mcfile.com

1. Brief Description

McFile is a Software as a Service (SaaS) solution for managing corporate information and data.

The solution is fully cloud-hosted, operating on global providers with high availability and security, scalable infrastructure, and international certifications.

As a cloud-based solution, McFile is scalable, elastic, and offers high availability for its services.

2. System Access

2.1. User access

Users can access the system in different ways.

Web Browsers

Access compatible with the latest versions of major market browsers, such as Google Chrome and Microsoft Edge.

Mobile applications

Available on the App Store (iPhone, iPad) and Google Play (Android).

They allow users to search, register, view, and share documents and system information.

McFile for Office / McOffice

Facilitates the registration and editing of documents directly from the Microsoft Office suite (Word, Excel, PowerPoint, and Outlook).

2.2. System Access / Integration

McFile provides RESTful APIs for developing integrations with its data and services. The complete API documentation is available at: apidocs.mcfile.com.

Integration is also possible through the McIntegrador application or McFile Integration Engine (MIE).

These methods use the API and can access local data, databases, or TXT files, for example.

Another alternative is the use of the McFile Widget, a JavaScript library that can be embedded into web applications, offering document insertion, search, and visualization features.

Each environment also has a webhook for email ingestion. When an account is created, an address environment@mcfile.com

is automatically generated and can be used for direct file submission to the system.

Emails can be manually categorized using hashtags (#) or automatically via McOffice, using reference tokens in the subject line (for example, [Ref. XXXXXX]).

3. Access security

Data in transit is protected by TLS 1.3 encryption over the HTTPS protocol.

Access to McFile requires valid login credentials, with individual permission control.

User management allows administrators to change privileges, define restricted areas, block access, and register new users.

Restricted areas function as secure vaults: records and documents created within a given area can only be viewed by users with access to the same area.

The system is protected by an application security layer (WAF) that applies OWASP rules, blocks malicious inputs and suspicious IPs, prevents code or SQL injection, and uses CAPTCHA and rate limiting to mitigate automated attacks.

Access can also be restricted by IP rules, blocking logins from addresses not previously registered.

McFile is compatible with OAuth 2.0 and OpenID Connect standards, enabling secure integration with identity providers.

4. Data and file management

4.1. Location

All McFile data is stored on servers and services located in the São Paulo region (Brazil).

4.2. Files

Files are stored using Amazon S3 (Simple Storage Service), replicated across multiple geographically distributed servers, ensuring resilience and high availability.

Data is encrypted at rest using the AES-256 standard, and all access is performed through APIs protected by authentication and encryption.

Permanent deletion of a file requires a special two-layer approval procedure, including the provision of an MFA (Multi-Factor Authentication) authentication code.

4.3. Database

The database uses Amazon RDS (Relational Database Service), maintained with the latest patches through periodic updates.

Data is encrypted both in transit and at rest, following industry standards.

4.4. Backup

In addition to automatic replication, the system adopts two complementary backup policies:

- **Database**

Automatic backups every 15 minutes, retained for seven days. Daily full snapshots.

- **Search index**

Daily backups, retained for seven days. The index can be restored from the database.

All backups are stored encrypted in S3, with redundancy across multiple availability zones.

4.5. Audit

All user and administrator actions are recorded in audit logs.

Detailed reports can be generated with full history by date, user, record, or file.

4.6. Guarantees

Customer data is protected by confidentiality agreements (NDAs) between the parties and is not transferred outside the AWS environment by the McFile team.

In the event of contract termination, data is returned to the customer in a folder structure and subsequently securely destroyed, in accordance with NIST 800-88 (media sanitization).

5. Infrastructure management

5.1. Monitoring and auditing

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

Services are used to detect malicious activity, verify integrity, perform health checks, and analyze logs.

Monitored threats include DDoS attacks, credential compromise, and suspicious API access.

Tools such as AWS Shield and AWS GuardDuty are employed for active protection and automated alerts.

All events are recorded in centralized logs, available for analysis by the technical team.

5.2. Vulnerability analysis tools

Periodic vulnerability scans are performed on servers and applications using automated tools.

These analyses identify and classify risks such as insecure configurations, outdated libraries, and known vulnerabilities, enabling proactive remediation actions.

5.3. Patches and updates

All infrastructure components, databases, operating systems, and applications are periodically updated with the latest security patches.

Major changes (such as database engine or operating system upgrades) are planned and communicated in advance to customers if they cause any system impact.

5.4. Disaster Recovery Policy

In the event of primary server unavailability, a contingency server is activated from an image, enabling rapid environment restoration.

The policy includes the following parameters:

- **RTO (Recovery Time Objective)**: 2 to 4 business hours
- **RPO (Recovery Point Objective)**: up to 15 minutes of maximum data loss

Files remain intact during the process, as they are stored redundantly across multiple availability zones, ensuring high availability and resilience.

Search indexes are restored from the most recent backup, and records are reindexed as necessary.

5.5. International Standards and Compliance

McFile's cloud services and providers follow international information security and management standards.

Destaque Gestão Documental adopts practices and controls based on ISO 9001, ISO 27001, and ISO 27018 standards.

Its team receives periodic training in information security, confidentiality, and LGPD compliance.

The security model also follows the shared responsibility principle in the cloud, see Section 6.

6. Shared security and customer best practices

McFile security is based on a shared responsibility model, in which both the platform and its users play essential roles in protecting information.

While McFile ensures the security of infrastructure, applications, and cloud data, customers and end users are responsible for adopting best practices when using the solution to maintain a secure environment.

6.1. Credential Protection

Users are responsible for keeping their access credentials secure, avoiding the sharing of logins and passwords.

The use of multi-factor authentication (MFA), strong and unique passwords, and periodic credential changes is recommended.

The administrative team must monitor and revoke access for former employees immediately upon termination.

6.2. Permissions and confidentiality management

McFile offers access profiles and restricted areas for granular information control.

Administrators must ensure that each user has only the necessary privileges (principle of least privilege) and that sensitive documents are stored in appropriate restricted areas.

Periodic review of permissions and access areas is essential to maintain a secure and compliant environment.

6.3. Integration with corporate login

Whenever possible, integration with corporate identity providers is recommended (Single Sign-On via OAuth 2.0 and OpenID Connect).

This practice centralizes authentication, facilitates the enforcement of organizational security policies (such as MFA and IP blocking), and reduces the risk of misuse of individual credentials.

6.4. Document storage and sharing

Users should use the secure sharing features provided by the platform, avoiding file transfers through external or unencrypted channels.

Confidential documents must always remain in restricted areas, with controlled viewing and download permissions.

6.5. Best usage practices

- Lock the computer or device whenever away.
- Do not reuse corporate passwords in other systems.
- Avoid accessing McFile on public or unsecured Wi-Fi networks.
- Use antivirus software and keep systems updated on all access devices.
- Notify the system administrator if suspicious behavior or unauthorized access is detected.
- Lock your computer or device whenever you're away.

6.6. Continuous review

Information security depends on constant updates to usage practices.

McFile recommends that companies perform periodic reviews of access, permissions, and restricted areas, as well as regular training on security and confidentiality best practices.

7. History of changes

DATE	REVIEW	HISTORY
01/10/2020	01	Initial release
08/10/2025	02	General overhaul: ISO standards update, inclusion of vulnerability scanning, DR testing, shared security section, and technical/drafting tweaks.