



Alfresco Cloud Services Specification

Hyland Cloud IS Policy Suite

Effective Date: August 11, 2025

Table of Contents

Introduction	3
Alfresco Cloud Overview	3
Alfresco Cloud Service Definition	3
Infrastructure	4
Data	5
Alfresco Cloud Platform Extensions and Access	5
Other Operations & Security Services	7
Customer Support & Training	8
Alfresco Cloud Service Offerings	9
Alfresco Cloud Service Levels	13
Alfresco Cloud Responsibilities	18
Alfresco Cloud Standards & Procedures	20

Introduction

The Alfresco Cloud Services Specification (“Specification”) details the various services supported, including the service definitions, service levels, security policies, and customer responsibilities, within the Alfresco Cloud Platform (“Platform”) provided by Hyland. This document **does not** address product support terms, which are covered in the [Alfresco Support Handbook](#). This Specification also assumes the Customer has agreed to the applicable Master Agreement (or Addendum) and has purchased the relevant Alfresco Cloud Services via an Order Form or other ordering document.

An electronic copy of the latest Specification is available to customers through the [Hyland's Alfresco web site](#) and through the [Hyland Trust Center](#). The Specification is reviewed by Hyland, periodically, and modifications of the revised Specification is posted on the listed web locations.

Alfresco Cloud Overview

The Platform, deployed as a Platform as a Service (“PaaS”), brings the Alfresco Digital Business Platform to organizations in an easy to consume fully managed environment. The Platform comprises three major components:

- On-demand services including Content as a Service, Process Automation as a Service, Governance as a Service, and AI as a Service
- A content app for organizations to use immediately with minimal configuration for enterprise content management consumed as a service
- A cloud-based, development platform enabling organizations to build and run their content intensive apps in a fully managed and hosted environment.

These cloud services enable organizations to build content intensive apps without the cost and complexity of deploying, managing, and updating the platform themselves. The Platform is a combination of infrastructure, operational capabilities, security monitoring and governance, and various products and solutions from the Alfresco product suite, as well as potential solutions from the Alfresco partner community.

Hyland supplies the software, infrastructure, personnel, systems, and processes to provide the Platform as described in this document.

Alfresco Cloud Service Definition

This Specification covers the various aspects of the service offerings running on the Platform and delineates the boundaries of the various components of a functioning Platform, including: the products and services provided by Hyland and its vendors, the products and services provided by Hyland's authorized solution providers, and the services and obligations fulfilled by the Customer and its partners or vendors. The information provided below applies for all Platform service offerings. See Alfresco Cloud Service Offerings for details regarding applications included with the

Platform.

Infrastructure

The Platform includes the necessary hardware, software, and networking infrastructure to operate and run the associated Alfresco application functionality up to the levels described in the service offering. This includes the necessary storage, operating systems, databases, load balancers, application servers, and related hardware components to host the purchased offering.

Third-Party Cloud Provider

Platform is built on public cloud infrastructure utilizing Amazon Web Services (“AWS”) in many key functions. Hyland deploys and manages the servers, OS services, storage, and network access and is ultimately responsible for the architecture and deployment of the cloud environment used to deploy the Platform. Hyland has no direct access to the physical infrastructure of AWS and enforces these requirements via contractual agreements.

Key Alfresco Cloud Architectural Components

The following is a summary of key architectural systems and services:

- Virtual Private Clouds are used to segment a Customer environment from other supporting technology and other customer’s environments.
- Web Application Firewalls are used to protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.
- Load Balancers are used for network traffic including support performance management requirements
- Application Servers are used to run and process services within the Platform and related Service Offerings and Applications
- High Availability Databases are used to support the application storage and performance needs as well as the Platform Business Continuity Requirements.
- Domain authentication technology is used for Customer access and Alfresco administration access. A Directory Service is used to provide user provisioning for access and group information for authorization inside the application.
- The Platform utilizes secure storage technology configured for multiple available zones to store solution content and files.
- The Platform utilizes TLS 1.2/1.3 for encryption in transit, and AES 256 for key management and encryption at rest. All communication to infrastructure resources, such as database, storage, directory, etc., is also encrypted.

Data

Customers maintain ownership of all Customer Data uploaded to their solution through the full lifecycle period. Customer Data is encrypted in transit and at rest within the Platform. Strict access control is in place. Customer administrators control user access, user permissions, and data retention with respect to the solution. Hyland treats Customer Data with the most restrictive data classification and applies technical controls as described in this Specification to comply with all applicable privacy and confidentiality laws, rules, and regulations (e.g., data encryption at rest and in transit, strict access controls). The Customer is responsible for ensuring that their solution meets the Customer's legal and/or compliance obligations.

As a multi-instance hosting platform, Hyland provides logically separated storage and Virtual Private Cloud technologies for each Customer, which prevents the documents and metadata belonging to multiple tenants from being comingled. Additionally, the Platform does support, in certain circumstances, the ability to choose the geographical region in which the Customer solution will be deployed.

Alfresco Cloud Platform Extensions and Access

The Platform supports several methods for accessing as well as extending the Platform in a supportable manner.

Platform Extensions

The primary method for extending the Platform is via custom applications using the Public REST APIs or Content Management Interoperability Services (CMIS) API. However, the Platform does support content repository extensions and ADF application hosting in certain Tiers. Customers should access the [Alfresco Product Documentation](#) website for more information regarding best practices on developing for the Platform.

For content repository platform extensions, the Platform supports all platform extensions that can be secured and managed in a PaaS environment. It supports deployments of custom platform repository JAR files or AMPs following a CI/CD process which incorporates industry best security practices.

There are a few exceptions that are not supported, and those are listed in the following section.

Unsupported Extensions

The following platform extensions and access methods are not available to be extended in the Platform. Customers are prohibited from using these extensions on the Platform.

