

FIPS 140-2 US Government Encryption Standard

white paper

FIPS 140-2 is a type of encryption validation standard required for US government compliance. This whitepaper goes into the history of FIPS 140, an overview of the regulation itself, and shows you how FileCloud's FIPS 140-2 certification can make your life easier.

US Government Standards

With how many important documents and files are shared online now, encryption is how we protect and keep sensitive information safe. But not all encryption standards are created equal, and when it comes to working with governmental authorities, advanced encryption standards must be in place – this includes not only US government agencies, but contractors and third-parties as well. These organizations must use a specific type of validated cryptography module that complies with FIPS 140-2 (Federal Information Processing Standard).¹

FIPS 140-2 is supported by the CMVP (or Cryptography Module Validation Program), a collaboration between the US government (specifically the National Institute of Standards and Technology or NIST) and the Canadian government to create a standard for cryptographic modules, validation, and compliance. The stated goals of this program are to: “promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.”²



FileCloud FIPS Validation - CMVP Certificate #3338

History of FIPS 140 Validation

FIPS validation has been around since 1994, when the first FIPS 140-1 publication was released. This validation was replaced by FIPS 140-2 in 2001 and will eventually be replaced by FIPS 140-3 in 2026. Currently though, the only available validation is for FIPS 140-2.

There is a difference between *validation* and *compliance* though.

FIPS 140-2 Validation

- FIPS 140-2 is a multi-month process where a product or system’s hardware and software is tested by a NIST-approved lab³. For example, an EFSS solution like FileCloud has 140-2 validation and the [certificate](#) to show it (CMVP Certificate #3338).

FIPS 140-2 Compliance

- FIPS 140-2 Compliance means that some parts of a system (hardware or software) meet the FIPS 140-2 requirements, but that the system is not fully validated and certified — compliance is a much easier process than validation and certification.⁴



Who needs FIPS 140-2 Certification?

As we said above, certain parties must use technology that is FIPS 140-2 certified, including:



US Government Agencies



US Government Contractors



Third-parties working with US agencies

Simply put, if you handle government data, your systems should ideally be FIPS 140-2 certified, but at a minimum, they must be FIPS 140-2 compliant.

A Deep Dive into FIPS-140-2 Requirements

Issued in May of 2001, the NIST report on Security Requirements for Cryptographic Modules replaced the FIPS 140-1 publication, which came out in 1994.

FIPS 140-2 specified the security that was required for a system protecting sensitive (though not classified) information.

It had four levels of security included, Level 1 being the least intensive, and Level 4 being the most.

The report says,

“These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.”

Below you'll see the chart that shows the four levels, and after that we'll go into each level a bit more in-depth.



	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.



	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			



1

As stated above, Level 1's requirements are the easiest to meet, and each level adds onto the level below. For Level 1, all components have to be production-grade, along with secure installation and basic security standards.

2

Level 2 includes everything stated in Level 1, but equipment must also have locks/have tamper-evidence, along with RBAC or role-based authentication.

3

Level 3 adds more physical requirements for tamper-resistance, identity-based authentication (rather than RBAC), and for data ports for "critical security" to be "logically or physically" separate from other ports.

4

Level 4 requires even more physical protection like tamper detection, have an even more secure operating system, and, in the case of an environmental attack, ability to delete information on a device.

These levels are covered in greater detail here. The NIST report that published the FIPS 140-2 standards goes on to say:

"Table 2 summarizes the physical security requirements, both general and embodiment-specific, for each of the four security levels.

The general physical security requirements at each security level are all three distinct physical embodiments of a cryptographic module.

