Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

SERVICE AGREEMENT

Between

The Maryland Department of Information Technology and

The Customer

MoveIT Transfer and Automation

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and the Serviced Customer. The parties agree as follows:

I. Service Description

DoIT offers a Secure File Transfer Protocol (SFTP) capability as a hosted service. The SFTP services are provided on the MoveIT platform using MoveIT Automation and MoveIT Transfer Services include SFTP hosting and file automation services for schedule transfers between internal and external systems. Available to state agencies only.

A. Standard Service:

The following components are included with the standard service:

1. MoveIT Transfer - The MoveIT File Transfer service provides secure/encrypted file transfer to and from various hosted services. DoIT offers this service, where sensitive files are delivered with complete visibility, security, and control. Agencies can share files with internal stakeholders, partners, customers, individuals, or other systems, while ensuring regulatory compliance with tamper-evident audit logs and encryption for data at rest and in transit.
2. MoveIT Automation - This service provides a mechanism (automatically pull, process, and push files to any platform, over any network architecture) for transferring files using automation. MoveIT automation jobs are used for scheduled transfers between MoveIT Transfer, agency servers or external sites.

B. What is included in the Service:

1. On-premise solution
2. Management and control over business-critical file transfers by consolidating them all on one system.

3. MoveIT Transfer's file encryption, security, tamper-evident logging, and centralized access controls.
4. Compliance with internal governance requirements and regulations like PCI, HIPAA.
5. Workflow automation capabilities without the need for scripting.

C. Service Exclusions:

The following elements are excluded from the standard service offering:

1. The costs for new licenses needed for new SFTP Organizations or other features not included in the base SFTP platform. (inquiry to Cloud Services for more information.)
2. Identify business owners and required automation transfers.
3. Establish connectivity to external servers at remote locations.
4. Provide training for staff that will operate and perform administrative support and user functions.
5. Configuring permissions at the file/folder level for non-enterprise agencies.

D. Optional Services

Auxiliary services may be available upon request from the Customer for an additional cost. These costs are not included in the budgeted services that DoIT provides and shall be the responsibility of the requesting agency. For any work requested in this area, DoIT will not be able to proceed until fully funded by the requester through a funds certification document.

The following services are add-ons that may be requested. Costs for these items are variable and will be clearly defined and agreed to before moving forward with the request.

1. Agency Branded UR
    a) Coordinate URL registration and implementation of unique URL if required. Using the following standard naming convention. XXXX.sftp.md.gov

II. Service Dependencies

To ensure the service described herein is delivered consistently and in accordance with state standards, the customer must meet the following requirements:

DoIT Services:	• Preliminary planning meetings with the agency to discuss the existing environment and the installation and base configuration of multiple MoveIT Transfer Webfarm nodes. • Acceptance of Managed Services agreement, which includes DoIT's standard SLAs

	• Payment for all service costs at the agreed interval, as published in the DoIT rate schedules • Reporting any service-related issues to DoIT help desk
Technical:	• Define Folder structure, including security and user permissions • Define Automation tasks and intervals
Non-Technical:	• Client role definitions for escalation • Provide 24 x 7 x 365 points of contact (3) for coordinating outages, emergency maintenance/restoration (with appropriate application access to provide technical assistance), and change management

III. Responsibility Model

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the customer and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

A. DoIT Responsibilities for Customer (Enterprise)

DoIT shall be responsible for the following activities in coordination with the Customer receiving DoIT enterprise managed services:

DoIT's Responsibilities for Enterprise Customers:

DoIT shall:

1. Coordinate on the set up of SFTP folder structure
    a. Configure folder access permissions.
    b. Configure file/group admins
    c. Administration of SFTP platform.
2. Provision new SFTP automation jobs.
3. Work with agencies to define scope of work as required.
4. For SFTP services that require additional modules in addition to the baseline installation:
    a. DoIT will create admin accounts for the customer on the SFTP server. In order to create the separation an ORG add-on license module may need to be purchased depending on the use case.
        i. An ORG license provides logical separation from the other SFTP folders and customers. The ORG will enable administration of the platform to be isolated and for data and configurations to be separated from other tenants using the platform. The ORG license will also allow for the site to be branded with its own unique URL information for

example DoIT-Transfer.md.gov, following DoIT's standard naming convention.

