



Etrieve Cloud  
Service Level  
Policy

## Etrieve Cloud Service Level Policy

This document provides information about the management of the production Etrieve Cloud environment including data backup and retention, restoration, disaster recovery, business continuity and availability, traditional and emergency change management, compliance, security and notifications. Please review in full to ensure your institution understands the full scope of services offered within the Etrieve Cloud platform.

Softdocs reserves the right to change the terms, practices, policies, procedures and conditions communicated within this document.

*Except as expressly provided in the Softdocs End User License Agreement, to the maximum extent permitted by applicable law, Softdocs does not make any other warranty of any kind, whether expressed, implied, statutory or otherwise, including warranties of merchantability, fitness for a particular use and non-infringement. Softdocs and its suppliers are not responsible or liable for the deletion of or failure to store any customer data and other communication maintained or transmitted through the use of Etrieve Cloud. Softdocs does not warrant that the operations of the software or the services will be error-free or uninterrupted. Neither the software nor the associated services are designed, manufactured, or intended for high risk activities.*



## Data Backup and Retention

Backups are an essential part of Etrieve Cloud and core to protecting your data. Softdocs has provided the general policies listed below in relation to the use of backups within the Etrieve Cloud offering.

### What data is being backed up?

There are five areas that Softdocs has focused on in relation to backups. The areas are outlined and described below.

**Table 1: Storage Definitions**

Storage Purpose	Description
Content Repository	Etrieve Content documents reside on Azure geo-redundant storage. This data is replicated three (3) times in the primary region and three (3) times in the secondary region.
Imports	Etrieve Content import files reside on Azure geo-redundant storage. This data is replicated three (3) times in the primary region and three (3) times in the secondary region.
Databases	Etrieve Content, Etrieve Central, and Etrieve Security databases reside on an Azure SQL Database server. Azure SQL Database is a Database as a Service offering that uses Azure Storage and its geo-redundant features to provide resiliency and durability.
Web Server	Windows Server-based virtual machines support the runtime operation of Etrieve. The OS disk is a standard Windows Server image that resides on locally redundant Azure storage and is replicated three (3) times.
Application	Application binaries and other files supporting the runtime operation of Etrieve reside on Azure geo-redundant storage. This data is replicated three (3) times in the primary region and three (3) times in the secondary region.



### How often is data being backed up?

The backup frequency of each storage area varies based on how it is used and operates. The table below outlines the storage type and backup frequency.

**Table 2: Backup Frequency**

Storage Purpose	Backup Frequency
Content Repository	Daily
Imports	Daily
Database	Hourly
Web Server	Maintenance Window Only
Application	Maintenance Window Only

### How long will Softdocs retain the backups?

Softdocs believes that, in most cases, 30 days is sufficient for meaningful recovery of data. The following table outlines the number of days or backups that are maintained for each storage type.

**Table 3: Storage Retention Policy**

Storage Purpose	Backup Retention Period
Content Repository	30 days
Imports	30 days
Database	30 days
Web Server	2 Maintenance Windows
Application	2 Maintenance Windows



## Restoration Policy

Backups are only as good as the restoration process. As such, Softdocs provides the following information about the restoration of data.

### What is Softdocs' Recovery Time Objective (RTO)?

The Recovery Time Objective is the duration of time Softdocs targets to restore Etrieve Cloud to functional operation. The Recovery Time Objective is outlined in **Table 4: Triggered Production Restoration**.

### What is Softdocs' Recovery Point Objective (RPO)?

The Recovery Point Objective is the maximum targeted period in which data may be lost due to an event. The Recovery Point Objective is outlined in **Table 4: Triggered Production Restoration**. Institutions should use the Recovery Point Objective to plan appropriate on-premises retention of source data (e.g. physical documents) to ensure full recovery in the event of a restore.

### What triggers Softdocs to restore data?

There are several events impacting the Etrieve Cloud environment which could trigger a restore of data. All event types, and the resulting restoration actions, are detailed in Table 4 and Table 5 below.

**Table 4: Triggered Production Restoration**

Event Type	Restoration Type	Recovery Point Objective (RPO)	Recovery Time Objective (RTO)
Content Repository storage experiences a catastrophic failure	Full restore from backup	24 hours	Up to 24 hours
Import storage experiences a catastrophic failure	Full restore from backup	24 hours	Up to 24 hours
Database experiences a catastrophic failure	Restore database to last known good configuration	1 hour	Up to 24 hours
Web server experiences a catastrophic failure	Provision new server	N/A	Up to 24 hours
Application storage experiences a catastrophic failure	Full restore from backup or release management system	N/A	Up to 24 hours



**Table 5: Client Requested Production Restoration**

Event Type	Information Required From Client	Softdocs Restoration Action
Client requested restore of Content Repository	Date and time of desired restoration point	Restore Content Repository at point of time nearest client specification
Client requested restore of Import staging folder	Date and time of desired restoration point	Restore Import staging files at point of time nearest client specification
Client requested restore of database	Date and time of desired restoration point	Restore database at point of time nearest client specification



## Disaster Recovery, Business Continuity, and Target System Availability

Softdocs understands that Business Continuity is extremely important to our clients. Disaster Recovery is a term used in association with a catastrophic loss of the system and how that system is restored to a functional state. In order to provide a better understanding of the policy, we will go through the different areas of the system and provide information about the recovery process.