- SURF customizations

- Custom AMPS for Share or Share Extensions
- WAR file modifications (via AMPs) for Share (exception is existing Partner add-ons that are tested and certified)
- Aikau support
- Bootstrap content
- Permissions or Custom Roles
- user-defined Content Stores
- Admin Console Components
- Authentication Extensions
- Patches
- FTP, WebDAV or CIFS usage
- Customizations to embedded workflow
- Inbound Email: The IMAP protocol is not supported. The Outlook Connector and Inbound SMTP are supported for Inbound Email

Platform Access Management

The Platform includes access management services as well as role-based access control for the monitoring and operation of the Platform. Active Directory Domains for domain authentication technology is required for both Customer and Hyland administrative access. Additionally, Platform supports integration to single sign-on (SSO) solutions using SAML integration to leading Identity Providers (IdPs) for secure access and authentication. LDAP integration capabilities are provided via a LDAP Agent or APIs for Customers to securely send their user and group information from their corporate LDAP domain to the Platform domain. Customers must provide an IdP that supports the SAML protocol, such as ADFS for integration with the Platform.

Application access to Alfresco Cloud Service Offerings is done via a Hyland provided URL using web browsers managed by the Customer. Customers may elect to provide their own URL. In this case, Customers must configure their own DNS and Certificates. Hyland will provide a DNS that can be used as the CNAME to complete the configuration.

More information about the access configuration is available on the [Alfresco Product Documentation](#) website.

Access Security Requirements

Access control is a critical element for enforcing cloud security requirements and best practices. Ultimately, Customers are responsible for the management of their users including:

- managing the entire user access lifecycle,
- managing user permissions to the application features and local directory services,
- managing the Active Directory syncing with the Platform,

- enforcing corporate password policies, and
- managing web browser multi-factor authentication configuration.

Customers must ensure applications and usage have the appropriate control in place to prevent unauthorized access to data and processes. Failure to comply with requirements may impact the ability to operate the service. Moreover, Hyland will enact security incident response protocols for suspicious activity and other security concerns, the result, in which, may include the suspension of services until the security issue is resolved by Hyland's security professionals.

Other Operations & Security Services

The Platform includes other services to support the ongoing operations and security of the Platform. Key services include the following:

- **People:** Hyland employees must undergo comprehensive screening during the hiring process. Background checks and reference validation are performed to determine whether candidate qualifications are appropriate for the proposed position. Hyland personnel are granted only the specific privileges required for them to carry out their normal duties in supporting the Platform. These individuals are also subject to additional, ongoing information security and confidentiality training in accordance with Hyland's security policies.
- **Infrastructure & Application Monitoring:** The Platform provides application and infrastructure monitoring. Uptime and other types of system monitoring information on the environment is available for Customers via [Hyland Community](#).
- **Patch & Upgrade Management:** For all hardware, networking, and software components within the Platform, Hyland provides scheduled patch and upgrade management as part of the Platform. Hyland will monitor for applicable updates to supported components and software, and schedule updates via change management procedures. The Platform utilizes a "Blue-Green" deployment technique to eliminate downtime ("zero-downtime deployments") and reduce risk.
- **Business Continuity & Disaster Recovery:** A base level of standard security, backup, and disaster recovery (DR) options is included with all Alfresco Cloud Service offerings.
- **Logging and Event Management:** The Platform provides a modernized event capture and logging infrastructure to provide feedback on all aspects of the Platform, including, but not limited to, security instances, infrastructure instances, security events, and application issues.
- **Encryption:** The Platform supports full encryption capabilities, including key management services, for data in motion between all Platform components as well as data at rest within the Platform.
- **Change Management:** Hyland provides the process and infrastructure for Customers to introduce change into their environment via change management. Hyland follows internal change management procedures. Generally, change requests are submitted via a change management system and are then evaluated by subject matter experts. Upon approval by such subject matter experts, changes are implemented, documented, and tested. Customers are responsible for testing all configuration changes, authentication changes, and upgrades to their solution.

Customer Support & Training

Hyland has several processes to support Customers' successful implementation of their Alfresco solution including:

- **Alfresco Support Portal & Handbook:** Website that serves as the initial point of contact for incidents, issues, enhancements requests, and new service offerings. Details on accessing the Support Portal, methods of contact, and other related items can be found in the Alfresco Support Handbook found on [Hyland Community](#).
- **Customer Support for Cloud Solutions:** 24x7x365 access to the Alfresco Support Portal for operations staff and support requests, email, and phone support for Alfresco solutions.
 - For prioritization and service level targets for production issues such as outages, major impacts, service interruptions, these service levels for the Platform follow the [Severity Definitions](#) and [Service Level Targets](#) as defined in the Alfresco Support Handbook.
 - Typical Level 6 requests that may require additional support from the Platform operations teams include:
 - **New License Keys Requests** - Renew and create new Product License Keys and Install keys on requested server.
 - **Additional Capacity Units/Storage Requests** - Customers can purchase additional capacity units (storage) in increments. Customers must coordinate with Hyland on scheduling, if applicable.
 - **Requests to Restore from Backup** - Customers can request that data be restored from backup. Customers must coordinate with Hyland on scheduling, if applicable.
 - **Requests to Deploy Product Extensions ("customizations") in Production or Staging** – Upon completion of their testing including functionality, performance, and security, Customers can work with Hyland to deploy customizations into their respective environments if they pass Hyland's requirements for security, performance, and change management. Customers must coordinate with Hyland on scheduling.
 - Customers can report potential product vulnerabilities using Hyland Community. For organizations without access to the Support Portal, product vulnerabilities can be reported using the information on [Hyland.com](#).
- **Customer Success Manager:** A Customer Success Manager (CSM) that will deliver personalized guidance to support the installation of solutions.
- **Product Support Levels:** The product support level is dictated by the offering. In some instances, Customers can purchase Premier support options, such as Technical Account Manager (TAM) that can be granted full access to their environment. Customers should work with their Hyland Account Manager to determine what options are available.
- **Training:** Detailed training on the Platform and its service offerings is available via the [Hyland University](#), additional fees may apply.
- **Professional Services:** Access to professional services and partner resources can be coordinated and granted as required. A separate Statement of Work or Services Proposal ("SOW") may be required.
- **Off-boarding Assistance:** Hyland will provide off-boarding assistance in accordance with the contractual terms between Hyland and the Customer. Professional Services may be required.

