授信目的有必要查調當事人之職業投保資料時，應先取得當事人書面或電子授權。
- (3) 使用單位應確實審核查調當事人職業投保資料之查調目的及身分，並對授權之驗證結果及真實性負責。使用單位於取得當事人書面授權或電子授權後，始可將授權書或授權資訊傳送至管理機構備查。授權資訊傳送至管理機構審核通過後，始得查調該當事人之職業投保資料。
- (4) 使用單位如透過線上取得當事人電子授權，意思表示授權同意查調職業投保資料，系統應留存記錄(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)，且其內容可完整呈現並可於日

後取出供查驗。

- (5) 使用單位查詢後無論核貸與否，均應確實保存當事人書面或電子授權相關資料、檔案及紀錄，不得任意銷毀，保存期限應至少保管至授信期間終止後五年，拒絕核貸則自拒絕日起保存五年，其使用單位有更長之保存期限者，從其規定。
- (6) 使用單位查詢人員查詢職業投保資料前，應填寫或輸入日期、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。

4. 使用

使用單位對於職業投保資料之使用及相關程序除遵循本管理規定外，應遵守中華民國銀行公會會員徵信準則、授信準則等各項使用單位業務自律章則及金融管理相關法令，確保資訊利用之適法性及合目的性，不得逾越特定目的之必要範圍，並應與所辦理之授信業務目的具有正當合理之關聯。查詢所查得之所有資訊，應保守秘密，嚴限內部參考，且不得跨境或國際傳輸；除當事人依法查詢其本人資料外，不得對外公開或移轉他人。

5. 保管與銷毀

使用單位資料查調及存放場所，嚴禁非相關人員進入或停留，並應有妥適的門禁或監控措施。使用職業投保資料之連線電腦設備應設定螢幕保護密碼，使用者離開時，應退出使用環境，每日下班前並應確實關機。查詢人員僅能進行所查調之案件資料查詢或列印，不得自行更改或竊取未經核准使用之資料；並於作業完畢或臨時離開座位時，應立即登出系統，以避免遭他人冒用。使用檔案傳輸批次／伺服器連線系統向管理機構進行查詢之使用單位，對於存放自勞保局查得資訊之相關資料庫，應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。

(三) 檢視與檢討

管理機構須每年定期檢視與檢討已由本會向勞保局申請核准之職業投保資料連結作業之使用情形，如確認使用單位已無查詢需求，應函請本會向勞保局申請終止該連結作業。

五、處理資料保密措施

(一) 使用者申請程序及管理

1. 使用單位主管應指定專人負責辦理查詢，未經指定者，應嚴禁擅自進行查詢。【使用檔案傳輸批次／伺服器連線系統向管理機構進行查詢之使

用單位，其授權程序及異動管理，請依據各使用單位作業流程自行訂定，惟建議系統應具「授權異動明細紀錄表」及「信用資訊查詢人員授權表」。

2. 受指定辦理查詢之人員（以下簡稱查詢人員）其姓名、職稱、擔任期間、持用之識別卡號碼或使用帳號等應設簿登記，並經使用單位主管核定。登記簿應保存五年備查，並於監督機關或管理機構請求時提供之。【使用檔案傳輸批次／伺服器系統向管理機構進行查詢之使用單位，請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，該授權表應保存最近五年之授權紀錄備查。】
3. 使用單位之單位主管對於執行查詢、覆核查詢紀錄及保管識別卡與密碼等人員之指定，應注意符合內部控制原則。
4. 使用檔案傳輸批次／伺服器系統對管理機構查詢之使用單位，查詢人員之密碼應保密及遵守使用管理機構查詢系統的設備密碼設定規定，密碼長度至少為八個字元並應設定密碼複雜度（數字、英文字大小寫及特殊符號混合）要求，密碼每九十天強制更新一次，至少不可以與前三次使用過之密碼相同。
5. 使用單位查詢系統應可限制資料使用者連續登入密碼失敗的上限次數，並訂定解除該帳號鎖碼機制。
6. 每位查詢人員應分別配予一組獨立帳號密碼。查詢人員應使用個人帳號密碼，不得使用他人帳號密碼，亦不得將帳號密碼借予他人使用。
7. 查詢人員帳號密碼為機密資訊，使用者應妥善保管不可外洩，為維護自身權益，查詢人員懷疑密碼已洩漏時，應立即變更。
8. 晶片卡查詢密碼，由管理機構以密件掛號寄交使用單位主管親收，再密交查詢人員使用，晶片卡與查詢密碼應分別指定不同人員保管。查詢人員異動或業務需要時，應向管理機構申請更換查詢密碼。
9. 查詢人員離(調)職時，帳號管理人員應至遲於離(調)職生效日移除/停用相關系統帳號與權限。
10. 使用單位管理者密碼之通知應具保密措施，防止被竊取，密碼應妥善保管，避免他人知悉。管理者不得使用非本人申請之帳號，且不得與他人共用。如遇人員調離職時，其所受配賦之帳號密碼不得交接予他人，應循程序註銷權限。管理者職務異動前辦理帳號異動程序，並於異動前或當日，由新任管理者於承接業務時停止原管理者帳號，並新增其管理者帳號。使用單位之系統無法變更管理者帳號時，新任管理者應立即變更密碼。