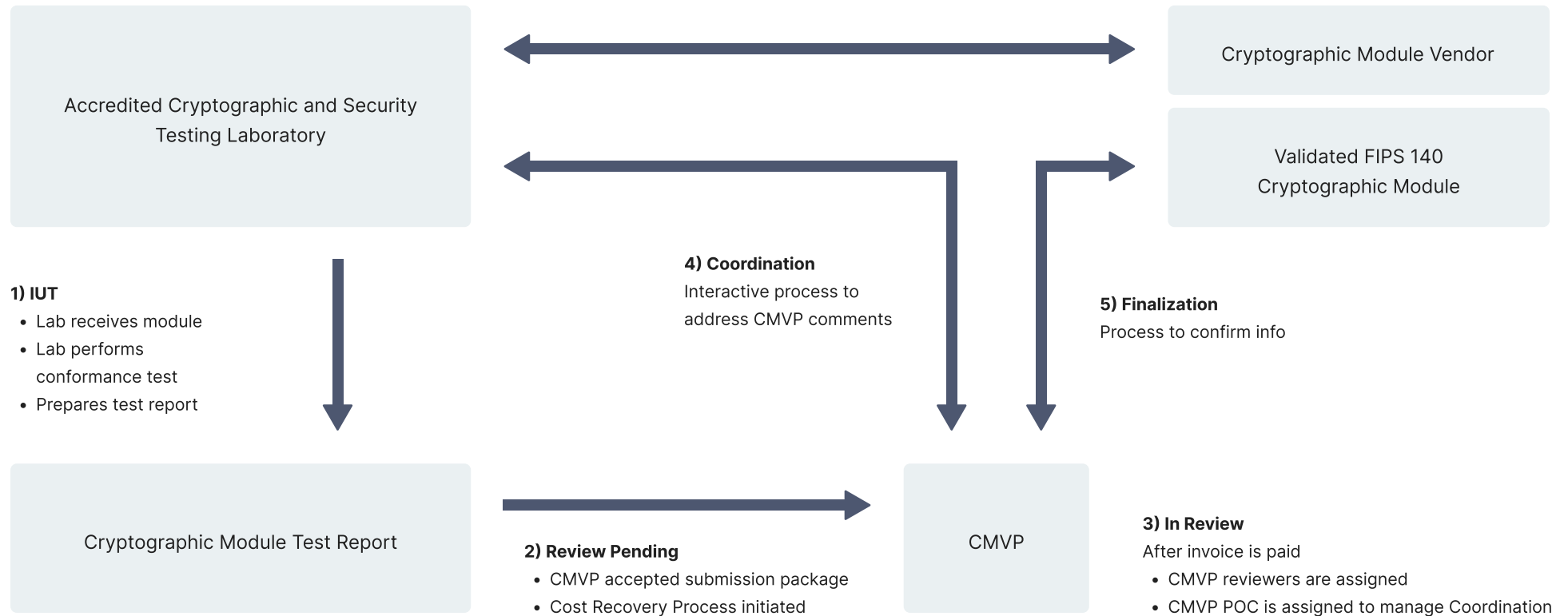
The embodiment-specific physical security requirements at each security level enhance the general requirements at the same level, and the embodiment-specific requirements of the previous level."



FileCloud FIPS 140-2 Validation

FileCloud was given FIPS 140-2 validation in early 2019. SafeLogic, an independently accredited lab, subjected the FileCloud encryption module through a series of tests. After proving conformance with the FIPS 140-2 standard, the module's test report was sent to CMVP, the Cryptographic Module Validation Program, operated by the United States National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of Canada. Their joint office confirmed compliance and issued certificate #3338, available publicly [here](#).

Getting this validation is not easy, as seen in this chart published by NIST. This rigorous process ensures that systems with NIST 140-2 validation can protect highly sensitive and confidential government data from misuse or abuse as well as mitigate risk of cyberattacks.



FileCloud's FIPS 140-2 Certified Encryption Protects Files at Rest and in Transit Security Standards

FileCloud security includes 256-bit AES encryption for data at rest, TLS/SSL protocols for data in transit, two-factor authentication, SSO (single sign-on), automatic anti-virus scanning, unlimited file versioning, file locking, endpoint device protection, comprehensive audit trails, and GDPR compliance. These features build a hyper-secure foundation that supports the FIPS 140-2 compliant encryption module to encrypt files at rest and in transit.