Additional information on Hyland's Alfresco support programs can be found in the Alfresco Support Handbook.

Alfresco Cloud Service Offerings

This section includes an overview of the current offerings available in the Platform. Each offering is described below, along with any specification requirements and/or relevant details for that offering.

- Alfresco Content as a Service
- Alfresco Governance as a Service
- Alfresco Process Automation as a Service
- Alfresco AI as a Service
- Additional Services

Alfresco Content as a Service

Alfresco Content as a Service offers a modern Content Services platform for organizations that require enterprise-grade scalability, performance, and support for business-critical content and compliance in a fully managed environment. This is the base offering for all Platform solutions.

The Content as a Service offering includes the Alfresco Content Services, Alfresco Application Development Framework (ADF), Alfresco Digital Workspace, Search, and the S3 Connector.

The ADF is a modern JavaScript-based framework to rapidly build engaging web applications on top of the content repository. It provides a rich set of reusable Angular UI components and services, command-line tooling and JavaScript APIs that surface Alfresco Process, Content and Governance Services (if purchased).

Alfresco Content as a Service Tiers

The Alfresco Content as a Service offering is available by tiers that set certain parameters of the environment, including potential software components, environments, and support options.

The following table depicts the default offerings per tier and identifies differences between tiers where appropriate. Any changes to these defaults will be listed on the Order Form or other ordering document, which will be the contract of record for users, storage, and other available 3rd party options.

OFFERING COMPONENT S	Consumption/ Request based model	Tier IV SLA	Tier III SLA	Tier II SLA	Tier I SLA
	User Based model	Tier I/XL SLA	Tier II/Large SLA	Tier III/Medium SLA	Tier IV/Small SLA
Instances		Production Staging/Pre-Production ¹	Production Staging/Pre-Production	Production Staging/Pre-Production	Production
Named Users		See Order Form			

Storage Level	See Order Form			
Security - Authentication	OAUTH/SAML	OAUTH/SAML	OAUTH/SAML	OAUTH/SAML
Security - User Provisioning	LDAP Agent	LDAP Agent	LDAP Agent	LDAP Agent
Backup Policy	30 Day Storage	30 Day Storage	30 Day Storage	30 Day Storage
Availability ⁱⁱ	Fault Tolerant (Active-Active)	Fault Tolerant (Active-Active)	High Availability	High Availability
Disaster Recovery	Multi-Region Support	Multi-Region Support	Multi-Region Support	Multi-Region Support
Product Extensions	APIs, UI, and Customer Product Extensions	APIs, UI, and Customer Product Extensions	APIs, UI, and Customer Product Extensions	APIs, UI, and Customer Product Extensions
Support Package Overview	Enterprise (Premier \$)	Enterprise (Premier \$)	Enterprise (Premier \$)	Starter
University Passport (Education)	5 Users	5 Users	3 Users	1 Users

Alfresco Governance as a Service

The Alfresco Governance as a Service brings a combination of simplicity and control to information governance. It strengthens compliance by integrating records management capabilities into business processes and allowing for automation in the complete record lifecycle—from capture through retention to final destruction. Alfresco Governance as a Service also provides the capability to perform deep archive (cold storage) use cases and includes the Alfresco Content Connector for AWS Glacier as part of the system.

The Governance as a Service option is added to the Alfresco Content as a Service environment and increases the functionality of that offering within the platform. The metrics and limits for Alfresco Content as a Service subscriptions also apply to Alfresco Governance as a Service. Similarly, the service levels, system sizing capabilities, performance specifications, etc. in this document applicable to Alfresco Content as a Service carry over to Alfresco Governance as a Service as well.

Alfresco Process Automation As a Service

Alfresco Process Automation helps enterprises to automate document-centric processes quickly and easily—such as customer onboarding, contract management, claims processing—or any process rich in unstructured content.

Process Automation Applications are built in the Alfresco Modelling Application and deployed, managed, and monitored in the Alfresco Admin Application. End-users start processes and manage their work from the Alfresco Digital Workspace or their own application based on the Alfresco Application Development Framework (ADF).

An Alfresco Process Automation Application can consist of the following self-contained components:

- Alfresco Content Models
- Alfresco BPMN Processes
- Alfresco Triggers
- Alfresco Scripts
- Alfresco UI Applications
- Alfresco Connectors
- Alfresco Forms
- Alfresco DMN Decision Tables

The Alfresco Process Automation is sized by Tier and sold with the Alfresco Content Services platform (Alfresco Content as a Service). Specific details are provided on the Order Form for any usage restrictions or sizing guidelines.

Alfresco AI as a Service

Alfresco AI as a Service (AI) makes it simple and easy for Customers to consume the benefits of the complex AI and Machine Learning technologies that can be leveraged via this offering without needing technical expertise. This offering works with the Alfresco Content as a Service offering to provide a seamless experience that helps companies extract knowledge from content and drive automation. As with Alfresco Governance as a Service, the Alfresco AI as a Service offering requires the purchase of Alfresco Content as a Service. The metrics and limits for Alfresco Content as a Service subscriptions also apply to Alfresco AI as a Service. Similarly, the service levels, system sizing capabilities, performance specifications, etc. in this document applicable to Alfresco Content as a Service carry over to Alfresco AI as a Service as wellⁱⁱⁱ.