(二) 使用單位查詢人員帳號及權限之使用狀況，應由使用單位帳號管理人員定

期審查，檢視使用者權限是否符合權限最小化原則，每年應至少進行二次帳號及權限審查，並留存紀錄，至少保存五年。

- (三) 管理機構負責資料連結作業之承辦人員或專責人員及單位主管異動時，應於異動後七日內通知勞保局。
- (四) 使用單位對於職業投保資料之使用，應確保資訊利用之適法性及合目的性，不得逾越特定目的之必要範圍，並應與授信業務目的具有正當合理之關聯。查詢所查得之所有資訊，應保守秘密，嚴限內部參考，且不得跨境或國際傳輸；除當事人依法查詢其本人資料外，不得對外公開或移轉他人。管理機構具資料存取權限者，對所查得資訊之蒐集、處理及利用，應限於職務之必要範圍內，並應保守秘密。

六、使用資料管制措施

(一) 作業規範與日誌、軌跡紀錄保存

1. 使用單位查詢人員查詢職業投保資料前，應填寫或輸入日期、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，採紙本申請單者應裝夾留存，作為日後查核依據。
2. 查詢時應避免非業務權責人員閱覽、攝、錄影或以其他方式擷取資料。
3. 資料查詢完竣後，如有併案或附卷必要，應妥善保管，紙本應以密件方式保存，電子檔應進行檔案加密。
4. 使用單位連線至管理機構查詢資料如逾時，系統應自動登出。
5. 系統應記錄查詢者帳號、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。
6. 每週應產出查詢紀錄單，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，並留存五年備查。

(二) 批次取得資料管制措施

1. 管理機構若以批次方式取得資料，應由專人辦理檔案傳輸，並檢核資料完整性。
2. 管理機構若以批次方式取得資料，取得資料載入系統應用時，應設定使用該資料之存取權限及核准使用期限。欲使用資料者，須經申請核准後始得使用，並應於核准期限內使用及應用於核准業務範圍，且資料禁止攜出機關辦公場所。
3. 管理機構若以批次方式取得資料，應保存資料檔案、資料庫之存取、增刪異動紀錄，如日誌與軌跡紀錄，至少保存五年。

七、指定專責人員辦理安全維護事項

- (一) 管理機構專責人員應遵循聯徵中心資訊安全準則、資訊安全控管作業規範辦理，並要求使用單位辦理資料使用者之指定與登記，且要求使用單位訂定「信用資訊查詢作業控管要點」，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- (二) 管理機構專責人員應依資通安全管理法、資通安全責任等級分級辦法暨其資通安全責任等級之公務機關應辦事項，接受並完成相應之資通安全教育訓練。

八、資料使用期限、刪除程序及期限

- (一) 資料使用期限：本計畫第一點所列重大政策終止後，停止介接使用。
- (二) 資料刪除程序
 1. 管理機構介接取得資料應指定專人或由系統設定排程刪除資料。
 2. 資料刪除範圍應包含資料暫存之資料庫及相關衍生檔案。
 3. 刪除程序完成後，應留存佐證資料備查，至少五年。
- (三) 資料刪除期限：管理機構介接取得資料之暫存期限為三天，應於期限屆滿24小時內完成刪除。
- (四) 使用單位對於介接取得之職業投保資料，於使用完竣且確認無保存必要後，一個月內刪除，內部應訂有相關資料刪除程序及刪除期限規範，據以遵行。

