Jersey Bank Depositors Compensation Scheme

SCV File Transfer Protocols (version 01.00)

The Jersey Resolution and Depositors Compensation Authority (JRDCA) has agreed upon the use of the Deloitte File Exchange tool as their primary method for Single Customer View (SCV) File transfers from eligible deposit holding Jersey Banks to the JRDCA for the purposes of testing, and in the event of a bank insolvency.

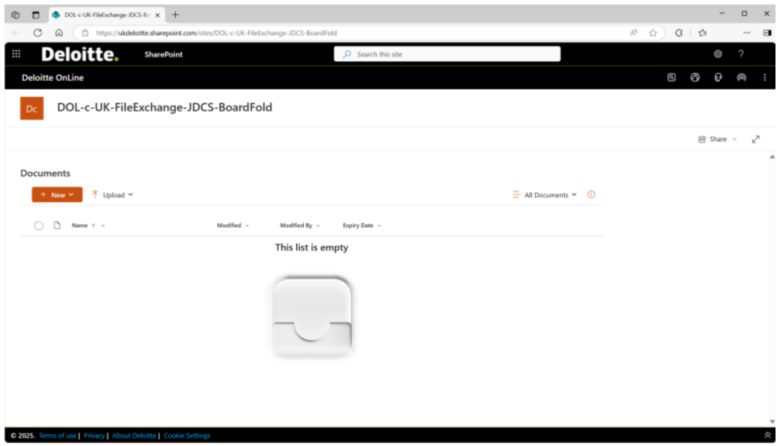
The File Exchange tool is Deloitte UK's secure tool for sharing and receiving large files with clients, vendors or suppliers. Its purpose is to transfer data, making it available for a brief period (maximum of 30 days) for recipients to download. The tool is built on SharePoint Online; however, end-user features are limited to uploading, downloading and sharing features only.

Upon receipt of a request for an SCV File submission, a bank will be expected to upload its SCV file and/or SCV Report through the File Exchange tool in accordance with the prescribed timeline. Any detailed results from testing will also be shared with the bank using this tool.

All data provided through the File Exchange tool will only be held until the completion of the task for which it has been submitted. After that, a secure deletion process will be enacted.

Each bank must nominate designated contacts to be set-up as users on File Exchange. These users will have read and write access to the bank's folders, in order to upload or download files as needed.

For further information or if you have any questions, please contactinfo@jrdca.org.je.



File Exchange Information Sheet

Server and storage security

The File Exchange tool is hosted in the UK on Microsoft Azure, in a cloud environment managed by Deloitte Cloud Services and vetted through a control framework to reduce the attack surface through vulnerability management system processes. Data is stored in a secure cloud environment. Microsoft Azure compliance certifications and assurances can be viewed at https://www.microsoft.com/en-us/trust-center. The tool is compliant with ISO/IEC 27001 and reviewed in compliance with SSAE-18, SOC-1 and AT 101 standards, and SOC-1 and SOC-2 control attestations.

Secure user access

A unique File Exchange segregated area is established for each bank that transfers files to, or receives files in relation to the JDCS. User login to the tool is provisioned only to the bank and to JRDCA approved users and requires multi factor authentication.

Account logs

All activity in File Exchange is logged and can be made available for review upon request.

Intellectual property rights

The uploading of files to File Exchange does not alter any preexisting intellectual property rights.

Data access

Files uploaded to File Exchange will be deleted after 30 days, or upon completion of the task for which the file has been provided, whichever occurs first. Where bank users are instructed to submit or receive files, users will be required to log in to the File Exchange platform using the credentials established when their access was set up.

Encryption of data in transit

Access to the File Exchange tool is strictly enforced through secure channels, ensuring that all connections are authenticated and encrypted. All communication to and within the File Exchange tool is encrypted using TLS 1.2, safeguarding data during transmission and preventing eavesdropping or unauthorised access.

Encryption of data at rest

All data stored within the File Exchange tool is protected with robust encryption methods. Databases housing File Exchange data are encrypted using transparent database encryption with 256-bit encryption keys, ensuring that even if storage media is compromised, the data remains unreadable without proper authorisation. For additional file-level protection, sensitive data within the File Exchange tool are encrypted using AES-256, a widely recognised and highly secure encryption standard.

Secure connection

Primary access is via the secure File Exchange user website.

Access controls

All user permissions are managed such that access to each bank's unique area is restricted to only the users approved by each bank, and to Deloitte staff acting for the JRDCA/JDCS.
Requests to add or delete a bank user should be sent to the JRDCA via info@jrdca.org.je.