High Level Architecture, Resilience and Security for Office 365 Environments
# Table of Contents

## 1 Introduction

1.1 Document Overview .............................................................. 5  
1.2 Repstor Products - an Overview ........................................... 5  
  1.2.1 Repstor affinity .......................................................... 5  
  1.2.2 Repstor assist ............................................................ 5  
  1.2.3 Repstor Custodian ....................................................... 5  
1.3 Supported environments ....................................................... 6  
  1.3.1 Repstor affinity and assist ........................................... 6  
  1.3.2 Repstor Custodian ....................................................... 6  
1.4 Repstor Platform High Level Architecture ................................. 6

## 2 Architecture Overview

2.1 Repstor Custodian Data Flow Architecture .................................. 8  
  2.1.1 Repstor Custodian Data Flow – Provisioning ........................ 8  
  2.1.2 Custodian Data Flow - Metadata updates ............................. 10  
2.2 Repstor affinity Data Flows ..................................................... 12  
  2.2.1 Repstor affinity – Synchronization configurations ................ 12  
  2.2.2 Repstor affinity-Content synchronization data flow ............... 14  
2.3 Custodian Low Level Architecture & Resiliency ............................ 15  
2.4 Custodian and Affinity High Level Data Interactions .................... 19  
  2.4.1 Scenario: Custodian Web Requests ................................ 19  
  2.4.2 Scenario: Affinity Metadata Requests .............................. 20  
  2.4.3 Scenario: Affinity Metadata File Events ........................... 22

## 3 Data Storage

3.1 Repstor affinity licensing server ............................................. 24  
3.2 Repstor Support Data .......................................................... 24  
3.3 Storage of Customer Data ...................................................... 24  
3.4 Data utilized for provisioning within SharePoint Online .................. 25  
  3.4.1 Matter, Client and list processing .................................... 25  
  3.4.2 Provisioning ............................................................... 25  
  3.4.3 Matter Narrative ......................................................... 25  
  3.4.4 Customer API Keys ..................................................... 26  
  3.4.5 Error Logging ............................................................ 26

## 4 Repstor Service Availability & Support

4.1 Service Level Agreements ...................................................... 27
4.2 Functional Availability ........................................................................................................... 27
4.3 Repstor Service Monitoring ................................................................................................... 29
4.4 Office 365 Service Monitoring .............................................................................................. 29
4.5 Repstor Support ..................................................................................................................... 29
4.6 Product Update Schedules ..................................................................................................... 30

5 Frequently Asked Questions ................................................................................................. 31
1 Introduction

1.1 Document Overview

This document provides a high-level architectural overview of the Repstor Matter Management Platform and describes the following:

- An overview of the Repstor applications and their purpose.
- An architectural view of the Repstor applications and how they are structured.
- Consideration of the resiliency and security of Repstor applications.
- Identification of data stored within applications and its locations.
- A review of the service monitoring agreed levels of service and incident management.
- Frequently asked questions by customers

Note The intended audiences for this document are Information Technology and Security professionals.

1.2 Repstor Products- an Overview

1.2.1 Repstor affinity

Repstor affinity provides uninterrupted online and offline access to Microsoft® SharePoint® and other systems through the Microsoft® Outlook® mail client. You can access content held on SharePoint systems or File Shares or other file storage repositories (dependent on product licensing) online and offline. You can add, view, edit content according to permissions you have relating to the source of the content. affinity then automatically synchronizes any changes back to the content repository. This means you do not have to wait for slow downloads and uploads to SharePoint and other content stores but continue to work without impact.

Repstor affinity also provides enhanced filing functionality through the Quick File module which enables you to locate recent folders quickly, and search for folders by name. Quick File is further enhanced with assisted filing through the Repstor assist.

1.2.2 Repstor assist

Repstor assist is a categorization engine which suggests the filing location based on an analysis of the content and context of the document/email being filed. This minimizes time spent navigating complex hierarchies with large folder structures and creates an optimized user-experience for filing.

1.2.3 Repstor Custodian

Repstor custodian is a case management system utilizing SharePoint (Either O365 or On Premise) as the repository for case documents and other content Repstor custodian's integration with Outlook enables users to work on cases directly from Outlook/Office increasing productivity while maintaining compliance and security. You can work online or offline and access content from the many different sources that may be required in addition to the case management system (e.g. File Shares/ EFS services/corporate records stores).
Repstor custodian enables organizations to take advantage of the broader Microsoft platform of products including capabilities such as analytics, compliance, workflow and Data Loss Prevention (DLP). Repstor custodian can integrate seamlessly with other professional applications such as Practice Management Systems (PMS), HR Systems, on-boarding applications, client-engagement systems, time and billing applications, and other workflow management applications.