FileCloud meets the necessary security requirements for Cryptographic Modules, formalized by the Federal Information Processing Standard FIPS security (FIPS publication 140-2) and validated by the US National Institute of Standards and Technology (NIST 800-171) and Canadian Communication Security Establishment (CSE).

In greater detail, FileCloud fulfills FIPS 140-2 validation with the following features and tools:

Cryptographic Key Management

FileCloud supports integration with encryption key management services, including AWS KMS. Clients can also bring their own encryption key.



Using AWS's Key Management Service (KMS)
in the AWS Government Cloud region lets government organizations that work with the U.S. government achieve complete control of their content encryption keys.

SSE + CPK (Customer Provided Key)

The customer provides a master key (this is also called SSE + CMK for Customer Master Key). This key is sent with every upload to the storage container.

- This key is not known to FileCloud and can only be read by you
- Slowest encryption speed

SSE + KMS (Key Management Services)

With KMS enabled, new data/objects uploaded to the system auto-generate a key. The object key is needed for decryption.

- KMS can be hosted in FileCloud Online or run on a customer's FileCloud Server account.
- Medium encryption speed



Role Based Access Controls (RBAC)

Role based access controls allow your main FileCloud admin to create different levels of admin roles to restrict access to different FileCloud admin portal sections and components. These different admin roles can be assigned to promoted admin users or groups.

This allows admins to assign users to multiple roles, and permissions are broken down into Read/Create/Update/Delete.

Search

FileCloud's content search indexes all the files and its content. Users can search using a name or partial name of a file, as well as keywords in the content of the file.

Any worthwhile FIPS 140-2 encryption software must come with advanced search functionalities, so data can be quickly located within the system.