ii. Coordinate URL registration and implementation of unique URL if required. Using the following standard naming convention. XXXX.sftp.md.gov

5. Infrastructure
    a. Assisting with any networking configuration, backup server connections, and storage space allocation. .
6. Enterprise Managed Services
    a. Perform patching and antivirus.
    b. Monitor the health, utilization, and availability of resources.
    c. Maintain backup and recovery.
7. Maintain ownership of the underlying hosting account and console access management.
8. Adhere to DoIT's Change Management process.

B. <u>DoIT Responsibilities for Customer (Non-Enterprise)</u>

DoIT shall be responsible for the following activities in coordination with the Customer for which DoIT does not provide enterprise managed services:

DoIT shall:

1. Coordinate on the set up of SFTP folder structure
    a. Configure file/group admins
    b. Configure folder access permissions.
    c. Administration of SFTP platform.
2. Provisioning of new SFTP automation jobs.
3. Work with agencies to define scope of work as required.
4. SFTP services that require additional modules in addition to the baseline installation.
    a. DoIT will create admin accounts for the customer on the SFTP server. In order to create the separation an ORG add-on license module may need to be purchased depending on the use case.
        i. An ORG license provides logical separation from the other SFTP folders and customers. The ORG will enable administration of the platform to be isolated and for data and configurations to be separated from other tenants using the platform. The ORG license will also allow for the site to be branded with its own unique URL information for example DoIT-Transfer.md.gov, following DoIT's standard naming convention.
        ii. Coordinate URL registration and implementation of unique URL if required. Using the following standard naming convention. XXXX.sftp.md.gov
5. Infrastructure
    a. Networking, server, and storage.
6. Enterprise Managed Services
    a. Perform patching and antivirus.

b. Monitor the health, utilization, and availability of resources.
c. Maintain backup and recovery.

7. DoIT maintains ownership of the underlying hosting account and console access management.
8. Adherence to DoIT's Change Management process.

C. Customer Responsibilities

The customer shall be responsible for the following activities:

1. Define and provide DoIT with folder structure and permissions access list for folders for Enterprise agencies. Configuring permissions for files and folders is the responsibility of the non-enterprise agency.
2. Define users requiring access providing user names and email addresses
3. Management of Users accounts that need access to use SFTP services. Notify the Service Desk of users no longer needing access.
4. Procure formalized training, if needed.
5. Designate user(s) as group/file administrators. Required for systems with 100+ users. Administrative responsibilities will include but may not be limited to, SFTP account management, password unlocks & resets, file & folder permissions and other custom configurations as required.
6. User Agency shall coordinate with customers of the SFTP system, cut-overs, account information and new URL domain name changes with users.
7. Users will provide all required information for custom connections to external systems via protocols that are not https (FTPS, SFTP, SSH are supported). Firewall ports for customers not using https may need to be open to facilitate job automation for moving files between systems.
8. Standard retention is 30 days.
    a) Custom file retention policies are available upon request.
9. The system is not designed to be used for long term storage. Offloading of files for long term archival storage is available upon request

IV. Service Level Agreements (SLA's)

A. Availability

Service availability includes the duration of time the service is operational during a twenty-four (24) hour period and the level at which the service functions. The table below further outlines DoIT's service targets.

Category	Measure
Availability	99.9% uptime
Capacity	N/A
Reliability	99.9%

B. Vulnerability Patching SLA for MoveIT platform

Critical Vulnerability Patching	15 days for patching. 1 day for network segmentation	A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs without warnings or prompts.
Moderate Vulnerability Patching	60 days	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations
Low Vulnerability Patching	90 days	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.

C. Maintenance

DoIT may modify the service without degrading its functionality or security features.

1. Scheduled Maintenance

   Regular maintenance must be performed to maintain availability and reliability standards and includes replacing hardware, upgrading software, applying patches, and implementing bug fixes.

   a) Scheduled maintenance will be performed outside of normal business hours (8 pm - 6 am Monday - Friday; weekends and holidays)
   b) The customer will be notified no less than five (5) business days prior to the scheduled activity.
   c) Within twenty-four (24) hours after the completion of the scheduled activity, the Customer will be notified.