For low-code developers who wish to use commodity AI services in their content applications, the service:

- Hides complexity of sending content to Natural Language, Image Detection, Intelligent OCR, and other content-driven AI capabilities allowing low-code developers to write simple, targeted rules
- Allows the ability to define very simple rules and actions based upon sophisticated AI output
- Comes with powerful out of the box rules/actions to add to folders, content, or custom content types
- Simplifies end-to-end processing of ingestion of documents to extracting information
- Allows the ability to re-use AI output for multiple purposes without re-running AWS service AI algorithms
- Allows the ability to build more helpful user interfaces that allow users to choose selected items or features based upon confidence levels or human knowledge
- Simplifies conversion of file format types that the AI service needs, by connecting

transformation engines to pass the right file format to the AI service, or to connect AI algorithms together, such as passing intelligent OCR.

Details of the various service offerings currently useable within Alfresco AI as a Service are below:

- **Extract Document Insights with Natural Language Processing**
 - Alfresco Intelligence Services uses Natural Language Processing (NLP) to drive more value out of the content that is stored in Alfresco. It analyzes text to gain insights. It removes the complexity of building text analysis capabilities into applications by making powerful and accurate natural language processing available with a simple API.
 - Entities (e.g., people, places, products, dates, events, organizations, quantities, things)
 - Language (100+)
- **Extract Textual Context and Analysis from Images**
 - Alfresco Intelligence Services removes the complexity of building image recognition capabilities into applications by making powerful and accurate analysis available with a simple API. Alfresco Intelligence Services uses deep learning technology and image recognition to extract textual context from images storing that information in Alfresco Content as a Service as document metadata. It can identify:
 - Objects (e.g., building, phone, car)
 - People (e.g., famous, noteworthy, prominent people's names)
 - Text (e.g., street names, captions, product names, license plates)
 - Scenes (e.g., parking lot, beach, city)
- **Extract Text and Data from Scanned Documents**
 - Alfresco Intelligence Services provides intelligent OCR and information processing service that allows organizations to take a mass ingestion of information and automatically classify the content faster than ever before. It is a self-learning service that improves its quality over time.
 - It automatically detects a document's layout and the key elements on the page, understands the data relationships in any embedded forms or tables, and extracts everything with its context intact.

Additional Services

The Platform supports a number of additional services and options that can be purchased and included in a subscription. Add-on services can change from time to time. As of the date of this document, the following tables describes the then-current additional add-on services. Customers should reference their Order Form or other ordering document to determine if an additional service option has been selected.

Add-On Service Options	
Alfresco Cloud Setup	One-time fee to initialize and provision the instance as well as conduct all the custom setup options for integration and authentication.
Additional Capacity Unit	Provides additional Capacity Units per TB of storage to support the needed space for the backup copy of the data, the required indexes to search the data, and the necessary management and security overhead to move and secure the data.
Additional Staging/Pre-Production Environment	Provides an additional staging/pre-production environment as defined in this specification.
Alfresco External Content Services	Provides external user access for authorized external users. External user access and limits will be documented in the Order Form.

Add-On Service Options	
Alfresco Modules, Add-ons & Components:	
Alfresco Enterprise Viewer	Hyland will deploy, maintain, and administer the Alfresco Module, Add-on, and/or Component as defined in the Order Form.
Alfresco Content Accelerator - Policy & Procedure	Hyland will deploy, maintain, and administer the Alfresco Module, Add-on, and/or Component as defined in the Order Form.
Alfresco Content Accelerator - Claims Management	Hyland will deploy, maintain, and administer the Alfresco Module, Add-on, and/or Component as defined in the Order Form.
Alfresco Content Accelerator – Human Resources	Hyland will deploy, maintain, and administer the Alfresco Module, Add-on, and/or Component as defined in the Order Form.
Alfresco Content Connector for SAP	Hyland will deploy, maintain, and administer the Alfresco Module, Add-on, and/or Component as defined in the Order Form.
Alfresco Content Connector for Salesforce	Hyland will deploy, maintain, and administer the Alfresco Module, Add-on, and/or Component as defined in the Order Form.
Alfresco Content Connector for Microsoft Outlook	Hyland will deploy, maintain, and administer the Alfresco Module, Add-on, and/or Component as defined in the Order Form.
Alfresco Cloud Enhanced Transforms	Hyland will deploy, maintain, and administer the Alfresco Module, Add-on, and/or Component as defined in the Order Form.
Third-Party Applications:	
Alfresco Cloud Marketplace Connector	Hyland will deploy and host the third-party/oem application as defined in the Order Form.
Arender Viewer	Hyland will deploy and host the third-party/oem application as defined in the Order Form.

Alfresco Cloud Service Levels

Service Level Agreements (“SLA”) described in this Specification pertain to the availability of the infrastructure for all Alfresco Cloud Service offerings. This document **does not** address Support Services Terms on product software support, response times, and/or priority definitions. This information can be found in the Alfresco Support Handbook on [Hyland Community](#).

Service Level Definitions

“**Downtime**” is calculated as the aggregate time (in minutes) each calendar month, as confirmed by Hyland following written notice from the impacted Customer, that the applicable Alfresco Cloud Service is experiencing a System Outage (as defined below). The length of Downtime will be measured from the time an incident occurs as confirmed by Hyland until the time when Hyland’s testing confirms that the failure condition(s) reported are no longer present. Downtime does not

include any failure condition(s) which occur due to an Exclusion Event (see below).

“Exclusion Event” means any of the following occurrences:

- (1) Scheduled or emergency system maintenance or other service interruptions agreed to by the Customer for the purpose of allowing Hyland to upgrade, change, maintain, or repair the Services or related facilities;
- (2) failure of a Customer’s or user’s equipment or facilities;
- (3) acts or omissions of a Customer or its user, including but not limited to (a) performance or non-performance of any services by a third party (other than Hyland) contracted by the Customer to provide services to the Customer or its users related to the Alfresco Cloud Service, (b) any failure that the Customer mutually agrees is not due to fault of Hyland or Hyland’s contracted third party service provider, (c) failure of any code or configurations managed or written by the Customer or any third party vendor to the Customer, or (d) any unauthorized use or access by the Customer or any of its users;
- (4) the occurrence of a force majeure event;
- (5) Internet failure or congestion;
- (6) any defect or failure of any third party software or hardware that Hyland may agree to host as part of the Alfresco Cloud Services offered, including where the manufacturer has discontinued maintenance and support of the third party software or hardware;
- (7) failure of equipment or systems not within the network, or of equipment or systems not provided, or not under the control or direction of Hyland including equipment or systems Hyland may obtain or contract for at the request of the Customer; or
- (8) failures or other failures caused directly or indirectly by known or unknown computer viruses, worms or other malicious programs (assuming Hyland hasn’t breached any of its obligations here or in the applicable agreement relating to virus protection protocols).