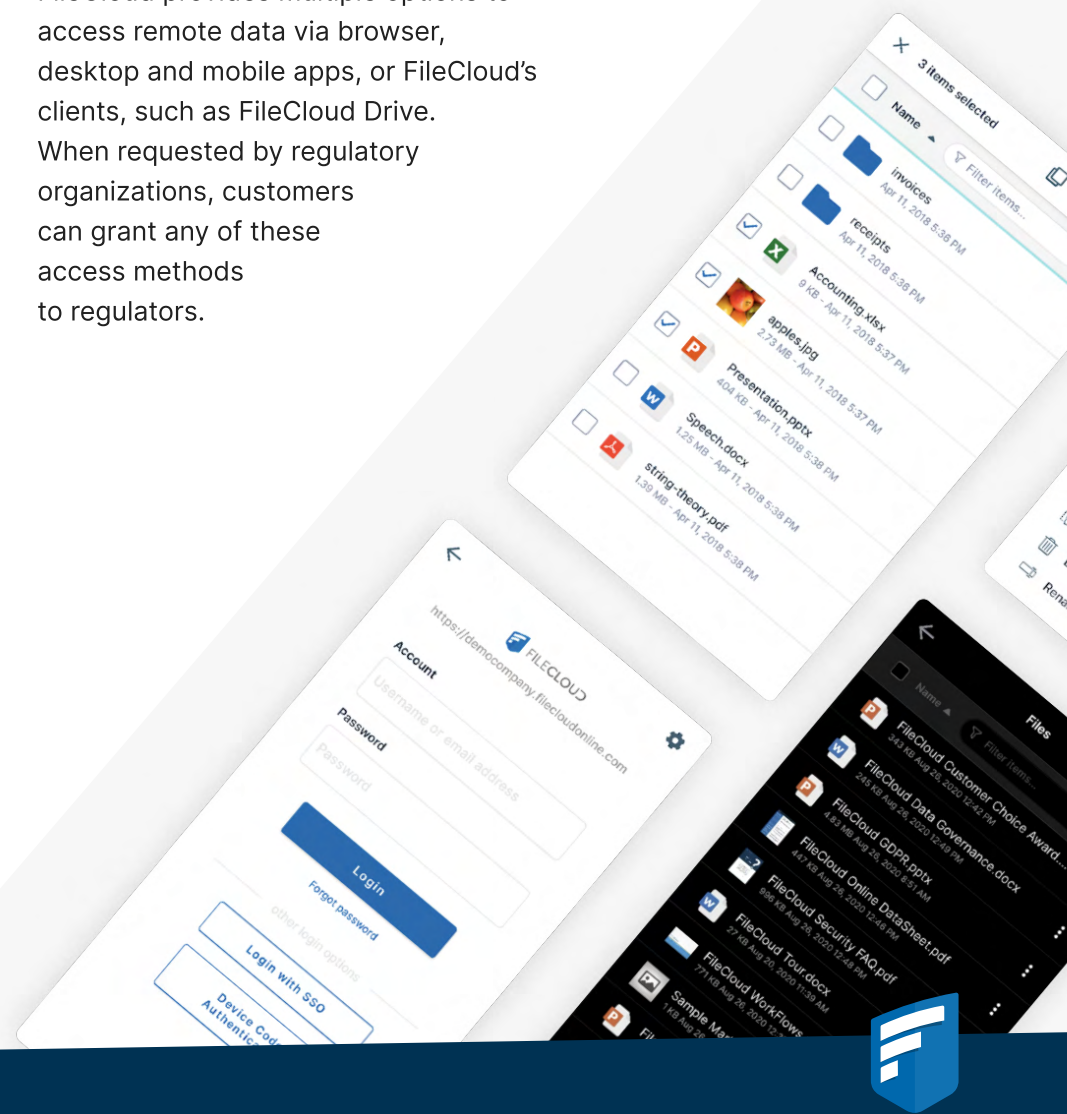
Prevent File Deletion

FileCloud could help you prevent file records from accidental deletion. If a user deletes any sensitive files, FileCloud can be configured to send email alerts to administrators and supervisors. Even if a file is deleted, it is not purged from the system; administrators can restore the files from the recycle bin.

Quick Access to Data

FileCloud provides multiple options to access remote data via browser, desktop and mobile apps, or FileCloud's clients, such as FileCloud Drive.

FileCloud provides multiple options to access remote data via browser, desktop and mobile apps, or FileCloud's clients, such as FileCloud Drive. When requested by regulatory organizations, customers can grant any of these access methods to regulators.



Report and Audit

All file changes are logged in comprehensive audit trails, along with information about who changed the file and when (timestamp) it was changed. Audit logs can be searched based on keywords or by user giving administrators the right tools to triage quickly.

Logs can also be exported as CSV files for ease of external audit or compliance review.

Data Loss Prevention

FileCloud's "High Availability" (HA) architecture helps customers build redundancy across all layers of its infrastructure, ensuring strong protection against losing access to the records.

Data Retention and Archiving

FileCloud features robust data storing, archiving, and retrieving settings, enabling customers or solution providers to create a compliant-ready enterprise file access and sharing solution. Hierarchical retention types ensure that files and folders can be retained according to their need, with restrictions on file modification, movement, or deletion, as well as automated archival after a certain period of time.

Policy Attributes

Policy Name*

Partnership – Close – Admin Hold

Policy Type

Admin Hold

Suspend any action to files due to other retention policies that might affect them.

Description*

John's Partnership – Close – Admin Hold

Hide Policy From Users ⓘ

☐

Enabled ⓘ

☒

Alert On Violation ⓘ

☒

Send email alert ⓘ

☒

Alerts*

johndoe@filecloud.com

Type in a comma-separated list of email addresses of users who need to know that a policy expires.