### What is the target system availability for the Etrieve Cloud environment?

Softdocs guarantees an availability level of **99.5%** monthly for the production Etrieve Cloud instance in each deployment region. This targeted availability level excludes any scheduled or announced maintenance events by Softdocs or Azure.

### What penalties are levied against Softdocs in the event target availability is not met in a monthly period?

If Softdocs fails to provide 99.5% monthly availability for the production Etrieve Cloud environment, excluding any scheduled or announced maintenance events by Softdocs or Azure, upon client request Softdocs will issue a credit equal to the pro-rated charges for 3 days of service (annual subscription amount/365 x3 days).

Additionally, in the event the production Etrieve Cloud environment is unavailable to the client due to failures within the Etrieve Cloud environment (not for client-side connectivity or ISP/telecom-related issues) for a period in excess of seven (7) consecutive days, upon client request Softdocs will issue a credit equal to the pro-rated charges for each day in which the production Etrieve Cloud environment is unavailable to the client (annual subscription amount/365 x days unavailable).

### Disaster Recovery and Etrieve Cloud

Disaster Recovery operations are meant to provide a method in which the Etrieve Cloud environment can be brought back to a functional state after a disaster has occurred.

### What qualifies as a disaster?

Softdocs considers an event a disaster if it forces the primary Azure Region supporting your production instance of Etrieve Cloud into a non-functional state. Azure Region disaster declarations are made by Azure Support. Softdocs coordinates with Azure Support to evaluate, classify, and resolve events impacting an Azure Region.

### What is Softdocs' primary recovery mechanism in the event of a disaster?

Softdocs leverages Azure technologies to replicate data generated in the primary region to the secondary region. Softdocs will coordinate recovery efforts with Azure Support to restore full functionality of the Etrieve Cloud environment in the secondary region or an alternate region as we deem necessary.



### Which data is part of the Etrieve Cloud environment and covered under the Disaster Recovery plan?

There are three main storage areas that Softdocs has focused on in relation to backup and recovery. Each are listed below with a description of the type of data and how it is related to the overall solution.

**Table 6: Storage Areas included in the Disaster Recovery Plan**

Storage Type	Description	Replication Technology
Azure Storage	Azure Storage is a highly available data storage system holding Etrieve documents, images, media, and application runtime support files. This data is replicated within the primary region and the paired secondary region within the Etrieve Cloud environment.	Local and cross-region geo-redundant storage.
Azure SQL Database	Azure SQL Database is performant, resilient, and durable Database as a Service.	Local and cross-region geo-redundant storage.
Azure Virtual Machine	Azure Virtual Machines are Windows Server VM's providing compute resources for Etrieve Cloud.	OS drive is replicated via regional redundancy.

### What activates the Disaster Recovery Plan for Softdocs?

The decision to invoke the disaster recovery plan is the responsibility of the Etrieve Cloud Operations Team with coordination with Azure Support. If Softdocs feels the system will be operational within the published availability metric, based on information from Azure, the Disaster Recovery Plan may not be invoked.

### When does Softdocs switch back to the primary operation environment?

Softdocs will revert back to the primary operation environment at the next normal maintenance window.





## Change Management

This section outlines the policies used by Softdocs to control Change Management in association to the Etrieve Cloud environment.

### What is Change Management?

Change Management within the scope of Etrieve Cloud pertains to the following areas:

1. Etrieve Product Updates
  - a. Major and minor releases
  - b. Hotfixes
2. Database Updates
  - a. Database version updates
  - b. Schema modifications
    - i. Table structures
    - ii. Trigger structures
    - iii. View structures
3. Operating System Updates & Modifications
  - a. Major Releases
  - b. Service Packs
  - c. Patches and Hotfixes
4. Azure changes which require a change to the Etrieve Cloud environment
5. Backup/Restore system modifications
6. Disaster Recovery system modifications
7. Alerting modifications
8. Policies (as defined in this document)

### How is Change Management controlled within the Etrieve Cloud environment?

1. Client requested changes made to any of the areas discussed in the previous section are requested through the Softdocs Support team.
2. Softdocs requested changes made to any of the areas discussed in the previous section are requested through the Etrieve Cloud Operations team.
3. The Etrieve Cloud Operations team maintains access control over the entire Etrieve Cloud environment.
4. The Etrieve Cloud Operations team is the only team authorized to make changes once they have been requested and approved.
5. Changes made to the Etrieve Cloud environment are a combination of automated and manual processes.