“Failover Notice” is a written notice (which notification may be made by electronic communication, including e-mail) indicating that Hyland is initiating a data center failover for the applicable Alfresco Cloud Service

“Monthly PaaS Fees” will be calculated based on the recurring monthly fees for the directly impacted Alfresco Cloud Services(s) during the month in which the applicable performance deficiency occurs, excluding any taxes, one-time fees, third party fees, travel or expense, professional services or similar additional fees. If fees are charged on an annual basis, the monthly fee will be the annual fees divided by 12, subject to the same exclusions above.

“Monthly Uptime Percentage” is calculated as the total number of minutes in a calendar month, minus the number of minutes of Downtime (as defined above) in such month, divided by the total number of minutes in such month.

“Recovery Point” means the minimum number of hours (prior to the time Hyland provides a Failover Notice) that the Customer’s data shall be stored within the Alfresco Cloud Service to qualify as eligible data. Customer data is deemed **“eligible”** if Hyland confirms it has been stored within the Alfresco Cloud Service for a number of hours (prior to the time Hyland provides a Failover Notice) that exceeds the applicable Recovery Point objective defined in Table 2 below.

“Recovery Time” means the number of hours from the time the required Failover Notice is

delivered to the time the Alfresco Cloud Service has been Restored (excluding any time during that period if/when an Exclusion Event affects both the current primary and secondary data centers).

“Restoration” occurs once access to the Alfresco Cloud Services has been restored such that:

- (1) eligible Customer content can again be stored in the Alfresco Cloud Service; and (2) new associated Customer Data (as anticipated by the applicable Alfresco Cloud Service(s) impacted) can be input into the Alfresco Cloud Service.

“System Outage” is defined by a loss of network connectivity or system availability resulting in either the Platform being not available by the user interface or API, as defined above, for any period outside of a scheduled maintenance window or emergency maintenance obligation.

Service Level Commitments

Table 1: Monthly Uptime Percentages

OFFERING COMPONENTS	Consumption /Request based model	Tier IV SLA	Tier III SLA	Tier II SLA	Tier I SLA
	User Based model	Tier I/XL SLA	Tier II/Large SLA	Tier III/Medium SLA	Tier IV/Small SLA
Monthly Uptime Percentage					
Monthly Uptime Percentage		99.90%	99.80%	99.50%	99.0%
Monthly Uptime Percentage Service Level Credits					
Monthly Uptime Percentage Service Credit Ranges and Applicable Credit Determinations	99.89 – 99.0%	99.79 – 99.0%	99.49 – 99.0%	Less than 99.0%	15% of the Monthly PaaS Fee
	15% of the Monthly PaaS Fee	15% of the Monthly PaaS Fee	15% of the Monthly PaaS Fee	15% of the Monthly PaaS Fee	
	Less than 99.0%	Less than 99.0%	Less than 99.0%	Less than 99.0%	
	20% of the Monthly PaaS Fee	20% of the Monthly PaaS Fee	20% of the Monthly PaaS Fee	20% of the Monthly PaaS Fee	

Table 2: Business Continuity

OFFERING COMPONENTS	Consumption /Request based model	Tier IV SLA	Tier III SLA	Tier II SLA	Tier I SLA
	User Based model	Tier I/XL SLA	Tier II/Large SLA	Tier III/Medium SLA	Tier IV/Small SLA
Business Continuity					
Recovery Point Objective		6 hours	6 hours	12 hours	24 hours
Recovery Time Objective		8 consecutive hours	8 consecutive hours	24 consecutive hours	24 consecutive hours
Business Continuity Service Level Credits					
Business Continuity Service Level Credit		25% of the Monthly PaaS Fee	25% of the Monthly PaaS Fee	25% of the Monthly PaaS Fee	25% of the Monthly PaaS Fee

Service Level Commitment Terms

Monthly Uptime Percentage. Hyland will meet the Monthly Uptime Percentage corresponding to the applicable service level purchased by the Customer, as identified in Table 1 above, during each calendar month.

Business Continuity. Hyland shall provide a Failover Notice prior to commencing such a failover of the Platform from the current region to any backup region. In the event Hyland delivers a Failover Notice to Customer, Hyland shall restore the Platform within the applicable Recovery Time objective set forth in Table 2 above (except to the extent caused or prevented by an Exclusion Event).

The Platform Business Continuity Management program establishes the standards and procedures that support the availability and resiliency of the Platform. The Alfresco Cloud Service plans are reviewed annually by representatives in all applicable Hyland business and functional areas to ensure appropriate coverage and consideration of business objectives.

Downtime Report. Following the occurrence of a Downtime event, upon request by the Customer, Hyland shall provide a report which will include, as applicable, a detailed description of the incident, start and end times of the incident, duration of the incident, business/functional impact of the incident, description of remediation efforts taken, and a description of outstanding issues or tasks relating to the incident.

Exclusive Remedies Terms

Monthly Uptime Percentage. In the event the Monthly Uptime Percentage during any calendar month is less than the applicable Monthly Uptime Percentage set forth in the Table 1 above, the Customer shall be eligible to receive the applicable credit against PaaS Fees specified in Table 1

above, provided Customer submitted a technical support request within twenty-four (24) hours of such Downtime.

