Secure File Transfer Protocol (SFTP) Onboarding for Business Partners

Introduction

Secure File Transfer Protocol (SFTP) is a mechanism available to transfer and exchange payroll reporting, retirement enrollment, and/or health enrollment files between a client and the California Public Employees' Retirement System (CalPERS) server through a secured connection. Business partners interested in utilizing SFTP must be able to properly create a myCalPERS compatible XML file prior to considering this method.

Note: This process does not apply to health/dental carriers or direct authorization vendors (DAVs).

Step-by-Step Procedure

The following steps provide direction on how to set-up files for submission via SFTP. Prior to proceeding with these steps, be aware of the following:

- Steps 4 – 6 may be done concurrently.
- Steps 7 – 8 must be completed **before** CalPERS Employers Account Management Division (EAMD) submits the formal request to initiate the SFTP folder setup.
- Steps 10 – 13 can only be completed **after** CalPERS assigns the business partner's SFTP connectivity request to a myCalPERS system release.

Step	Who	Action
1	Business Partner	Will a third-party administrator submit data on behalf of the business partner? • Yes, proceed to Step 2 • No, skip to Step 4
2	Business Partner	Requests to establish a business partner relationship by following the steps outlined in the Business Partner Relationships Student Guide (PDF).
3	EAMD System Support Team	Approves the appropriate service relationship(s) within myCalPERS.

![CalPERS logo]

Step	Who	Action
4	Business Partner/ Third-Party Administrator	Reviews the Employer Technical Toolkit (ZIP) that provides documents and schema files needed to build XML files to report health, membership, and payroll/Supplemental Income Plan (SIP) to CalPERS. **Note**: Contact CalPERS to obtain access to the file readiness test environment and request assistance with file development and error resolution. SFTP requests may be postponed if files are not correctly formatted and tested.
5	Business Partner/ Third-Party Administrator	Reviews the PDF file named 'Encryption_Decryption_File_Naming' within the Employer Technical Toolkit (ZIP) to ensure the business partner adheres to **all** SFTP protocol requirements outlined in the documentation. This includes proper encryption, decryption, and transport requirements. A thorough review of this document should be done by a business partner's data transfer team. **Note**: SFTP requests may be postponed until the business partner/third-party vendor adheres to all encryption/decryption requirements.

6	Business Partner/ Third-Party Administrator	Notifies CalPERS of intent to submit files via SFTP. The following information must be provided:
		
		1. CalPERS business partner name and CalPERS ID
		2. Third-party administrator name and CalPERS ID (if applicable)
		3. The interface number required to submit data:
		    • IA00007 – Retirement enrollments
		    • IA10006 – Payroll reporting
		    • IA50031 – Health enrollments
		4. Contact information for the CalPERS business partner
		5. Contact information for the third-party administrator (if applicable)
		
		Note: Contacts provided should be individuals who can review and sign CalPERS security documents. Contacts should also include those with data transfer and interface exchange knowledge.

7	EAMD System Support Team	Completes the ***Sending Electronic Information Agreement*** (SEIA) security document, obtains required internal signatures, and sends to the Information Security Office (ISOF) for approval.

Step	Who	Action
8	EAMD System Support Team	Opens ServiceNow request to setup an STFP interface and attaches the approved, signed copy of the SEIA received from ISOF.
9	ServiceNow Application	Creates a task for the Application Development team to submit a template to the Enterprise Scheduling Output Management (ESOM) team to create a new batch job stream.
10	Information Technology Services Branch (ITSB) Application Integration Services (AIS) Team	Contacts the business partner's/third-party administrator's middleware team to confirm SFTP protocols are met by reviewing the PDF file named 'Encryption_Decryption_File_Naming' found in the Technical Toolkit.
11	ITSB AIS	Works with the business partner/third-party administrator to test file transmission once the SFTP account has been established and implemented.
12	ITSB Application / Interface / Release Support (AIRS) Team	Works with the business partner/third-party administrator to test the file using batch job stream for functionality.
13	EAMD System Support Team	Notifies the business partner/third-party administrator when the SFTP connectivity is implemented and available in the myCalPERS production environment.