2. Unplanned Maintenance
    a) DoIT will attempt to notify the Customer of any unplanned maintenance activities no less than two (2) hours prior to commencement. Note: Emergency activities requiring immediate remediation may not allow ample time for notification.
    b) Within twenty-four (24) hours after the completion of unplanned maintenance activity, the Customer will be notified.

D. Service Delivery

DoIT will deliver the requested services to the customer in a timely manner according to the following standards.

Category	Measure
Initial Ticket Response and Customer Contact	1 Business Day during normal hours for Incidents with priority 2 and 3
Major Incident	Priority Incidents (P1), 15 minutes. This includes security breach, Infrastructure crash

V. Support and Service Management

A. Support

DoIT will provide support via telephone, email, or in-person according to the SLA's outlined above.

1. The DoIT Service Desk is available twenty-four (24) hours a day, seven (7) days a week, to provide Tier 1 telephone support.
2. Tier 2 support will be provided during regular business hours (8 am - 5 pm) Monday thru Friday, excluding state holidays and state closings.
3. Tier 3 support will be provided as needed to address further escalations
4. DoIT will serve as the primary support provider of the service outlined herein except when third-party vendors are employed.

B. Incident Management

Incidents reported to the DoIT Service Desk will be triaged and managed based on priority as follows*:

Priority (P)	Description	Response Time	Resolution
P1	An incident that results in a total cessation of service across the Customer	[2] hours	[24] hours
P2	An incident that results in a partial cessation or	[4] hours	[2] business

	disruption of service, administrative access issues, or loss of other essential business functions.		days
P3	Disruption of service for of non-essential functionality, service questions, and administrative requests such as account creation, deletion, and changes	[2] business days	[5] business days
*Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.			

C. Request Management
Requests to move, add, or change service shall be handled as follows:

1. New Service(s)
Entities seeking to utilize the service or deploy optional services outlined herein must:
    a) Submit a request via email to doit.intake@maryland.gov explaining the business needs or challenges.
        - DoIT will evaluate the request to ensure that the service meets the entity's business needs.

2. Service Modifications
To increase, decrease, or alter existing service, the Customer must:
    a) Submit a request via email to doit.intake@maryland.gov
        - Service modifications include increasing or decreasing quantity of units, relocation of service.
        - DoIT will log the request and assign it to the appropriate team for fulfillment.
        - Requests that involve increases to costs will result in billing changes to the agencies which will require a Statement of Work and fund certification to make the change.

D. Outages
DoIT will notify the Customer via email of any outages or service degradation resulting from maintenance, fault isolation, or other disruptions.

E. Support and Service Management Exclusions:
While DoIT strives to tailor support and maintenance activities to match the customer's mission, there may be limitations that hinder our ability to satisfy changing business needs. As such, support and service management activities do not include:

1. Integrate Customer application into MoveIT

VI. Costs for Service

DoIT provides this service via a shared service model, which allows the state to recognize reduced pricing based on economies of scale.

A. The Customer charges budgeted for the current fiscal year are outlined in the DoIT Shared Services Annual Invoice.
B. The unit of measure for which charges are derived for this service is per agency.
    a) Secure Automated File Exchange Service:
        - Monthly
        - Per User Account

The cost is derived based on the total license consumed by the agency

2. Reference the current fiscal year Rate Sheet for additional information

C. All services delivered by DoIT under this agreement are done so on a 100% reimbursable model and therefore costs will be evaluated and adjusted annually to account for fluctuations in the number of shared services used and the underlying costs to deliver that service.

VII. Termination of Service

This service will automatically be renewed unless the customer and DoIT mutually agree in writing to adjust or discontinue.

A. The customer must provide ninety (90) days advance written notice to terminate services. Due to the nature of the state financial system budgeting for IT services, terminations will only be effective at the end of the fiscal year following the conclusion of the ninety (90) day notice period.

VIII. Warranty, Limitations, and Exclusions

This section is not applicable