For example, purposes only, assume the Customer purchased the Tier 2 offering. In such event:

if Monthly Uptime Percentage is equal to or greater than 99%, but less than 99.5%, the customer shall be eligible to receive a one-time credit against PaaS Fees in an amount equal to fifteen percent (15%) of the Monthly PaaS Fee.

Business Continuity. If, following delivery of a Failover Notice, the Alfresco Cloud Service is not Restored within the applicable Recovery Time objective set forth in Table 2 above, the Customer shall be eligible to receive the applicable credit against PaaS Fees specified in Table 2 above, provided the Customer submitted a technical support request within twenty-four (24) hours of such Downtime.

Maximum Service Level Credit. Notwithstanding anything to the contrary, Customers are only entitled to a maximum of one (1) service level credit for all events occurring in a particular calendar month. The Customer shall be entitled to only the largest service level credit which may be payable for one or more of the service level failures occurring in such calendar month.

Application of Service Level Credits. Service level credits will be applied first to any outstanding amounts which are due and owing from Customer, and then to future PaaS Fees.

Termination Remedy. If Customer earns a service level credit either: (i) in two (2) consecutive calendar months, or (ii) in three (3) calendar months during any six (6) consecutive month period; then the Customer may, by written notice to Hyland delivered within thirty (30) days after the last credit described in either clause or (i) or (ii) above is earned, terminate the subscription to the Alfresco Cloud Service(s) to which the credit(s) specifically apply.

Exclusivity. The remedies set forth above constitute the sole and exclusive remedies available to a Customer for any failure to meet the service level commitments set forth in this Specification.

System Maintenance

For the purposes of the Service Level Commitment, Scheduled Maintenance is defined as:

Alfresco Scheduled Maintenance Windows.

Windows Modification or repairs to shared infrastructure or platform patching and upgrades that Hyland has provided notice of at least seventy-two (72) hours in advance or that occurs during times noted below in the Alfresco Schedule Maintenance Windows by Region section.

Alfresco Scheduled Maintenance Windows by Region:

EU customers: 12AM - 2AM CET

US customers: 12AM - 2AM EST

APAC Customers: 12AM - 2AM JST

Scheduled Customer Maintenance. Maintenance of Customer configuration that Customer requests and that Hyland schedules with Customers in advance (either on a case-by-case basis, or based on standing instructions), such as hardware or software upgrades.

Scheduled Customer Deployments. Customer requests that Hyland schedules with the Customer in advance (either on a case-by-case basis, or based on standing instructions), for the deployment of customizations, add-ons, or new roll-outs of services that require the system to be restarted or taken offline.

Emergency Maintenance. Critical unforeseen maintenance needed for the security or performance of Customer configuration or the Alfresco Cloud Service's network.

Alfresco Cloud Responsibilities

Hyland Responsibilities

Hyland will:

1. Provide access to the Platform for use by the Customer by deploying application and solution customizations and managing system components including performing the appropriate infrastructure sizing within the Platform boundaries, as defined within this document. This hosting service will be delivered in a manner that is consistent with the underlying agreement.
2. Manage configuration changes performed on behalf of Customer based on written requests from authorized Customer employees or authorized third parties, when applicable.
3. Maintain logging and monitoring processes which includes capacity management and alert response procedures in alignment with the incident response handling program.
4. Perform vulnerability and patch management including the monitoring and deployment of security updates in accordance with Service Level requirements.
5. Report and respond to qualified security incidents. If Hyland has determined the Customer's deployment has been negatively impacted by a security incident, Hyland will deliver a root-cause analysis ("RCA") summary to the Authorized Support Contact. The RCA will not be unreasonably delayed but will only occur after initial corrective actions have been taken to contain the threat and stabilization of the Platform has been completed. Assistance from the Customer may be required.
6. Respond to reported availability incidents. This may include, but is not limited to, activities required to restore access to the Customer's deployment. If Customer has reported an availability incident to Hyland Technical Support, Hyland will deliver a RCA or Downtime Report to the Authorized Support Contact. The RCA will not be unreasonably delayed but

will only occur after initial corrective actions have been taken to contain the threat and stabilization of the Platform has been completed. Assistance from Customer may be required.

7. Maintain disaster recovery preparations, including data replication, backups, and periodic reviews.
8. Use reasonable efforts to test work performed by Hyland employees and Hyland vendors.
9. Use reasonable efforts to monitor the overall security and availability of the Platform.
10. Upon request of Customer, provide information on available features and functionality of Customer's deployment that could assist Customer in storing confidential or personal identifying information.

Customer Responsibilities

Customer will:

1. Designate Authorized Customer Administrators who are authorized to communicate Customer's policies, perform access control, submit configuration requests to Hyland, or speak authoritatively on behalf of Customer and shall receive and provide, as applicable, all notifications related to maintenance, security, service failures and the like.
2. Perform user authorization and password management for users within the Customer's solution, including controlling user group membership and the related permissions.
3. Be responsible for revocation of access to the environment immediately for unauthorized users and reporting changes to the Authorized Customer Administrator as soon as possible to prevent inappropriate access and privileges.
4. Access the Platform remotely in accordance with the technical requirements necessary for secure access and functionality.
5. Provide web browser software, other compatible client software, and necessary connectivity to the Platform.
6. Ensure that allocated storage limits are not exceeded.
7. Install and manage system components and processes outside of the Platform boundaries, as described in this document.
8. Identify and make use of Alfresco product features to properly store confidential information and personal identifying information.
9. Be responsible for ensuring that the deployment meets Customer's legal, regulatory, and other compliance obligations and use best efforts to ensure the accuracy, quality, and legality of the data being provided to Hyland.
10. Be responsible for all testing of the cloud deployment upon installation prior to any production use, except as otherwise set forth in a Hyland Services Proposal, when applicable.
11. Be responsible for all testing of any configuration changes to the Alfresco software, except as otherwise set forth in a Hyland Services Proposal.

