www.mcfile.com

1. Brief description

McFile is a Software as a Service (SaaS) for information management and business data. The solution is fully hosted in the cloud, mostly using Amazon Web Services (AWS) and Google Cloud Plataform (GCP) pontual services.

For being in the cloud, McFile is scalable, elastic, and has high availability in their services.

2. Access to the system

I. Access by user

Users can access the system in different ways

- Browsers: It can be accessed normally by the most current versions of the browsers used in the market, Chrome, Firefox, Edge, IE and Safari.
- Apps: Available from the App Store (iPhone, iPad) and Google Play (Android). Through them it is possible to search, register, consult and share documents and information contained in the system.
- McOffice (Plug-in Office): Makes it easy to register and edit documents directly by the Office suite (Word, Excel, Powerpoint and Outlook).

II. System Access / Integration

McFile has Web Services available so that integrations with your data can be developed. These calls follow the REST model and must be made by HTTP POST.

Integration is also possible by using the Java McIntegrator application, available on GitHub publicly. It makes use of the Web Services described above and can access data locally from a database or TXT files, for example.

Another possibility of integration is the use of a "Widget", a Javascript library that can be added in a web application for communication with McFile. It has functions of inserting, searching, and viewing documents.

Every environment also has an emails insertion webhook. When you create an account in McFile, a client@mcfile.com inbox is automatically created, which can be used to easily send files to the system.

These emails can be categorized manually using hashtag (#) or by McOffice through reference tokens ([Ref. XXXXXX]) in the subject of the email.

3. Access security

Data in transit is protected through the HTTPS protocol, with TLS 1.3 certificate.

To access McFile, you must enter valid login and password. A user has their access and permission controlled by a user management screen, where you can change privileges, confidentiality areas, and block access and register new users.

Secrecy areas function as vaults in the system, documents created in one area can only be viewed and accessed by people who have access to it (editing or viewing).

System is protected by CAPTCHA technology, to block access attempts by malicious agents.

Integration calls are also authenticated, using integration key, which can be of two types: per user or global.

Each user's access can also be configured with IP rules, blocking logins that do not respect previously registered IPs. Thus, you can control where selected users use the tool.

System is enabled for integrations through OAuth 2.0 protocol and OpenID Connect.

4. Data and file management

I. Localization

All data stored in McFile is kept on servers and services in the São Paulo region.

II. Files

The files in McFile are stored in the Amazon S3 (Simple Storage Service) solution. They are replicated on multiple geographically separated servers so that they are protected from any malicious action or system crash. In addition, the files are stored encrypted using standard AES-256.

All access to the files is done through api protected by encryption and access keys.

For final deletion of a file, a special two-tier approval procedure is required, providing Multi-Factor Authentication (MFA) authentication code.

For more information about S3, see: https://aws.amazon.com/s3/

III. Database

The database uses Amazon RDS (Relational Database Service) and is maintained in the latest version of patches through periodic updates.

Data is encrypted in transit and at rest, using market standard AES-256.

For more information about RDS: https://aws.amazon.com/rds/

IV. Backup

In addition to automatic file replication, the system has two more backup policies.

Database: Backup occurs every 15 minutes and is retained for a week. Full snapshots are created daily.

Search index (used by the search module): Backup occurs daily and is retained for one month. Can be generated again by the database.

Backups are stored encrypted in S3, also having redundancy on different servers.

V. Audit

All activity of service users is monitored and logged in audit logs.

Administrators and managers can generate full reports with a user's entire history and/or file.

VI. Warranties

Customer data is protected by NDA (Non-disclosure agreement) between the parties. Additionally, they are not trafficked out of the Amazon environment by the McFile support team.
In the event of a contract termination, the data is returned to the customer in a folder structure and subsequently destroyed, as defined in the contract.

Data destruction is done by disabling media using nist market standard 800-88.

5. Infrastructure management

I. Monitoring and auditing

The entire cloud environment is continuously monitored to ensure performance, security, and auditing.

Monitoring is done through services against malicious activities, unauthorized behaviors and health checks that validate availability and response time of services.

Among the malicious activities, we can highlight DDoS attacks, compromise of credentials, API calls from known malicious IPs, among others.

For more information on some services used, the two websites can be found below:

1. https://aws.amazon.com/shield/
2. https://aws.amazon.com/guardduty/

In addition, any action is logged in audit logs that can be analyzed and compiled in case of need.

II. Patches and updates

Database, operating systems, and tools are periodically updated with last patch available.

Larger changes, such as operating system versions or database engine, are scheduled in advance, informed to customers if there is any impact, and made by a specialized team.

III. Disaster Recovery Policy

In case of interruption of the primary server, contingency server is triggered through AMI technology (Amazon Machine Images), which enables the creation of a machine image. This image can then be used to create servers whenever necessary.

The policy has the following parameters:

- RTO (Recovery time objective): 2 to 4 working hours, depending on dns propagation time.

- RPO (Recovery point objective): Database is retrieved to its state up to 15 minutes before the claim occurred. Files are saved according to premise S3. The previous day's index is retrieved, and the most recent records are reindexed.

IV. Compliance and ISO

Cloud vendor servers and services operate with ISO 27001 standard quality standards, standard for Informations Security Management System (ISMS).

Professionals of Destaque Gestão Documental receive periodic training on security practices and commitment to the data they manage.

Destaque also follows procedures and standards defined by ISO 9001:2015, ISO 27001:2013 and 27018:2018.

6. History of changes

DATE	REVIEW	HISTORIC
08/03/2021	01	Initial version