



MOVEIT CLOUD SERVICE DESCRIPTION

1. **Service Description**

1.1 We agree to provide you with use of a MOVEit Cloud Service (“**Service**”) fully operated by us, subject to the Terms of Service published on Ipswitch website at www.ipswitch.com (as may be relocated by Ipswitch from time to time).

1.2 Your Service will include one dedicated MOVEit Cloud Organization.

1.3 **Unless you subscribe to the PCI Compliance Toolkit, you may not use the Service for storage or transfer of Cardholder Data (CHD).**

1.4 **Unless you subscribe to the HIPAA Compliance Toolkit, you may not use the Service for storage or transfer of Protected Health Information (PHI).**

2. **Service Availability**. Our Cloud Operations team performs proactive maintenance and monitors the Service 24x7x365. Assuming incidents and events are within our reasonable control, we will use commercially reasonable efforts to make the Service available 99.9% of the time (the “**Uptime Performance Target**”).

2.1 **Service Credit**. In the event that the actual Uptime Percentage (as defined in Section 2.2) is less than this Uptime Performance Target (as defined in Section 1.4.2) in any given month during the term of this Agreement, you can request (as described in Section 2.3) a “**Service Credit**”. A Service Credit will represent the right to extend this Agreement at no cost to you for the length of time shown in the table in Section 2.3 below. In the event that the actual Uptime Percentage is less than 95% in any two consecutive months or any three months during any 12 month period, you may elect to terminate this Agreement upon 15 days written notice, in which event you will receive a pro-rata refund for the number of prepaid months remaining in the then-current term of the Agreement. The Service Credit and the early termination provided for in Terms of Service will be your sole remedies in the event that we fail to meet the Service Levels described herein.

2.2 **Uptime Percentage** is calculated by us as total minutes the Service is available in a given month divided by the total minutes in such month less exclusions. The following events are excluded from the Uptime Percentage calculation:

2.2.1 Acts or omissions of you or your employees, agents, contractors or representatives,

2.2.2 Use or failure of any equipment you own or provide;

2.2.3 Your failure to follow instructions or procedures issued by us;

2.2.4 Scheduled maintenance as described in Section 2.7 below;

2.2.5 Emergency maintenance as described in Section 2.8 below; or

2.2.6 Failure or unavailability of any third party or external facilities, software or services, failure or unavailability of any electronic or mechanical equipment, failure or unavailability of any third party or external communication lines, or telecommunications or telephone facilities or other interconnect problems, unauthorized access, or other events that are not within our reasonable control.



2.3 Uptime Performance Targets and Service Credits

Monthly Uptime Performance Target	Service Credit
99.0 to 99.9%	three (3) days
95.0 to 98.9%	ten (10) days
Less than 95.00%	thirty (30) days

2.4 **Service Credit Request Procedure.** To receive a Service Credit, you must submit a claim by opening a case with Ipswitch Support. To be eligible, the credit request must be received by us no later than 30 days following the end of the month when the incident occurred and must include:

- 2.4.1 The words “MOVEit Cloud SLA Credit Request” in the subject line;
- 2.4.2 The dates and times of each downtime incident that you are claiming;
- 2.4.3 The affected MOVEit Cloud organization IDs; and
- 2.4.4 Your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).
- 2.4.5 If the Monthly Uptime percentage of such request is confirmed by us and is less than the Uptime Performance Target, then we will notify you of confirmation of the Service Credit in the month following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

2.5 **Recovery Point Objective (RPO).** In case of unforeseen Service degradation we will strive to restore the level of Service within 15 minutes.

2.6 **Response Time Objective (RTO).** In case of unforeseen Service degradation we will contact you with acknowledgement and status update within two hours.

2.7 **Scheduled Maintenance.** We perform regular scheduled Service upgrades, enhancements and general maintenance on Sundays between the hours of 4:00 pm and 7:00 pm EST. During this time the Service may have limited availability or not available at all. We will provide a minimum of 30 days’ notice on the Status Site (as defined in Section 2.9 below) for every Scheduled Maintenance.

2.8 **Emergency Maintenance.** In the event of severe service degradation or risk of security breach, the Service may become temporarily unavailable. As we work to restore the Service, we will communicate our progress on the Status Site and refer to this Service unavailability as Emergency Maintenance.