### 1.3 Supported environments

The following are the hardware and software requirements to use the Repstor suite of products in an Office 365 environment.

#### 1.3.1 Repstor affinity and assist

<table>
<thead>
<tr>
<th>Software or Hardware component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System(s)</td>
<td>Windows 10, Windows 8.1, Windows 7 Service Pack 1</td>
</tr>
<tr>
<td>Microsoft Office Version(s)</td>
<td>Office ProPlus, Office 2019, Office 2016, Office 2013, Office 2010</td>
</tr>
<tr>
<td>Internet Browser(s)</td>
<td>The current version of Microsoft Edge, Internet Explorer, Chrome, or Firefox</td>
</tr>
<tr>
<td>Minimum Hardware</td>
<td>1.6 gigahertz (GHz) or faster, 2-core; 4GB RAM; 4GB of available disk space; 1280 x 768 screen resolution</td>
</tr>
</tbody>
</table>

#### 1.3.2 Repstor Custodian

<table>
<thead>
<tr>
<th>Software or Hardware component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint Versions</td>
<td>SharePoint Online</td>
</tr>
</tbody>
</table>

#### 1.4 Repstor Platform High Level Architecture

The following figure shows the three key architectural components that make up the Repstor platform.
1. **Client Apps – integrated with Repstor affinity** The End-User integrations allows end users to access and store structured content in the Storage Service from their Office applications, in addition they can use Repstor assist to enable enhanced end user filing capabilities.

2. **Microsoft Office 365 – enhancing SharePoint Online with** Repstor custodian SharePoint Online storage allow users to store business content in a highly secure storage repository, structured and organized with metadata through the Repstor provisioning engine.

3. **Microsoft Azure – providing Repstor custodian**

   The Repstor provisioning application takes a data feed (e.g., from a Line of Business Interface or entered through a User Interface) and uses this to provision tightly controlled, highly structured entities representing Business Concepts (e.g., Clients, Matters etc.) in SharePoint Online. It then makes these entities available to end users to use in the Client Apps via a simple subscription process to synchronize data between SharePoint Online and the Client Apps.
2 Architecture Overview

2.1 Repstor Custodian Data Flow Architecture

This section visually depicts the flow of data for two frequently performed activities within Repstor custodian.

- Provisioning a storage location within SharePoint Online.
- Updating metadata properties through Repstor custodian, which are cascaded to SharePoint Online.

Data flow description to understand the actions within each activity block is provided.

2.1.1 Repstor Custodian Data Flow – Provisioning

Repstor custodian typically creates well-structured storage repositories within SharePoint Online to securely store content in relation to Case and Matter Management. These storage locations include the following structures within SharePoint Online:

- Site Collections
- Sub-Sites
- Document Libraries and Lists
- Folders

The data flow diagram below provides the type of data that is captured throughout the provisioning process and the actions completed during provisioning.
Figure 2 Repstor custodian provisioning – data flow diagram
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Request for Creation | A request is created and posted to *Custodian*, to provision a storage repository aligning to a well-defined structure via the metadata captured during the request process.  

The request is created under the context of the user logged in to Office 365 using OAuth 2.0 authentication. The request itself is posted through a *Custodian* API to the *Custodian* Application server, which is SSL encrypted during transfer.  

The request data is also stored within a *Custodian* request list within the customer's SharePoint Online environment. This a hidden list and can be reviewed by the customer for compliance or auditing purposes. |
| 2    | Custodian App | The *Custodian* Application servers handle the initial request, placing the request within a SQL Database for the purpose of a temporary cache. The provisioning servers then execute jobs at the target location on a round-robin basis, using REST API integration.  

For successful provisioning jobs, the request metadata is removed from the SQL Database within sixty seconds. For unsuccessful jobs, the error code is posted to the customer's logs within their own SharePoint Online environment for any future troubleshooting. |
| 3    | SharePoint Online Repository | In the event of a successful provisioning process, the storage repository is created aligning to the type of repository that was requested at the start of the process such as a Site Collection, Sub-Site or Document Library.  

In addition, the location of the repository will be added to the Central Repository List which is held within a customer's SharePoint Online environment. This will allow the assignment or subscription of the location to nominated users henceforward.  

**Note** This depends on the security requirements of the repository which was defined at the request stage. |
| 4    | Assignment or Subscription | Users with *Repstor* affinity, will be able to subscribe to the repository to store data through the Outlook interface. As the repository has associated metadata, it will allow nominated users to review additional properties such as metadata created with the request or other properties which are significant during the case or Matter lifecycle. |

### 2.1.2 Custodian Data Flow- Metadata updates

*Repstor custodian* can update metadata which is associated to the storage repository. This is completed during the lifecycle of a Case or Matter and allows the nominated users access to properties to understand the status of outstanding and work and other important metadata.  