12. Transfer files to the Platform using supported protocols and standards, ensuring all content uploaded is free of malware/viruses.
13. Use reasonable efforts to monitor business processes and quality controls that are unique to the Customer's Hosted Solution. This includes batch processing of documents uploaded to the Platform.
14. Comply with current technical documentation, including API and developer guides and provide Customer AWS accounts when required for functionality. Technical documentation is maintained and available from [Alfresco Product Documentation](#).
15. Validate any custom applications and code to be run out of the Platform is stable, secure, and will not cause a performance or security risk to the Platform, including cloud applications, associated computer resources, and other Platform Customers. If issues are discovered, Hyland may reserve the right to suspend service until the issues are resolved.
16. Report and respond to security and availability incidents of which Customer becomes aware. Customer should report all such incidents to Hyland's Technical Support Department. The Hyland Technical Support representative will serve as the primary point of contact for the duration of the support issue unless Customer is advised differently by Hyland.

Alfresco Cloud Standards & Procedures

To ensure the integrity of the environment and the systems and users involved in the maintenance and governance of said systems, Hyland maintains the following good computing practices and procedures subject to ongoing review, testing, and adjustment as needed. This section is provided as a summary of the practices, procedures, and guidelines, as instituted in the actual policy currently in place. The Platform and operations are governed by the Hyland Cloud IS Policy Suite ("HC IS Policy Suite") which aligns the ISO/IEC 27001:2022 standard including Annex A controls.

Acceptable Use

As a platform service, continued use of the services is critical to all our customers. Use is subject to the standard Acceptable Use Policy terms Hyland provides for the Platform. We monitor use by each of our customers, and we may adjust or limit usage if we determine any abuse, excessive use or similar events are occurring (such as reducing data flows / ingestions that are causing instability in the environment).

Access Control

Access to the infrastructure is strictly controlled. Infrastructure access is exclusively granted through managed, audit-tracked controls that employ PKI encryption. n. Accounts with access to the production environments are regularly reviewed. Access credentials are only provided on an "access required" basis to personnel who have undergone appropriate training and have passed all applicable background checking and onboarding requirements at the time of hire. These individuals are also subject to additional, ongoing information security and confidentiality training in accordance with Hyland's security policies.

Security

Software Development Life Cycle (SDLC)

Hyland has controls throughout the software development life cycle to verify the security of Hyland's product portfolio including manual and automated tests as part of the CI/CD process. As code is committed into the source code repositories, there are static analysis tools to verify the code against well-known vulnerabilities such as the OWASP Top 10 and the CWE/SANS Top 25.

To help ensure software supply chain security, Hyland uses tools that scan compiled Alfresco code (including third party software libraries and components, if applicable) for known vulnerabilities from the NIST Vulnerability Database and other sources. This happens as part of the CI/CD process within the SDLC and continuously for all supported versions of Alfresco products. This alerts the Alfresco engineering teams of the need to upgrade libraries. To this aim, Hyland also uses tools that scan for new versions of third-party components to be available and automatically create pull requests to upgrade to the new versions.

On an at least annual basis, Hyland conducts an application penetration test using a third-party security firm.

Cloud Platform Security

The infrastructure in the Platform is configured with firewalls, security groups and network access control lists to only allow expected network traffic. To protect your connections to the Platform, all web traffic will be protected using TLS 1.2 as a minimum. Additionally, the environments are protected by AWS load balancers.

Virtual machines that make up the Platform are built on security hardened base operating systems, which are regularly updated with the latest security patches.

Hyland maintains a vulnerability management program to identify, assess, mitigate, and protect against security vulnerabilities and threats. Patch management procedures have been established to ensure the timely implementation of security patches in accordance with their assigned severity and risk.

Hyland protects the AWS infrastructure that hosts the Platform by making use of the AWS GuardDuty tool to enable threat detection and continuous monitoring for malicious activity and unauthorized behavior to protect AWS accounts, EC2 workloads, container applications, and data stored in Amazon Simple Storage Service (S3). The AWS infrastructure follows the CIS Amazon Web Services Foundations Benchmark.

The Platform protects data by providing encryption at-rest and in-transit encryption capabilities throughout the Platform. These capabilities use cryptographic standards at current industry-standard levels and make use of the underlying AWS services for Key Management.

Periodic vulnerability scans are performed across the Platform networks to proactively address potential security issues. In addition, penetration tests are performed by a third-party firm at least annually.

Incident Management

Hyland has an incident response policy and plan for dealing with information security incidents that occur in the Platform in a timely manner and with all relevant communication. Our response plan includes identifying the necessary involved parties, defined management protocols of the incident, reporting protocols and requirements for Alfresco personnel, defined incident response, notification and handling protocols and protocols for post-incident reviews.

Business Continuity & Disaster Recovery

Hyland has established comprehensive disaster recovery processes for the Platform. If the Service is disrupted, Hyland will initiate its disaster recovery protocols to help ensure the timely restoration of the Service for the customer base. Depending on the type of disruption that has occurred, Hyland may elect to phase restoration to maximize benefit for its customer base (e.g., first restore the service with indexes being rebuilt as required). Any data not immediately accessible after a disruption in the Service will be restored from the most recent backup.

Monitoring

The Platform environment is monitored for availability, capacity, and security incidents. All infrastructure components, and the Platform itself, are configured to capture key events and logs to enable the Alfresco team to have full visibility of the functioning of the system. Key activities include:

- Monitoring Uptime availability
- Monitoring Critical System Services, including but not limited to:
 - Firewall and Load Balancer health checks
 - Resource Capacity on Servers (CPU/Memory/Disk Space)
 - Operating System Health
 - System Logs
 - Application and Infrastructure Access Logs
 - Search Indexes State and Performance
 - Database Health and Performance of Database Indexing
 - Repository Size and Performance
 - Transformation Services Health and Performance
 - Other background services such as deployment level backups
- Monitoring system-wide performance and audit logging functionality

Backups

The Platform has been designed following the recommendations and best practices defined in the

AWS Well Architected Framework. One of the benefits of this is that cloud deployments are spread redundantly across multiple availability zones providing resilience against underlying hardware failure. To ensure consistency and repeatability, the deployments of the Platform are fully automated with no manual steps. This gives confidence in correct deployments as the mechanisms used for deployments will have been fully tested before being run with no manual steps involved.