ServerSync

Changes in the local Windows File Server are seamlessly synchronized to a remote FileCloud Server or FileCloud Online site via ServerSync. These changes include:



**New Files
Added**



**Edits to
Existing Files**



**Files Being
Removed**

ServerSync can also optionally sync FileCloud's folder-level permissions.

The FileCloud permissions can be synchronized to local folders

These permissions are applied as View-Only Access

Having a comprehensive system that handles a variety of permissions is critical. FileCloud can enforce varied levels of access, ranging from full access (read, write, move, delete, download, share) to 'view only' access, which allows users to view files but not download

ServerLink

FileCloud ServerLink is a feature that seamlessly replicates changes on one FileCloud site to another. Replicated data includes:

- Files and Folders (Managed Storage Only)
- User Accounts
- User Groups
- Comments
- Favorites and Favorite Lists
- File and Folder Shares
- Folder Level Permissions
- Metadata
- Sort URLs
- ACLs
- Policies
- Retention Policies
- Notification Path Rules



Data Governance with FileCloud

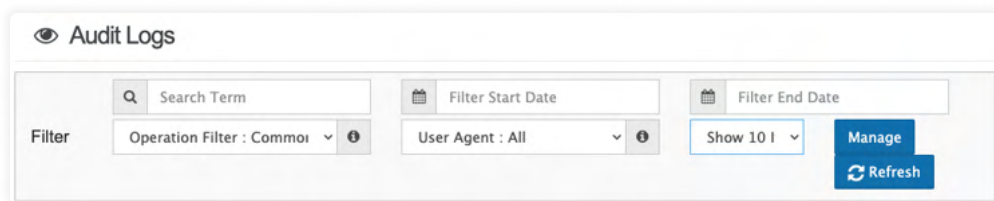
FileCloud is a Content Collaboration Platform (CCP) that specializes in hyper-security and data governance. With standard and enterprise options for on-premises or cloud systems, you can rest assured knowing you have the tools to safeguard and govern your data to comply with regulatory requirements and to build business value. FileCloud offers specific features and functionalities to meet record-keeping and audit log requirements.

Following are some of the FileCloud tools for Compliance



Comprehensive Reports and Audit Logs

FileCloud offers various administrative features to maintain user control over data such as file analytics and reports, as well as detailed, unchangeable audit trail logs. These logs capture who (username) did what (access, modify and delete) to what data (files/folders), when (timestamp), where (IP address), and how (web, mobile, sync client and drive). Admins can search transactions and export audit logs as CSV files for detailed analysis.



Digital Rights Management (DRM)

DRM prevents unauthorized sharing, screenshot capturing, copying, or printing of intellectual property including contracts, sales/marketing reports, eBooks, training materials and other sensitive documents. For even greater control, files can be shared through a secure viewer, where only specific elements will be visible.

Password requirements ensure only authorized users access shared information, and download limits curtail distribution of materials. Share links and permissions can also be updated and access revoked at any time.



Retention Policies

Retention policies are a critical functionality when it comes to record-keeping. With a FileCloud license, you can leverage a hierarchical list of retention policies to meet the distinct needs of your organization. Admins can automate retention processes to secure and manage sensitive or confidential financial information with more consistency and to meet industry or regulatory standards. Available policies include:

Legal Hold:

Freezes digital content to aid discovery or legal challenges. During a legal hold, file modifications are not allowed.

Trash Retention:

Can be configured for automatic and permanent deletion of all files in the Trash bins or to expire with no actions.

Retention:

Identifies digital content to be kept around for an unlimited amount of time before being deleted or released.

Archival:

Moves and stores old organizational content for long term. No Deletion is allowed until a specified time period is reached. After this time, content gets moved to a specific folder.

Admin Hold:

Outranks all other policies and prevents any update or delete of digital content for an indefinite period of time.

Retention policies are attached to files and folders and allow you to define the conditions under which a file/folder is changed/modified/moved. This allows admins to easily and quickly know the data under their control won't be altered or moved.