2.9 **Service Status.** You can monitor the availability of the Service at any time by visiting <http://status.moveitcloud.com> (“**Status Site**”). We use the Status Site to make announcements about all Service availability-impacting work we perform, including Scheduled Maintenance and Emergency Maintenance as defined below. Whenever possible we include details about the nature of the work being performed and offer



guidance on the expected maintenance completion. We recommend you sign up for proactive alerts available from this Status Site.

3. **Service Utilization.** We will measure your Service utilization based on the number of user accounts as well as storage and bandwidth use as follows:

3.1 **Users.** Total number of end users and Group Admins. We take daily snapshot of total end users and then average the daily totals over the month.

3.2 **Bandwidth.** Total cumulative size of all files uploads and downloads recorded in the MOVEit Transfer audit logs. Calculation is based on files sizes and resets at the start of each calendar month. If you have a cloud test environment provisioned for you any usage there will be included in the total monthly bandwidth usage.

3.3 **Storage.** Total sizes of all files stored on MOVEit Transfer. We take daily snapshot of disk space usage and then average the daily totals over the month. If you have a cloud test environment provisioned for you any usage there will be included in the total monthly storage usage.

4. **Overages** We will invoice you for any overages in bandwidth utilization, storage utilization and/or user accounts as set forth below in the next quarterly billing following the month during which the overage occurred. Such invoices will be payable by you, Net 30 days. We may waive billing for overages in our sole discretion.

The Following Sections (4.1, 4.2, 4.3) apply to all User-Based Pricing Customers

4.1 **Bandwidth**

4.1.1 If you subscribe and pay us for a combined total of fewer than 400 users per month, we agree to provide each of your licensed users with up to 5 gigabytes (“**Per User Allowed Bandwidth**”) of bandwidth utilization to/from the Service per month.

4.1.2 If you subscribe and pay us for a combined total of 400 or more users per month, we agree to provide you with up to 2,048 gigabytes (“**Total Allowed Bandwidth**”) of bandwidth utilization to/from the Service per month, for all your users combined.

4.1.3 You agree to pay us for bandwidth utilization (as measured by us) in excess of Per User Allowed Storage or Total Allowed Bandwidth (as specified above) at the rate of \$2.00 per gigabyte, per month.

4.2 **Storage**

4.2.1 If you subscribe and pay us for a combined total of fewer than 400 users per month, we agree to provide each of your licensed users with up to 5 gigabytes (“**Per User Allowed Storage**”) of storage utilization for the Service per month.

4.2.2 If you subscribe and pay us for a combined total of 400 or more users per month, we agree to provide you with up to 2,048 gigabytes (“**Total Allowed Storage**”) of storage utilization for the Service per month, for all your users combined.

4.2.3 You agree to pay us for storage utilization (as measured by us) in excess of the Per User Allowed Storage or Total Allowed Storage (as specified above) at the rate of \$3.00 per gigabyte, per month.



4.3 Users Accounts

4.3.1 You may create up to the pre-purchased quantity of unique end user accounts (“**Allowed User Count**”) for the Service.

4.3.2 You agree to pay us for additional end user accounts in excess of Allowed User Count at then current rate for our new contracts, as defined by us, plus \$3.00, per end user account, per month.

The Following Section (4.4) applies to all Block Pricing Customers

4.4 Usage Limits

4.4.1 You may create an unlimited number of end user accounts for this Service.

4.4.2 We agree to provide you with the level of bandwidth utilization to/from the Service (combined for all your users) up to the number of prepaid by you storage and bandwidth blocks (“**Blocks**”) measured in terabytes (TB). Bandwidth is defined as the file upload and download transfer volume by any of your users, including any test environments, measured in gigabytes (GB), where 1,024 gigabytes is equivalent to 1 terabyte (1TB).

4.4.3 We agree to provide you with the level of storage utilization for the Service (combined for all your users) up to the number of prepaid by you Blocks. Storage is any file stored in all the organizations, including any test environments, created and maintained for you by us, including files in folders, ad hoc package attachments and archived logs or packages measured in gigabytes (GB), where 1,024 gigabytes is equivalent to 1 terabyte (1TB).

4.4.4 In the event that your consumption exceeds then-current bandwidth and/or storage limits (as measured by us) you agree that you will purchase pro rata the additional Block(s) required to accommodate measured consumption for the remainder of the term of this Agreement. For billing purposes, we aggregate the bandwidth utilization over the course of the month, and we average the file storage over an entire calendar month.

4.4.5 You have 45 days to purchase additional Block(s) following receipt of invoice from us. Failure to purchase additional block(s) required to accommodate measured consumption after 45 days will constitute a breach, for which we may terminate the agreement.