九、督考及相關稽核措施

- (一) 監督機關對管理機構及使用單位稽核：
 1. 對管理機構每半年至少辦理一次書面查核，每二年辦理一次實地查核。
 2. 由本會檢查局對使用單位進行金融檢查時，併同辦理本項查核，配合本會檢查局年度查核規劃，至少每五年完成一輪。
- (二) 管理機構內部稽核及對資料使用單位稽核：
 1. 使用單位若以晶片卡向管理機構進行查詢，晶片卡使用情形由管理機構定期通知，各使用單位主管應切實核對，對於使用異常或鎖卡者應追蹤原因，以防範弊端發生。
 2. 管理機構依據「銀行間徵信資料處理交換服務事業許可及管理辦法」第二十九條第二項及聯徵中心會員規約第十六條及第十七條第十一項之規定訂有「財團法人金融聯合徵信中心會員機構信用資訊查詢作業安全控管查核辦法」，據以執行查核使用單位有關信用資訊查詢安全控管機制、遵循查詢作業程序及資訊保密條款等之執行情形。
 3. 為確保使用單位查調需求符合授權事項，管理機構事後並採取各項查核機制，且每年至少查核一次，查核機制包括以下至少一種：

- (1) 實地查核或書面查核：由管理機構人員赴使用單位請其提供客戶相關線上或書面授權紀錄進行查核，或於必要時洽請使用單位提供書面或電子授權相關記錄文件予管理機構審核。
 - (2) 指定項目會員自行查核：由管理機構指定查核項目及內容，函請使用單位自行查核，並將查核結果回報管理機構。
 4. 管理機構若發現有資料外洩或相關資安事件，應立即通知監督機關及勞保局，勞保局得立即終止或停止該使用單位查調資料之一切權利。
 5. 管理機構依據「財團法人金融聯合徵信中心自行查核作業須知」及「內部稽核作業要點」辦理各項自行查核與內部稽核作業。另監督機關及勞保局辦理實地稽核作業時，管理機構應配合提供相關資料，相關人員並應配合辦理。
 6. 管理機構應每年辦理資料安全稽核工作，並應包含使用勞保局資料之作業，作成稽核紀錄，至少保存五年。
- (三) 使用單位內部自行查核及內部稽核
1. 使用單位每週應產出查詢紀錄單，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，並留存五年備查。
 2. 內部自行查核：
 - (1) 管理機構提供之使用單位查詢紀錄資訊，使用單位主管應指定專人抽核，每月至少抽核百分之二查詢紀錄，且不得少於十筆（查詢紀錄總筆數少於十筆者，應全數查核）。【使用檔案傳輸批次／伺服器系統向管理機構進行查詢之使用單位，請增加核對其系統自動產生之「查詢紀錄」，查詢紀錄應至少保留五年。】
 - (2) 本規定之執行情形，各使用單位應列入內部自行查核，每年至少查核一次，查核報告副本應依規定時間由（總機構指定單位）彙總送管理機構。
 3. 內部稽核：本規定之執行情形，使用單位應列入內部稽核查核項目，使用單位每半年應至少執行一次內部稽核作業，如有查調異常現象，得不定期進行稽核作業，稽核紀錄並應留存五年備供查核。
 4. 監督機關、勞保局及管理機構辦理實地稽核作業時，使用單位應配合辦理或提供相關資料。
 5. 使用單位若發生資料外洩或相關資安事件，應立即通知管理機構及勞保局，勞保局得立即終止或停止該使用單位查調資料之一切權利。

十、管理制度之佐證

管理機構通過「國際資訊安全標準 ISO／IEC 27001」，並每年維持證書之有

效性。另管理機構通過「臺灣個人資料保護與管理制度 (Taiwan Personal Information Protection and Administration System, TPIPAS)」，亦每年維持證書之有效性。

十一、 違反規定之責任

- (一) 管理機構及使用單位對於職業投保資料之處理及利用，若有違反個人資料保護法規定致當事人權益受損者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
- (二) 使用單位如有違法或未依本規定進行查調之情事，依管理機構會員規約第十七條及十八條辦理，情節重大者，除予以停查或撤銷會員資格外，監督機關、勞保局及管理機構得立即終止該使用單位查調資料之一切權利，倘有侵害第三人權利，使第三人受有損失時，使用單位應自負相關法律責任及賠償第三人所蒙受之損失。
- (三) 使用單位暨其查詢人員對資料之使用，應遵循相關法令，違反者則視違法性質，移送各該主管機關或司法機關依相關法律處罰。如致生他人損害，應負賠償責任。
- (四) 管理機構及使用單位如涉及違反法令者，應由所屬機關議處；其相關管理或專責人員未盡善良管理人注意義務之責，亦同。

十二、 個資安全事故通報與協力損害防免義務

管理機構及使用單位如發生職業投保資料相關之個人資料安全事故，或疑似事故時，應採取必要之緊急應變措施，包含事故調查、責任釐清及避免損害擴大之防免措施，另應將相關情形及資料通報監督機關及勞保局。