6. Softdocs maintains a private test system where changes are tested prior to any of the following:
  - a. Etrieve product updates
  - b. Database version updates
  - c. Database schema modifications
  - d. Major OS releases and service packs
  - e. Azure changes that require a change to the Etrieve Cloud environment

### Is there a normal maintenance window for change management?

Softdocs will publish a schedule to all clients utilizing the Etrieve Cloud environment as soon as maintenance is required. Non-emergency maintenance windows will be scheduled on Saturdays or Sundays (in the United States) as required, with notifications provided at least three weeks prior to the expected maintenance window. Notifications will include the date(s) and estimated time(s) of day when maintenance will occur.

### How long will an outage occur during normal maintenance?

Softdocs works to keep the maintenance windows as short as possible. Depending on the update to be applied to the system, the maintenance window may be as short as 15 minutes or as long as eight hours. If the maintenance window is anticipated to be longer than eight hours, we will provide an estimate of the duration during our maintenance notification.

### Does Softdocs have a system of record for Change Management?

The Etrieve Cloud Operations team uses a ticketing system to record all changes made to the Etrieve Cloud environment. This system is leveraged for both normal maintenance and unplanned emergency maintenance.

### What is the method of notification that Softdocs uses to communicate maintenance in the system?

Softdocs utilizes email heavily for maintenance notification purposes. Maintenance notifications will be sent to the designated client contacts for Etrieve Cloud and will include the following information:

1. Scheduled Maintenance Date/Time (Time Zone specific)
2. Expected outage window (duration)
3. Description of the maintenance taking place
4. Information related to any changes necessary on a client-based system which might need to occur prior to, or after, maintenance to the Etrieve Cloud environment.

### If a change to a related system, such as the Etrieve Cloud Hybrid Server, is required, where are instructions and relevant files located?

Softdocs will include the location of any required update files or changes to a client portion of Etrieve Cloud in the notification email. This information will be communicated prior to the maintenance window and will include links to documentation on how to update related systems.



## Emergency Change Management

This type of change management outlines steps which may need to be taken in the event of an emergency update to the Etrieve Cloud environment. Softdocs makes every effort to test any and all changes in a test environment prior to making changes to the production environment.

### What qualifies for emergency change management?

1. Etrieve product updates which are required for the production system to remain operational in the manner it was at time of deployment
2. Database updates which are required for the production system to remain operational
3. Communication port changes related to overall operation of the system
4. Critical operating system security updates needed to maintain a secure environment
5. Anything not specifically covered by the points above that prevents the production system from operating

### What does not qualify for emergency change management?

1. Non-critical operating system updates
2. Notification updates

### What is the notification method for emergency change management?

**Method 1:** Softdocs utilizes email heavily for notification of changes. Change notifications will be sent to the designated client contacts for Etrieve Cloud and will include the following information:

1. Description of the issue and why it warrants immediate action by the Etrieve Cloud Operations Team
2. Expected outage window
3. Information related to any changes necessary on a client-based system which might need to occur after this maintenance window to the Etrieve Cloud environment.

**Method 2:** The Etrieve Cloud Operations team will make phone calls to designated client contacts for Etrieve Cloud and provide the following information verbally.

1. Description of the issue and why it warrants immediate action by the Etrieve Cloud Operations Team
2. Expected outage window
3. Information related to any changes necessary on a client-based system which might need to occur after this maintenance window to the Etrieve Cloud environment.

### How is the emergency change documented?

Softdocs will use the same ticketing system used for normal maintenance windows to document any emergency changes to the Etrieve Cloud environment.

### Who authorizes emergency changes in the system?

Etrieve Cloud Operations staff will communicate the need to the Softdocs Senior Support and Development Management teams for authorization.



## Compliance Policy

Softdocs understands that institutions may have regional compliance or data residency requirements. With that in mind, Softdocs will utilize the following compliance policy.

### How does Etrieve Cloud support compliance and data residency requirements?

Softdocs employs a regional data center model for institutions that have specific regional compliance or data residency requirements. Etrieve Cloud is deployed within Azure Regions. When provisioning Etrieve Cloud and associated storage for an institution, Softdocs will select the primary region nearest the same geographic region as the institution's primary campus. Softdocs will replicate client data to a secondary region based Azure geo-redundant secondary region pairings. The primary and secondary region will always reside within the same country as the institution.

Softdocs' hosting partner, Microsoft Azure, undergoes routine audits to ensure data centers and operational processes are compliant with published industry standards. To obtain the most recent copies of compliance documentation, please visit the Microsoft Trust Center: <https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>



## Security Incident and Notification Policy

Softdocs secures and protects client data using industry best practices. Softdocs will monitor the Etrieve Cloud environment activity to detect possible threats to the environment and data. Events will be evaluated to determine if they constitute a violation of computer security or acceptable use policies and should be classified as a security incident.

When an incident is identified, the Softdocs Etrieve Cloud Operations Team will follow Softdocs Security Incident procedures to determine the scope and impact and promptly notify our clients if data has been compromised.



[www.softdocs.com](http://www.softdocs.com)



888.457.8879



803.695.6911



807 Bluff Road  
Columbia, SC 29201