5. Support

We may update this Service Support Policy (the "Policy") at any time, in our sole discretion, however such updates will not result in a material reduction in the level of Technical Support for the Service (the "Support") provided for which the applicable Service Subscription fees have been paid.

5.1 You are only eligible to receive Support if you have an active support agreement, remain current on all Service Subscription fees due and payable to us, and are otherwise compliant with your applicable contractual obligations to us. At our sole discretion, we may make other fee-based tiers of support or Service Subscription offerings available that provide specific, customized, and/or more comprehensive forms of enhanced support terms.



5.2 Support consists of infrastructure and application support, provided by us in our sole judgment, in order that the Service provided under the Terms of Service and the applicable Order Form may operate satisfactorily. Support will be provided in a timely and professional manner by qualified support engineers in accordance with this Policy.

5.3 Technical Support.

5.3.1 Depending on the nature of your issue, you may be assisted by our Technical Support or Customer Service as described on Ipswitch Support Online at <https://community.ipswitch.com/s/About-Support> (“**Support Site**”).

5.3.2 **Business Hours.** Our normal business hours for Technical Support and Customer Service are published on the Support Site. Please refer to the time zone corresponding to where you consume our Service. For example, if you consume our Service in North or South America – EST time zone applies. If you consume our Service in Europe, Middle East and Africa (“**EMEA**”) – GMT time zone applies.

5.3.3 Technical Support includes:

- The ability to open and manage support Incidents via the Support Site or, in the case of Severity (Priority) 1 Incidents, by telephone.
 - Severity 2-4 Incidents during Business Hours
 - Extended Support after hours for Severity 1 Incidents
- Interactive remote diagnostic support allowing Ipswitch Support engineers to troubleshoot securely through a real-time browser-based remote control feature.
- Access to Service documentation, Ipswitch Communities, knowledgebase articles, FAQs, webcast recordings and demos as such are made available by us.

5.4 Service Level Objectives: Response Times

5.4.1 We will use reasonable efforts to meet the Service Level Objectives stated in the table below and will provide continuous efforts to resolve Severity 1 service Incidents. For Severity 1 Incidents, we will work 24x7x365 until the Incident can be downgraded to a lower severity. For Severity 1 Incidents, your Support Contact(s) must be available at all times via telephone and online to provide us with relevant and requested information, data gathering and testing necessary to resolve the Incident. Severity 2-4 calls can be logged with us on a 24 hours per day, 7 days per week, 365 days per year basis and will be responded to during published business hours as per the Service Level Objectives table below.

Service Level Objectives				
Incident Severity (Priority)	1	2	3	4
Initial Response Time	2 hours	4 business hours	24 business hours	48 business hours



Service Level Descriptions		
Severity Level	Business Impact	Description
1	Critical	<p>System Down/Service Unavailable condition severely impacting Production environment involving:</p> <ul style="list-style-type: none">• Service outage or failure severely impacting Customer's business operations.• Widespread unavailability of business critical features/functions of the Service causing major disruption of the Customer's ongoing business operations.• There is serious performance degradation that significantly impacts a large group of Customer's end users.• Unscheduled Service downtime resulting from an emergency change request which needs to be applied to the system.• An issue for which there is no immediate workaround available.
2	High	<p>A high impact business condition where:</p> <ul style="list-style-type: none">• Service is available but its functionality is significantly restricted thereby causing disruption to Customer's normal business operations.• The Service's Available Functionality is not working, thereby negatively impacting Customer's business productivity.• There is no workaround available for the issue.
3	Low/Minor	<p>Service is available and Available Functionality is generally usable, however Service has an issue causing minor operational challenge(s). Issues may be isolated to specific end-users and/or may have little impact on the availability/functionality of the Service.</p>
4	Minimum/No	<p>A minor defect that has no impact on the Service, or a general enquiry on the functionality of the Service including how to/informational queries.</p>

5.5 Customer Responsibilities

5.5.1 You must designate one primary and up to four backup named individuals ("**Support Contacts**") to serve as liaisons with Ipswitch Support for each active Service from us. Support Contacts should be fully trained in the use and application of the Available Functionality. At our sole discretion, we may agree to additional Support Contacts in order to help you meet specific business requirements. You must notify us whenever the list of Support Contacts changes by logging an issue on Ipswitch Support Online.