Hyland schedules backups for all instances in the environment. Backup processes are monitored and checked for backup system operation errors, and regularly scheduled tests of the restoration procedures are performed.

Additionally, Hyland stores an entire system back-up for 30 days. This backup includes a snapshot of the database and versioned backups of the content store that is replicated to a secondary region for fail-over services. Access to or restoration of backup files are done in accordance with Hyland's Disaster Recovery and Incident Response procedures. The following is a detailed listing of the backed-up components and their retention period:

Component	Retention Period
Content	30 Days
Database	30 Days
Application Configurations	30 Days
User Directory	30 Days
Search Index	7 Days
Application and Infrastructure Logs^{iv}	7 Days active available via API 1 Year long-term archive for forensic analysis only

Solution Decommission

Hyland will decommission solutions in accordance with contractual obligations and security requirements. An overview of the Customer-facing activities is provided below detailing the general off-boarding process. Customers should refer to their hosting agreements for details regarding data availability and required professional services fees.

Off-Boarding Overview

As a customer contract approaches their contract end date, The Account and Alfresco Cloud team confirms with the primary customer contact to either begin outlining a contract renewal or to confirm that the customer wishes to end their Alfresco services. Once the request to end the customers Alfresco contract has been made, the customer offboarding process begins. Customers will be given the option to access their data for up to thirty (30) days from the contract expiration date. Evidence of the purge and attestation to its permanent removal from all Cloud Systems will be provided to the customer.

Off-Boarding Communications

Three email communications are sent to customer contacts throughout the offboarding lifecycle. The following information breaks down what communication is and when.

- **Initial notification.** Approximately 1 month prior to the end of a customer's contract end date, an initial notification email will be sent to all known customer contacts notifying them of their upcoming contract end date and the termination of access and data dates.
- **Access Removal Notification.** On the day of the customer's contract end date, all customer access will be removed from Alfresco Cloud systems. An email notification is sent on the contract end date as a reminder of the access removal from their systems and a one-month notification of the date scheduled termination of data.
- **Data Termination Notification.** This email notification is sent on the scheduled termination date and acts as final notice that all data has been purged for that customer's Alfresco Cloud Environments.

Alfresco Cloud Off-Boarding Assistance

Hyland will provide the following off-boarding assistance for 30 days:

- The customer will continue to have access to the data extraction capabilities for 30 days. This allows the customer to extract all content within the Alfresco Cloud.
- If the customer provided custom code for Hyland to deploy, upon the customer's written request, Hyland will return a copy of that custom code to the customer.
- If the cancellation is related to a migration (i.e., the customer is purchasing an on-premises license for the corresponding Alfresco enterprise software program), Hyland will provide copies of any content models and similar materials deployed within the Alfresco Cloud for that solution to allow transition to the on-premises Alfresco solution.
- For large content repositories, Hyland will work with the customer to find the most cost-effective method for retrieving or transferring the data. Additional fees may be required for this assistance and/or to migrate content in bulk.

Compliance and Audits

Hyland has a comprehensive governance, risk, and compliance (GRC) program for all solutions within Hyland's cloud portfolio which includes the Platform. The Hyland Cloud GRC program includes, but is not limited to, the facilitation of risk assessments, customer assessments, compliance research, privacy programs, and certification audit programs, for all of Hyland's cloud platforms.

Policies are maintained to ensure governance is applied and enforced within Hyland Cloud operations. The Hyland Cloud IS Policy Suite is aligned to ISO

27001/27002 standards and all employees working in the Hyland Cloud environment are provided

Risk Assessment	Policies & Procedures	Standards Research
Internal Audit	Compliance Review	SOC 2
ISO 27002	GDPR	HIPAA
Incident Handling	Business Continuity	Vendor Reviews

access to all relevant policies and procedures.

Alfresco Cloud Solutions

Hyland's cloud platforms are subject to a SOC 2 Type II covering Security, Availability, Confidentiality, and Privacy. An internal audit program is established to continuously monitor for conformity. Customer-facing attestations are typically completed on an annual schedule and currently utilize the SOC 2 standard. A copy of Hyland's most recent SOC 2 report is available to all applicable customers upon written request and confidentiality agreement.

Third-Party Cloud Provider

As noted, the Platform is built on public cloud infrastructure utilizing AWS in many key functions. Hyland has no direct access to the physical infrastructure of AWS and enforces these requirements via contractual agreements.

All third-party Internet Service and Cloud Providers used by Hyland have demonstrated compliance with the AICPA Service Organization Controls ("SOC") Reports for Service Organizations and/or ISO 27001 attestation standards (or a reasonable equivalent). Hyland validates the audit status of each third-party provider on an annual basis. A copy of the most recent audit report is available to Customers in accordance with the third-party's audit report distribution policies. For AWS Artifact, more information is available here:

<https://aws.amazon.com/artifact/getting-started/>.

ⁱ Staging/Pre-Production environments are designed for product extension and integration testing only. They are non-clustered environments with 20GBs of storage. They support no more than 30 concurrent sessions, and there is no backup or DR for staging environments. If the environment becomes unstable or there is a serious issue, the environment will be reset to a clean state.

ⁱⁱ High Availability: if a node goes offline, the system will automatically deploy the service in a different datacenter or availability zone in the same region.

ⁱⁱⁱ Provides the connector and Alfresco software to enable AI & ML Services for Natural Language, Image Detection, Intelligent OCR and other content-driven AI capabilities. A Customer provided AWS account for AWS specific AI services (Rekognition, Comprehend, Textract) and operation is required.

^{iv} Infrastructure logs are not accessible to Customers due to security and confidentiality requirements.