Hyper-secure File Sharing for Federal Agencies & Contractors

"The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten [...] the American people's security and privacy. The federal government must improve its efforts to protect against these campaigns by ensuring the security of information technology assets across the federal enterprise."
- Cybersecurity Infrastructure Security Agency (CISA) Binding Operational Directive 22-01

FileCloud helps state, local, and federal government agencies and organizations remain efficient and compliant with complete data ownership and governance. As a hyper-secure Enterprise File Sync and Share (EFSS) solution, FileCloud provides powerful file sharing, sync, and mobile access capabilities on public, private, and hybrid clouds.

The full feature set includes industry-leading governance controls such as remote access authentication, workflow and retention automation, data leak protection, Zero Trust File Sharing®, compliance support, and granular sharing controls.

FileCloud Security Features

- Endpoint backup
- Multi-factor and CAC authentication
- Unlimited file versioning
- Antivirus scanning and malware protection
- File locking
- 256-bit AES encryption for data at-rest
- SSL/TLS encryption for data in-transit
- Client application security policies
- Active Directory and LDAP integration
- Granular access and share permissions
- Comprehensive audit trail
- SSO and SIEM integration
- Air-gapped network deployment
- Smart Data Leak Protection (DLP)
- Digital Rights Management (DRM)

Zero Trust File Sharing®

FIPS 140-2 Compliant Encryption

At-rest and In-transit encryption

S3 storage encryption with AWS cross-account KMS key

Server-side encryption with AWS KMS-Managed Keys (SSE-KMS)

Server-side encryption with customer-provided keys (SSE-C)

We Can Help You Achieve Compliance!

FIPS 140-2
Federal Information Processing Standard Publication

HIPAA
Health Insurance Portability and Accountability Act

NIST
National Institute of Standards and Technology

CMMC
Cybersecurity Maturity Model Certification

federal@filecloud.com

Security and Data Protection FAQ

FileCloud is used by millions of users around the world, including top Global 1000 enterprises, educational institutions, government organizations, and managed service providers. These organizations trust FileCloud to provide a user-friendly collaboration system while securing digital data

Here are some **frequently asked questions** on the security features provided by FileCloud.

How secure is FileCloud?

FileCloud is hyper-secure, with multiple levels of protection for your data, including:

- High levels of encryption for at-rest and in-transit data
- Granular user and file-sharing permissions
- Client application security policies
- Active Directory integration
- Two-factor authentication (2FA)
- Malware screening
- Access controls through share expiration, file change notifications, download limits, NTFS shares, and Zero Trust File Sharing®

What type of user access does FileCloud support?

- Identity management systems, such as Active Directory and LDAP
- Federal smartcard authentication (CAC/PIV)
- Secure Sockets Layer (SSL) protocols
- Single sign-on (SSO) through NT LAN Manager (NTLM)
- Security Assertion Markup Language (SAML) SSO
- Code-based device authentication for clients and mobile apps
- Unlimited external accounts

How does FileCloud secure shared data?

User Share Options: public and private sharing, expiring shares, password-protected share links, and Zero Trust File Sharing®.

Admins controls: centralized analytics, audit logs, Smart Data Leak Prevention rules, Digital Rights Management, remote device management (remote wipe/client block)

At what level can access permissions be controlled?

FileCloud admins can control access permissions with global, group, and user policies, as well as granular file and folder permissions and Data Leak Prevention rules.

Access permissions are enforced, regardless of location or access method. The most restrictive policy is applied.

federal@filecloud.com