5.5.2 In order to receive maintenance, support requests must contain all pertinent information, in English, including but not limited to, Customer or site identification name, Incident severity, Service name, area of Service (Production or Non-Production identified



by URL), Incident description, and a technical contact familiar with your environment or the problem to be solved. You must make reasonable efforts to communicate with Ipswitch Support in order to verify the existence of the problem and provide information about the conditions under which the problem could be duplicated.

5.5.3 As set forth above, for Severity 1 Incidents, your Support Contact(s) must be available at all times via telephone and online to provide us with relevant and requested information, data gathering and testing necessary to bring the Incident to resolution.

6. Admin Access

6.1 Activities for which Ipswitch Cloud Operations may request permission to act as a Admin include:

6.1.1 initial ORG setup (evaluation or production);

6.1.2 transition ORG from an evaluation to production environment;

6.1.3 Admin password change, when no other Admins exist;

6.1.4 removing IP Lockouts, if an Admin isn't able to log in;

6.1.5 modifying default access rules, if an Admin isn't able to login; or

6.1.6 troubleshooting Org specific issues/questions like setup questions, permission issues, or upload/download issues.

6.2 Our SysAdmin account cannot upload or download files, read a user's files, or send/receive messages in any organization other than the System organization.

6.3 To authorize Admin access to your System organization you will need to do one of the following:

6.3.1 Contact Ipswitch Technical Support requesting a web meeting, and provide Admin access to an Ipswitch Technical Support Engineer to troubleshoot and resolve their issue, while the customer observes the steps being performed.

6.3.2 Provide written permission (logged as electronic permission in a Salesforce case is acceptable) for Admin access to MOVEit Cloud Operations before the MOVEit Cloud Operations team will act as a Admin within your ORG.

6.4 Delay in providing authorization in a timely manner will affect our ability to meet the response and resolution times in Section 5.4 above.



The following section only applies to customers who subscribe to PCI Compliance Toolkit

PCI Compliance Toolkit

1. Services

- 1.1. We agree to provide you with our PCI Compliance Toolkit consisting of the following tools to demonstrate compliance interfacing with, and using the Service to support cardholder information holding, processing, or exchange:
 - 1.1.1. Executive Summary of Report on Ipswitch PCI Compliance
 - 1.1.2. Responsibility Matrix of Controls
 - 1.1.3. MOVEit PCI Cloud Compliance Report Template
 - 1.1.4. Support in working with your Qualified Security Assessor (QSA)(up to four (4) hours per year and subject to availability)
 - 1.1.5. PCI Attestation of Compliance (AOC) document
- 1.2. PCI Compliance Toolkit is an ancillary service to the Service and, except as expressly set forth in this Exhibit, is provided in accordance with the terms for the Service. PCI Compliance Toolkit must be co-termed with the Service, with relevant fee paid in full per annual assessment period. Assessment periods of less than a full year shall require complete payment of annual fee, due to the same annual assessment support requirements dictated by PCI.
- 1.3. PCI Compliance Toolkit is subject to the following:
 - 1.3.1. PCI Compliance Toolkit does not provide certification of PCI DSS compliance. Certification can only be provided by a third party QSA.
 - 1.3.2. Because certification of PCI DSS compliance depends on many factors beyond our control, we can not guarantee that use of PCI Compliance Toolkit will result in certification.
 - 1.3.3. Execution of a non-disclosure agreement is required.

2. Fees

- 2.1. Fees as specified by us for the PCI Compliance Toolkit Service (provided such fees shall not be less than the fees for the PCI Compliance Toolkit Service as of the effective date of this quotation), a one-time set-up fee, and other fees (if applicable) as described in the quotation. Services are invoiced annually in advance.

3. Notifications

- 3.1. We will notify you if we discover that a data breach has taken place. Data breaches are defined as unauthorized disclosure, modification or destruction of you data. We are only responsible to notify you of data breaches originated by our staff and subcontractors or unauthorized outside parties that successfully subvert access control mechanisms or other data protection controls. Monitoring for data breaches by client-managed users involving normal access control mechanisms are your sole responsibility.