The data flow diagram below provides the mechanism of updating metadata throughout the Case or Matter process and the actions completed during these updates.
Figure 3 *Repstor custodian* metadata updates – data flow diagram

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Update on a Matter or case</td>
<td>An update to the metadata is requested. This can include a change in the status of a Case or Matter, or additional properties captured during the lifecycle of the Case or Matter. The request is created under the context of the user logged in to Office 365 using OAuth 2.0 authentication. The request is posted through the <em>Custodian</em> API to the <em>Custodian</em> Application Server, which is SSL encrypted during the transfer.</td>
</tr>
<tr>
<td>2</td>
<td>Custodian App Server</td>
<td>The <em>Custodian</em> App server receives the update and directs it to SharePoint Online via the Microsoft SharePoint Online REST API to the SharePoint Online service, which is again SSL encrypted during the transfer. The exception to this rule is, if a third-party customer integration is utilizing the <em>custodian</em> API. This means that all requests are held and managed in the request database to throttle API requests and ensure high performance of the application</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>SharePoint Online List Update</td>
<td>The change is posted to a SharePoint Online Custodian List within the customer’s environment. The list metadata is therefore available to nominated users who are assigned or subscribe to the Case or Matter.</td>
</tr>
</tbody>
</table>

2.2  Repstor affinity Data Flows

*Repstor affinity* typically synchronizes content from SharePoint Online and stores a synchronized copy for offline access. This section provides a data flow image to explain this activity. A description of the data flow is also available to understand the actions within each activity block.

2.2.1  Repstor affinity– Synchronization configurations

*Repstor affinity* synchronizes content from SharePoint Online from repositories that are created via *Repstor custodian* and other common storage types within SharePoint Online, such as the following:

- Site Collections
- Sub-Sites
- Document Libraries and Lists
- Folders

Content Synchronization can be configured to meet the requirements of our customers while making the following core configurations available.
<table>
<thead>
<tr>
<th>Synchronization configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Headers synchronization | *Repstor affinity* can synchronize and store locally, the headers of the files within the synchronized storage locations, which happens every hour by default.  
Headers provide a benefit for performance, as the headers are small and only a few kilobytes in size, ensuring that the performance of the synchronization in storage locations with many thousands of files is the most efficient.  
Header-synchronization does not include the underlying file itself; the files are downloaded on-demand when a user opens a file through *Affinity*. This process is hidden from the end user as the file is downloaded on-demand and immediately opened in the relevant application, such as Word or PowerPoint.  
The main constraints of Header Synchronization, are:  
- *Repstor affinity* only has access to the header when users generate search queries, the search capabilities within *Repstor affinity* are more restrictive than the alternative of Content synchronization.  
- Limited access to files when working Offline through *affinity*, as they must be downloaded when the user is Online and has access to the content area.  
**Note** In organizations with hundreds of thousands or millions of files, we do recommend reviewing the use of Header Synchronization as it can have benefits for larger organizations in such environments. |
| Headers and Content synchronization | *Repstor affinity* has another configuration option that builds on the ability to synchronize Headers. This allows the synchronization of the underlying content such as the Word or PowerPoint file to which the header was associated.  
The file content synchronizes automatically every hour by default. But it will only synchronize file content that has been updated or changed since the last synchronization. This therefore limits the amount of content being synchronized ensuring only the most recent content is synchronized.  
This allows an excellent search experience with both the file and header being available for search queries that the user will generate while providing the ability to work offline with synchronized files.  
All content that is synchronized, is securely stored within the user’s offline cache which is typically BitLocker encrypted (depending on customer configuration) within the Windows File Storage location. There is also no direct end user access to this content through the offline cache, as content must be opened through *Repstor affinity*.  
Organizations with thousands of files, may find that Header & Content synchronization is a better configuration to meet their requirements in such environments. |
### Repstor affinity-Content synchronization data flow

*Repstor affinity* synchronizes headers and content regularly, which is both invoked by the end user and invoked using an automated schedule. The data flow diagram below explains the mechanism of the content synchronization during normal use of *Repstor affinity.*