Hyper-Security

FileCloud supports a multi-tiered approach to security, including automatic antivirus scanning upon upload, ransomware and malware prevention, integrations with security event and incident management (SIEM) software, and implementation of REST APIs for precise data management functionality.

Admins can set additional login requirements through Single Sign-on (SSO) and two-factor authentication (2FA) or integrate with Active Directories. File locking and unlimited file versioning ensure that data is preserved internally, so that collaboration never leads to data loss or overwrite.

FileCloud also uses advanced encryption modules, including AES 256-bit encryption for data at rest, SSL/TLS secure tunnels for data in transit, and FIPS 140-2 encryption certification. Bring Your Own Key policies mean clients can leverage site-specific, managed encryption keys in a multi-tenant setup.

Metadata

FileCloud has built-in metadata sets including image metadata, document lifecycle metadata, color metadata, and many more (along with totally customizable metadata sets) that you can use to provide extra info about files and folders, which can be especially helpful when trying to find files and folders or trying to apply a broad rule across specific file types (for example, you could find all metadata with a color tag easily).



Content Classification

Classification is a major component of data governance. With FileCloud, admins and users can leverage either default or custom metadata tags to support the content classification engine (CCE). FileCloud's smart CCE automatically sorts uploaded content, enabling improved search optimization (including e-discovery and pattern search). Files and data can be easily located and accessed with the use of metadata tags, fulfilling a major component of SEC compliance.

With a classification system in place, admins can also leverage FileCloud's Data Leak Prevention (DLP), which uses a system of rules and metadata to guard against unauthorized sharing or access. The DLP expression builder ensures even team leaders and managers without an IT background can set up the rules they need to secure their data. This feature prevents unauthorized sharing of sensitive financial data.

Endpoint/Remote Device Management









Endpoint device management provides an inventory of all the devices connected to the FileCloud system such as computers, laptops, and smartphones. Administrators can remotely block users or even wipe data on any connected device. The Access Map in the Admin dashboard provides a unique view of connected IP addresses (Geo-IP) to support identification of suspicious activity.

Granular Sharing and User Policies

Admins and users can utilize granular sharing options to ensure only specified information is distributed, whether that information resides in a folder, sub-folder, or a specific file. Share links can be sent as public or private (password protected) with varying degrees of permission (read, write, download, share). For data that falls within the purview of the SEC's record-keeping rules, these permissions can be adjusted as a user, group, or global policy to reflect the WORM format. Shares can also be set to expire after a certain time, and Admin access can be fine-tuned through role-based access controls (RBAC).

DLP

FileCloud's Smart DLP allows admins to monitor malicious or neglectful activity, helping prevent data leaks and losses. DLP allows admins to closely control who gets to access/change what file and when. Admins can create their own DLP rules using IF/THEN statements and the rule expression builder, which, when applied, can prevent data leaks.

Smart DLP							
Add DLP Rule							
Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Client PII	SHARE	(_metadata.exists('cce.pii'))	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	  
Deny Shares of files with ePHI	SHARE	(_metadata.existsWithValue('content.category','ePHI'))	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	  
Deny Download	DOWNLOAD	(_file.pathStartsWith('/master/DLP/DLP Download'))	DENY	ENFORCE	0	<input type="checkbox"/>	  



Learn More

To learn more about FIPS 140-2, click the links below.