The following section only applies to customers who subscribe to HIPAA Compliance Toolkit

HIPAA Compliance Toolkit

1. Services

- 1.1 We agree to provide you with our HIPAA Compliance Toolkit consisting of the following tools to demonstrate compliance interfacing with, and using the Service to support protected health information (PHI) holding, processing, or exchange:
 - 1.1.1 Executive Summary of Report on Ipswitch HIPAA Compliance
 - 1.1.2 Responsibility Matrix of Controls
 - 1.1.3 MOVEit HIPAA Cloud Compliance Report Template
 - 1.1.4 Support in working with your 3rd Party Auditor to demonstrate HIPAA compliance (up to four (4) hours per year and subject to availability)
 - 1.1.5 Advice for storing and transmitted ePHI with MOVEit Cloud
- 1.2 HIPAA Compliance Toolkit is an ancillary service to the Service and, except as expressly set forth in this Exhibit, is provided in accordance with the terms for the Service. HIPAA Compliance Toolkit must be co-termed with the Service, with relevant fee paid in full per annual assessment period. Assessment periods of less than a full year shall require complete payment of annual fee, due to the same annual assessment support requirements recommended by HIPAA.
- 1.3 HIPAA Compliance Toolkit is subject to the following:
 - 1.3.1 HIPAA Compliance Toolkit does not imply your compliance with HIPAA requirements. Compliance can only be determined by a third party auditor.
 - 1.3.2 Because compliance with HIPAA requirements depends on many factors beyond our control, we cannot guarantee that use of HIPAA Compliance Toolkit will result in compliance.
 - 1.3.3 Execution of a non-disclosure agreement is required.

2. Fees

- 2.1 Fees as specified by us for the HIPAA Compliance Toolkit Service (provided such fees shall not be less than the fees for the HIPAA Compliance Toolkit Service as of the effective date of this quotation), a one-time set-up fee, and other fees (if applicable) as described in this quotation number. Services are invoiced annually in advance.

3. Business Associate Agreement

- 3.1 We do not meet the definition of business associate as that term is defined by 45 C.F.R. Section 160.103. We do not create, receive, maintain, have access to, use, disclose or transmit protected health information (as that term is defined by 45 C.F.R. Section 160.103) to perform any service for you or on your behalf. If any arrangement between us and you results in our meeting the definition of business associate, and such arrangement does not fit within an exception to the requirement for a business associate agreement under the HIPAA regulations (45 CFR Parts 160 and 164), we will notify you in writing and execute our standard Business Associate Agreement prior to creating, receiving, maintaining, having access to, using, disclosing or transmitting protected health information pursuant to such arrangement.



The following section only applies to customers who subscribe to GDPR Readiness Toolkit

GDPR Readiness Toolkit

1. Services

- 1.1 We agree to provide you with our GDPR Readiness Toolkit consisting of the following tools to demonstrate compliance interfacing with, and using the Service to support cardholder information holding, processing, or exchange:
 - 1.1.1 Executive Summary of Report on Ipswitch GDPR Compliance
 - 1.1.2 Responsibility Matrix of Controls
 - 1.1.3 GDPR Compliance Report Template
 - 1.1.4 Support in working with your 3rd Party Auditor to demonstrate GDPR compliance (up to four (4) hours per year and subject to availability)
- 1.2 GDPR Readiness Toolkit is an ancillary service to the Service and, except as expressly set forth in this Exhibit, is provided in accordance with the terms for the Service. GDPR Readiness Toolkit must be co-termed with the Service, with relevant fee paid in full per annual assessment period. Assessment periods of less than a full year shall require complete payment of annual fee, due to the same annual assessment support requirements dictated by GDPR.
 - 1.3 GDPR Readiness Toolkit is subject to the following:
 - 1.3.1 GDPR Readiness Toolkit does not imply your compliance with GDPR requirements. Compliance can only be determined by a third party auditor.
 - 1.3.2 Because compliance with GDPR requirements depends on many factors beyond our control, we cannot guarantee that use of GDPR Readiness Toolkit will result in compliance.
 - 1.3.3 Execution of a non-disclosure agreement is required.
 - 1.3.4 Use of GDPR Readiness Toolkit is also governed by our standard Data Protection Addendum.

2. Fees

- 2.1 Fees as specified by us for the GDPR Readiness Toolkit Service (provided such fees shall not be less than the fees for the GDPR Readiness Toolkit Service as of the effective date of this quotation), a one-time set-up fee, and other fees (if applicable) as described in the quotation. Services are invoiced annually in advance.

3. Notifications

- 3.1 We will notify you if we discover that a data breach has taken place. Data breaches are defined as unauthorized disclosure, modification or destruction of you data. We are only responsible to notify you of data breaches originated by our staff and subcontractors or unauthorized outside parties that successfully subvert access control mechanisms or other data protection controls. Monitoring for data breaches by client-managed users involving normal access control mechanisms are your sole responsibility.