#### Figure 4 *Repstor affinity* content synchronization- data flow diagram

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | affinity synchronization | When a user opens a content repository within *affinity, it triggers a* synchronization for any newly updated content since the last synchronization. A timestamp is captured in the local machine configuration, to confirm the most recent time of synchronization.  
If the synchronization is triggered by the default one-hour period, *affinity* will synchronize all newly updated content from the time of the last synchronization and again capture a timestamp in the local machine configuration, to confirm the time of synchronization.  
In both cases, when a user attempts to open a file from the synchronized location, the file will be opened from the encrypted offline cache of the user's machine to ensure fast retrieval of the data. |
| 2    | SharePoint Online File Storage | SharePoint Online will hold all the file content, to which *affinity* is attempting to synchronize.  
1. A query generated to the SharePoint Online location to identify the files that have changed since the last synchronization.  
2. The files are identified and then downloaded to the machine by *affinity* and placed within the offline cache for use.  
All authentication is handed under the context of the end using OAuth 2.0. Users will only be able to synchronize content to which they have access to. |
2.3 Custodian Low Level Architecture & Resiliency

The following image describes the components of Repstor custodian. The table provides an overview of each component and its purpose in the delivery of the Repstor custodian service.

Figure 5 Repstor Custodian architecture diagram
<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
<th>Resiliency</th>
<th>Security</th>
</tr>
</thead>
</table>
| Azure Traffic Manager for Geographic Routing & Load Balancing           | Azure Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints.  
  Repstor custodian has instances in many Azure regions, for failover and performance. Therefore, all requests to authenticate to custodian are handled by Azure Traffic Manager and are routed firstly by the user's location and will either be routed to the North Europe or Australia regions.  
  When the request has been routed to the relevant region, it will then be routed to the primary web server handling requests with a failover being available to be routed in the event of an outage or unforeseen impact in service. | By design, Traffic Manager components are resilient to a complete failure of any Azure region. This resilience applies to all Traffic Manager components: the DNS name servers, the API, the storage layer, and the endpoint monitoring service.  
  In the unlikely event of an outage of an entire Azure region, Traffic Manager is expected to continue to function normally. Applications deployed in multiple Azure regions can rely on Traffic Manager to direct traffic to an available instance of their application. | Azure Traffic Manager requests are encrypted with SSL and the service is hosted within Microsoft Azure and aligns to its existing service protections including at rest encryption. |
| Azure Custodian Application Servers                                     | Repstor custodian application services process the requests for provisioning and updates to Matters and Cases.  
  The Repstor custodian application servers use Azure Web App architecture and provide separation between the Provisioning Services and Web Applications handling requests. | Repstor custodian is highly resilient with a minimum of three dedicated application servers within the Azure North Europe region, with a further two dedicated application servers within the Azure Australia region with Azure auto-scaling on demand in both regions. | Authentication to the Repstor custodian web services are use the OAuth 2.0 authentication mechanism in the context of the end user generating the request via an SSL encrypted request. |
<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
<th>Resiliency</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Redis Fast Cache</td>
<td>Repstor custodian has been built to quickly access SharePoint Online configurations through a Redis Cache Service, which is hosted within Azure, but this does not hold any confidential client data.</td>
<td>Azure provides a redundant pair of virtual machines configured for data replication to ensure maximum reliability.</td>
<td>Azure Cache for Redis supports industry-standard SSL to secure your data in transit and Azure Storage disk encryption at rest.</td>
</tr>
<tr>
<td>Azure Encrypted Key Database</td>
<td>Repstor custodian allows customers to set their own API keys to be utilized in customers third party integrations or customizations.</td>
<td>Azure platform fully manages every Azure SQL Database and guarantees no data loss and a high percentage of data availability. Azure automatically handles patching, backups, replication, failure detection, underlying potential hardware, software or network failures, deploying bug fixes, failovers, database upgrades, and other maintenance tasks. This architecture is designed to ensure that committed data is never lost and that maintenance operations are performed without affecting workload.</td>
<td>All keys stored are hashed in SHA-512 with the Repstor team having no ability to decrypt the keys.</td>
</tr>
<tr>
<td>Component</td>
<td>Purpose</td>
<td>Resiliency</td>
<td>Security</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Azure SQL Job Database</td>
<td><strong>Repstor custodian</strong> queues the jobs for provisioning within an Azure SQL Database, which acts as a cache and provides job management for enhanced performance. The jobs are permanently deleted following completion with further detail in the Section Four of this document. The SQL database is provided through Azure, ensuring high levels of security and performance.</td>
<td>Azure platform fully manages every Azure SQL Database and guarantees no data loss and a high percentage of data availability. Azure automatically handles patching, backups, replication, failure detection, underlying potential hardware, software or network failures, deploying bug fixes, failovers, database upgrades, and other maintenance tasks. This architecture is designed to ensure that committed data is never lost and that maintenance operations are performed without affecting workload.</td>
<td><strong>Repstor</strong> Azure Databases are utilizing Azure Transparent Data Encryption. TDE performs real-time I/O encryption and decryption of the data and log files. TDE protects data &quot;at rest&quot;, meaning the data and log files. It provides the ability to comply with many laws, regulations, and guidelines established in various industries.</td>
</tr>
<tr>
<td>Custodian SharePoint App</td>
<td><strong>Repstor custodian</strong> requires a SharePoint provider app installed in a specific Site Collection, to integrate the client-side components of Custodian and provide trust between the customers SharePoint Online environment and the custodian application. The app file itself is effectively a secure authentication re-direct to the custodian application hosted within Azure via a manifest file, so it is small and has minimal underlying components.</td>
<td>The SharePoint Online app is resilient within the wider SharePoint Online service and the underlying Microsoft service architecture provides access to this SharePoint app. This Microsoft Cloud service architecture is resilient in line with the SharePoint Online architecture.</td>
<td>SharePoint Online Provider apps utilize the most up-to-date SharePoint Online app architecture. As the underlying application architecture is hosted within Microsoft Azure, the app itself is setup to provide trust and authentication between the customers SharePoint Online environment and the custodian application. In highly secure environments, we offer customers to the ability to restrict trust to a single Site Collection, rather than the customers SharePoint Online environment.</td>
</tr>
<tr>
<td>Component</td>
<td>Purpose</td>
<td>Resiliency</td>
<td>Security</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SharePoint Online and Office 365</td>
<td>All customer data including custodian configuration data and the underlying customer files are all stored within the customers SharePoint Online environment.</td>
<td>SharePoint Online is highly resilient and utilizes the Microsoft Cloud Service Architecture which provides a Microsoft Quarterly 99.9% financially backed SLA (dependent on the customers product licensing).</td>
<td>Office 365 is verified to meet the requirements specified in ISO 27001, European Union (EU) Model Clauses, the Health Insurance Portability and Accountability Act Business Associate Agreement (HIPAA BAA), and the Federal Information Security Management Act (FISMA).</td>
</tr>
</tbody>
</table>