[What is FIPS 140-2 and Why is it Important](#) →

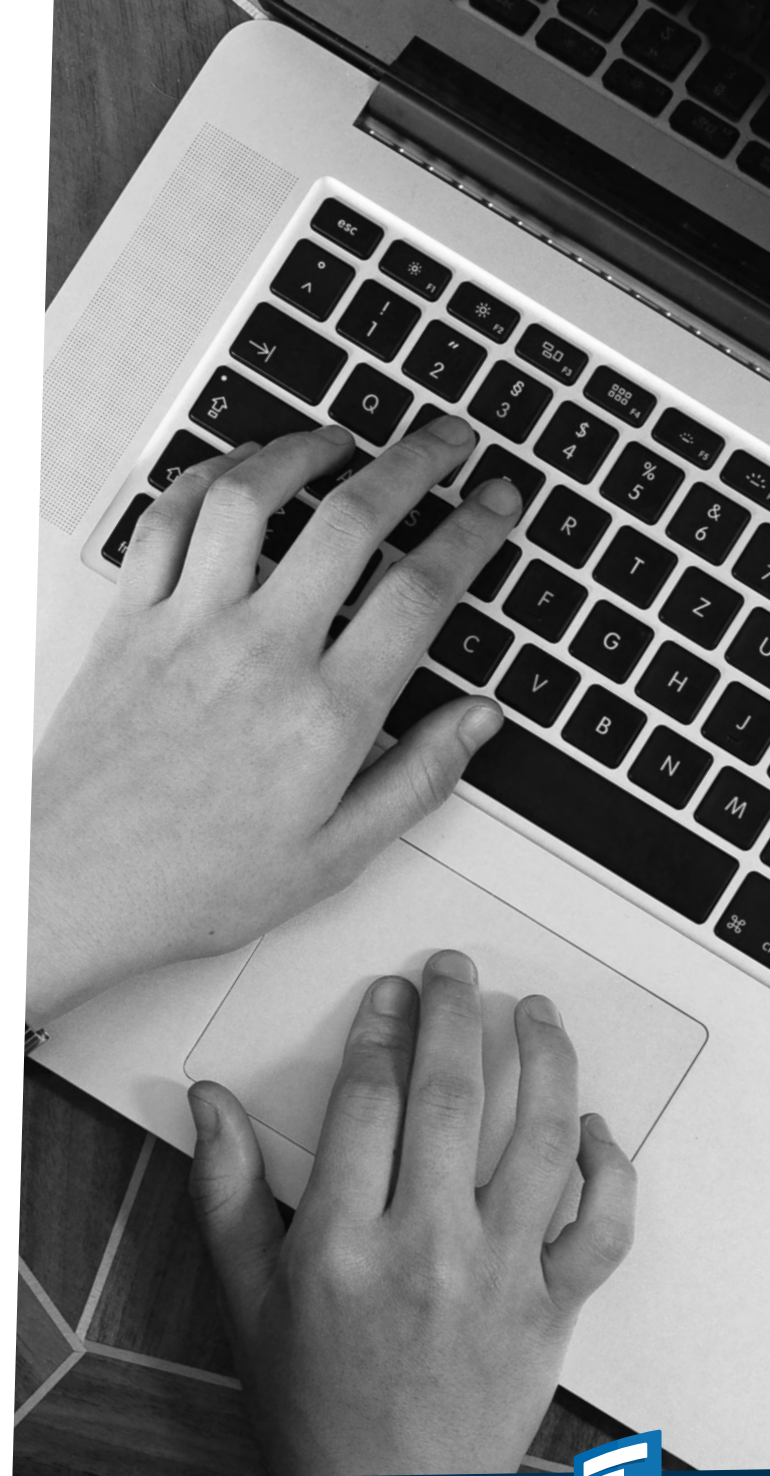
[Cryptographic Module Validation Program](#) →

[FIPS Certified vs. FIPS Compliance: Here's What You Need To Know](#) →

[FIPS 140-2: Validation versus Compliance](#) →

[FIPS 140-2](#) →

[FIPS-140-2-CMVP Management Manual](#) →



About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.



1M+
USERS



3000+
ENTERPRISES



100+
RESELLERS



90+
COUNTRIES



13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480

Fax: +1 (866) 824-9584

CONTACT US



**US Army Corps
of Engineers**



Deloitte.

Copyright Notice

© 2023 FileCloud. All rights reserved.
No reproduction without written permission.

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.

