OKLAHOMA
Office of Management
& Enterprise Services

Batch File Transfer Standard

Introduction

This standard specifies batch file transfer standards for Oklahoma state agencies. The standard describes tools included in the state reference architecture. This document and all information contained within are applicable to all State of Oklahoma agencies and partners.

Modern applications usually interoperate with other applications using modern interfacing methods, such as application programming interfaces or APIs. However, when the state's legacy applications were developed, the usual way of sharing data between applications was the basic file transfer process. The state still has many applications that rely heavily on file transfers to share data.

The most common method for sending these files and receiving files from other applications is using the file transfer protocol, or FTP. FTP does not encrypt the data during transit whereas secure FTP (e.g. SFTP, SCP, etc.) does encrypt data during transit.

Whenever business requirements call for a new file transfer process, the development and implementation of the process often spans multiple OMES IS departments and is very laborious and time consuming.

The basic file transfer protocols are intentionally designed to not abend when the transfer does not work. This causes issues for processes that depend upon successful file transfers because downstream processes continue to run even when the transfer failed.

Today, the state and its agencies have a large number of file transfers but no coherent or consistent way of managing them. There is no established way to inventory all the file transfers that are in production, how much data is being moved, where the data is coming from, where it is going, what type of data is being moved, who owns the process, etc.

Purpose

The purpose of this document is to describe the state standard for batch file transfers. The goal of this standard is to control costs, reduce technical debt, reduce file transfer sprawl, enable creation of file transfers in a consistent, standardized manner, reduce time needed to create new file transfers, enhance the state's ability to support file transfers and collect metrics around file transfers. Developing on common tools and platforms creates shared context for understanding state data and facilitates knowledge transfer between agencies, departments and teams.

Definitions

FTP – File transfer protocol. A method of sending one or more files from one computer to another. The data is not encrypted during transit.

MFT – Managed file transfer. A software tool designed specifically to facilitate file transfers.

SCP – Secure copy. A method of sending one or more files from one computer to another. The data is encrypted during transit.

SFTP – Secure file transfer protocol. A method of sending one or more files from one computer to another. The data is encrypted during transit.

Standard
Agencies developing file transfers should utilize one of the tools from our reference architecture.

- File transfers must be secured.
- File transfers must have retry functionality.
- File transfers must have alert notification functionality in the event of failure.
- In the event of a failure, the file transfer system must have the ability for an operator to retry any failed jobs after corrections have been made.
- File transfers must have the ability to log anomalies, errors and failures to Splunk or current log/event monitoring system.
- File transfer processes must be documented in a central repository.
- File transfers must have the ability to promote configuration changes to multiple environments.

The two MFT tools supported by OMES are: MuleSoft and MOVEit.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§

34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 05/24/2022	**Review cycle:** Annual
Last revised: 05/24/2022	**Last reviewed:** 08/14/2023
Approved by: Joe McIntosh, Chief Information Officer	