### 2.4 Custodian and Affinity High Level Data Interactions

#### 2.4.1 Scenario: Custodian Web Requests

In this scenario, a user generates a request to Custodian to either retrieve or post metadata updates from a Custodian supported -web browser.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User Authentication</td>
<td>To access Custodian, a user must be authenticated to the customer’s Azure Active Directory and have a valid access token to access the customer’s SharePoint Online environment in which Custodian has been configured. When the user accesses Custodian through SharePoint Online, the user access OAuth2.0 token is encapsulated and encrypted using TLS 1.2 and utilised by the Custodian Web Services. These requests are issued from the web browser as HTTPS requests and utilise the Microsoft SharePoint Online API.</td>
</tr>
<tr>
<td>2</td>
<td>Custodian App</td>
<td>The Custodian Application servers handle the initial request and depending on the request, will execute different methods designed within the application. For example, a user attempting to access metadata will have an API query issued from the Custodian App using the user access token to get metadata from a specific Custodian configuration list within the customer tenancy. Other requests can be long running and may take longer to complete or the user token may not have specific privilege to complete these requests. In this event, the app access token is utilised to complete such requests. These types of requests are designed to use app access tokens within the architecture of Custodian and therefore any request to access or update metadata will use the user access token, to ensure that data confidentiality is maintained.</td>
</tr>
</tbody>
</table>

### 2.4.2 Scenario: Affinity Metadata Requests

In this scenario, a user generates a request to Custodian to either retrieve or post metadata updates from Repstor affinity within Outlook.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User Authentication</td>
<td>To access Custodian, a user must be authenticated to the customer’s Azure Active Directory and have a valid access token to access the customer’s SharePoint Online environment in which Custodian has been configured. When the user accesses Custodian through SharePoint Online, the user access OAuth2.0 token is encapsulated and encrypted using TLS 1.2 and utilised by the Custodian Web Services. These requests are issued from Affinity as HTTPS requests and utilise the Microsoft SharePoint Online API.</td>
</tr>
</tbody>
</table>
### Step 2

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custodian App</td>
<td>The Custodian Application servers handle the initial request and depending on the request, will execute different methods designed within the application. For example, a user attempting to access metadata will have an API query issued from the Custodian App using the user access token to get metadata from a specific Custodian configuration list within the customer tenancy. Depending on the customer configuration of Repstor affinity, other requests can be long running and may take longer to complete or the user token may not have specific privilege to complete these requests. In this event, the app access token is utilised to complete such requests. These types of requests are designed to use app access tokens within the architecture of Custodian and therefore any request to access or update metadata will use the user access token, to ensure that data confidentiality is maintained.</td>
</tr>
</tbody>
</table>

#### 2.4.3 Scenario: Affinity Metadata File Events

In this scenario, a user generates a request to SharePoint Online to access or edit a file. In this scenario clients will access SharePoint Online directly with no Custodian interaction.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User</td>
<td>Authentication To access files within SharePoint Online, a user must be authenticated to the customer’s Azure Active Directory and have a valid access token to access the customer’s SharePoint Online environment in where the content is being stored. When the user accesses or synchronises files through affinity, the user has authenticated to SharePoint Online using Modern Authentication (OAuth 2.0) and this session is utilised to access files and upload changes to the customer environment. These requests are issued from Affinity as HTTPS requests and utilise the Microsoft SharePoint Online API. There are no Custodian requests as this is not required for the download and access of files to ensure quick throughput and customer confidentiality.</td>
</tr>
<tr>
<td>2</td>
<td>SharePoint</td>
<td>App SharePoint Online utilises Modern Authentication and any requests are handled in line with Microsoft standard practice. Further information on the synchronisation of files within Repstor affinity are included within Section 2.2.2 of this document.</td>
</tr>
</tbody>
</table>
3 Data Storage

In line with customer requirements, we at Repstör strive to ensure that we do not store any customer data unless it is required for a specific purpose and held for the minimal amount of time, in a secure manner.

We at Repstör want customers to be fully clear on what type of data is held, for how long, the purpose and the security that is applied to data. The following sections outline where any data is held and provide a full description of its use.

3.1 Repstör affinity licensing server

The Repstör licensing server is used to activate Repstör software and access to our cloud services. Our Licensing server is an Azure hosted application and will store minimal details in order to ensure that license limitations are adhered to. The data stored for this purpose is as follows:

- The primary email address of the user
- The machine ID of the system where the software is being used/from which the service is being accessed
- The Repstör software version
- The Microsoft Office version

This data is accessed internally only for licensing and support. For example, if we at Repstör discover an issue with a specific version of Repstör software when used with a specific Office version, Repstör can notify customers if necessary. This data can be destroyed if customers request it for valid and rational reasons.

3.2 Repstör Support Data

On some occasions, Repstör may access request logs or other internal analytics to investigate support incidents and to support problem management. When a support request is received, Repstör stores the request logs and data related to the request in our secure support application.

This data can be deleted either on customer request or after an appropriate period following closure of the support request. In all cases, customers can check the contents for any sensitive data prior to providing the contents to Repstör.

3.3 Storage of Customer Data

All customer data is stored in the customer’s own Office 365 and SharePoint Online environment. For example, this data includes Office files and other confidential data to which Repstör does not have access.

No customer data is stored in our custodian application through Azure. Customer data to support the implementation and use of our application are stored within the customer’s SharePoint Online environment. Customer data includes all configuration data, metadata, lists of matters and clients etc.
3.4 Data utilized for provisioning within SharePoint Online

*Repstor custodian* application will process data (as described below) on behalf of users to provide the specific services and functions. This processing of data does not expose any of the data being processed to *Repstor* employees.

### 3.4.1 Matter, Client and list processing

To show the set of clients or matters that have been pinned by the user, or the full list to which the user has access, custodian processes list data in user sessions that are secured to the individual user. These interactions are secured by encryption in transit to and from the *custodian* service with OAuth 2.0 authentication in the context of the end user.

The *Repstor custodian* application processes data stored in the matter and client lists to present users with lists of items to which they can subscribe and to provision new matters, and clients when requests are made.

### 3.4.2 Provisioning

When an item is provisioned, the *Repstor custodian* application accepts requests that are driven by the *custodian* user interface or by the API with a customer API key. Depending on customer requirement, areas to be provisioned may include customer data, such as the Matter Name or the Client Name that must be captured and used in the provisioning process. For example, customers name their storage repositories in line with the Matter or Client name to help identify it for content access or for filing in the future.

Therefore, the requests may contain specific customer data during the provision process, but this data is not accessible by *Repstor* employees whilst being processed. The request data may be temporarily cached on in a provisioning database to complete the provisioning request, which is fully TDE encrypted and managed within Azure.

When provisioning is complete (can take several minutes depending on complexity of the request) we will permanently delete the request data within sixty seconds of a successful provisioned state. If provision fails due to a service issue, the *custodian* app writes the error code to the customer environment configuration list and the request is permanently deleted.

Any other system logs that the *custodian* application utilizes, will not include any customer specific data but may include limited information of a specific request. For example, it can include the start and end time of a provisioning job to support troubleshooting or problem management.

### 3.4.3 Matter Narrative

Our customers require the ability to include narrative on Matters or Cases that help track the status of work and include specific text comments on the progress of a Matter or Case. This narrative is stored within a secure SharePoint List within the Customer Environment to which *Repstor* does not have access.
3.4.4 Customer API Keys

Some customers require the ability to integrate third party applications with the custodian application, for specific use cases. We offer the ability for each customer to create their own API key to retrieve or post changes to their specific customer instance of custodian.

These keys must be highly secure and as described within Section 2.3, all keys are SHA-512 hashed and the original keys are irretrievable. If necessary, we can restrict the access of the API key to specific IP ranges, to further restrict access to them from specific customer integrations.

3.4.5 Error Logging

No customer data is included in error logging in the custodian service, which include system errors for the purpose of support.
4 Repstor Service Availability & Support

4.1 Service Level Agreements

It is important for us at Repstor to ensure our Cloud Applications are available to all customers. For our custodian application, which is Microsoft cloud hosted, we target to deliver a 99.5% service level agreement.

Where possible any scheduled maintenance will be carried out of normal (UK) business hours and will be notified at least two days in advance. Scheduled downtime periods for maintenance or upgrades are not normally required because of our application architecture resiliency.

4.2 Functional Availability

The following key Repstor Matter Management Platform components are cloud-based and utilize services provided through the Microsoft Cloud Service.

- Repstor custodian
- SharePoint Online

These services are architected and designed to be highly available; however, if there is a temporary outage of any Microsoft Cloud Service, the architecture described in this document ensure minimum impact on end users.

This is described in the functional availability table below:

<table>
<thead>
<tr>
<th>Function / Feature:</th>
<th>Available when all services online</th>
<th>Available if Provisioning Service (custodian) offline</th>
<th>Available if Storage Service (SharePoint) offline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access existing content</td>
<td>✔</td>
<td>✔</td>
<td>✔ (Previously Cached Content only)</td>
</tr>
<tr>
<td>Edit existing content</td>
<td>✔</td>
<td>✔</td>
<td>✔ (Previously Cached Content only)</td>
</tr>
<tr>
<td>File new emails and other content</td>
<td>✔</td>
<td>✔</td>
<td>✔ (Previously Cached Locations only)</td>
</tr>
<tr>
<td>Use Repstor assist to enhance filing of content</td>
<td>✔</td>
<td>✔</td>
<td>✔ (Previously Cached Locations only)</td>
</tr>
<tr>
<td>End User Features</td>
<td>Function / Feature:</td>
<td>Available when all services online</td>
<td>Available if Provisioning Service (custodian) offline</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>View and update Content Metadata</td>
<td>✔</td>
<td>✔</td>
<td>✓</td>
</tr>
<tr>
<td>Search for content in the local cache</td>
<td>✔</td>
<td>✔</td>
<td>✓</td>
</tr>
<tr>
<td>Search for content not in the local cache</td>
<td>✔</td>
<td>✔</td>
<td>✘</td>
</tr>
<tr>
<td>Access Content Version Histories</td>
<td>✔</td>
<td>✔</td>
<td>✘</td>
</tr>
<tr>
<td>Update custodian metadata on existing matters?</td>
<td>✔</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>Search for / subscribe to new matters</td>
<td>✔</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>Provisioning Features</td>
<td>Administrative configuration of custodian</td>
<td>✔</td>
<td>✘</td>
</tr>
<tr>
<td>Availability to Line of Business Integrations</td>
<td>✔</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>Provisioning of new structures in SharePoint</td>
<td>✔</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>Update of metadata on existing structures in SharePoint</td>
<td>✔</td>
<td>✘</td>
<td>✘</td>
</tr>
</tbody>
</table>
4.3 Repstor Service Monitoring

We understand that ensuring our cloud-based applications are monitored, is very important to all customers. We monitor our custodian application using Azure Application Insights (available to our support personnel and development team) for early insights into any application issues.

Within Azure Application Insights we can understand and review the performance of our underlying service, any application issues that require review and receive immediate notifications of issues that could impact our service.

As the Azure Application Insights is only available for internal purposes, we also update the Service Health Dashboard which is available on our Service Status Page which you can find publicly available at http://www.Repstor.com/service-status.

![Repstor Service Status Page](Image)

Figure 6 Repstor Service Status Page

4.4 Office 365 Service Monitoring

Repstor applications are continually monitored but customers can be concerned about the service availability of the underlying Office 365 services. Repstor is keen to ensure how best customers can manage the health of the service, especially they are new to using Office 365.

The first consideration is that Microsoft commit to providing a 99.9% guaranteed quarterly uptime agreement, which is financially backed with Microsoft and dependent on your product licenses. We encourage customers to understand more with their Microsoft Service Providers or Account Managers, to understand more about the service level agreements and how to best manage your service moving forward.

To know more about managing and reviewing the on-going health of your Office 365 environment, we recommend the following areas to review:

4.5 Repstor Support

Repstor offers customers the ability to extend support through a support and maintenance agreement that provides access to our Support team for 3rd and 4th line support requests. We require the customer’s IT function to handle 1st and 2nd line support queries. Customer IT teams are better placed to understand common queries that can include user and computer management that the Repstor team have limited access to support.

You can do one of the following to raise a support ticket:
• e-mail our dedicated support Inbox

• call us within UK business hours to discuss and diagnose your support queries.

The support queries are logged into Repstor’s support system. Each support query generates a unique support reference ticket number and sends an acknowledgement to our customer. The acknowledgement includes our reference for further correspondence.

**Note** We do not currently provide integration of our own support system with other customer support applications, we hope to investigate in the future.

Repstor will respond in accordance to any agreed SLA for the severity of reported issue. This may include an e-mail response or a WebEx session to help investigate the reported issue. We may request for specific logs, diagnostics and other additional information to help diagnose and resolve issues.

If you wish to understand more about our support and maintenance agreement, please discuss this with a member of the Repstor team.

### 4.6 Product Update Schedules

*Repstor* regularly updates its products to include new features, resolve customer-identified issues and include security improvements. Different products have different release schedules and the availability of updates is as follows:

<table>
<thead>
<tr>
<th>Repstor product</th>
<th>Release schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repstor affinity</td>
<td>Quarterly releases</td>
</tr>
<tr>
<td>Repstor assist</td>
<td>More frequent releases if necessary, to address performance or security issues.</td>
</tr>
</tbody>
</table>

**Note** By default, all new additions to functionality are disabled to ensure that customer’s existing capabilities are not impacted.
5  Frequently Asked Questions

Customers can have questions about Repstor applications or how we manage specific areas within our company. To help customers with these topics, we have listed several frequently asked questions. If you have any other questions, please contact a member of the Repstor team.

Q 1. Do you have a formal, documented production change control process?

The Repstor development process includes a tight change control process for Repstor custodian. This uses a multi-stage deployment process. Each stage allows full end-to-end testing of the service. The final stage switches from the staging services directly to production, without interrupting the service.

Q 2. Do we have access to Logs to troubleshoot issues?

Yes, there are application logs available via the custodian application and there is an Office 365 Audit Log available in Office 365, where you can access specific events for troubleshooting or compliance requirements.

Please note, Repstor employees have no access to your Office 365 Audit Log.

Q 3. How do Repstor monitor their systems for malicious use or unauthorized access?

All our customer services run on Azure. Repstor has access to Azure Logs which log all configuration changes or access attempts. We regularly review these and ensure that only the relevant people have access to our Azure environment. Access is regularly reviewed.

Q 4. How will the Repstor team authenticate to our environment during a project?

If you would like us to access your Office 365 environment during a project, we would recommend that you invite that specific Repstor employees account into your Office 365 environment. You can revoke access when the project is complete.

Q 5. How does Repstor manage access to our customer instance of custodian?

In short, we don’t.

We provide the ability for customers to manage access to customer data using SharePoint user authentication. This allows you to easily add or remove people to content using the secure login methods.

Q 6. How do we backup the data within SharePoint Online?

As your data is stored within SharePoint Online, this process is managed by Microsoft and backups are taken at minimum once a day, over a rolling fourteen-day period. However, file backups are different, if deleted files or folders can be restored by end users up to ninety-three days following deletion. If you require a more advanced backup plan, we can look to recommend other partners to assist you.

Q 7. Are Repstor Employees and/or Contractors, required to acknowledge and accept internal polices and accept a non-disclosure agreement?

Yes, this is part of our internal processes.

Q 8. How are secure coding practices achieved in Repstor?

We have a well-honed development process which evolved through many years from an ISO 9001 model. The development process has comprehensive automated testing which includes security testing. We also enforce code reviews for each check-in. The Repstor development team have worked together for many years within the Enterprise Content Management industry – and have a comprehensive background in very secure customer environments.
Q 9. Are Repstor ISO27001 certified?

*Repstor* have achieved both ISO27001 and Cyber Essentials Plus certification.

Q 10. When was your disaster recovery process last tested?

We depend on many routing and recovery capabilities built into Azure. This involves routing customers between different application instances depending on issues occurring at one of them. This is the same process we use to test changes to the product. *Repstor* internally, and selected *Repstor* partners are redirected to the preview application instance where the updated software is deployed. We will test this mechanism at each update of the product.

Q 11. Does the installation of the *Repstor affinity* add-in within Outlook, provide *Repstor* with access to our e-mails?

No, the add-in is installed and configured on the client machine with any files stored on the client machine. We do not have the ability to retrieve or access your private e-mail data for any purpose within *Repstor*. 