

Content Compliance for International Businesses

white paper

An expanding regulatory landscape and globalized marketplace mean companies need innovative solutions to untangle the web of compliance requirements.

Compliance – More Than Meets the Eye

When we consider compliance, we usually think of external regulations set by national or international governing bodies. This association is strengthened by recent regulations that have gone into effect such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These bodies establish requirements around data security and privacy that companies and organizations must meet.

However, content compliance permeates much deeper into our business norms than these external regulations. Certainly there are legal obligations that businesses must fulfill, but there are also business expectations about data security on behalf of customers, employees, subcontractors, and vendors.

This business expectation is often unspoken yet acknowledged across industries, entrenched in best practices as a means of competing in the market. Many business dealings are and will be informed by this subtle pressure to instill protections around data, particularly as more and more business is done online and more data is created in this digital/cloud landscape.



The Value of Compliance

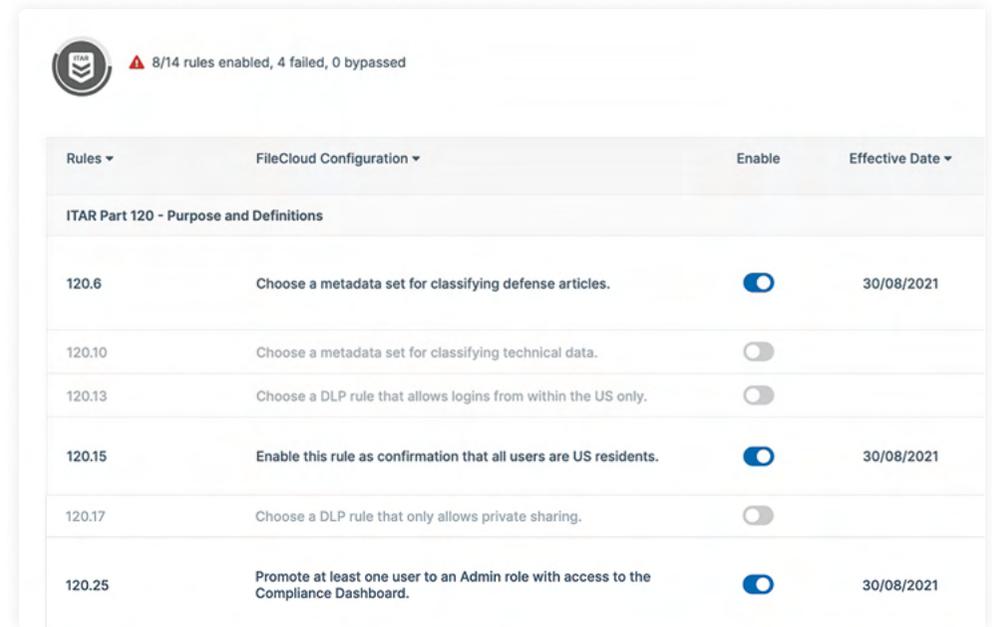
Not all data is created equal, and not all content will require the same level of scrutiny or security protections.

The 2015 [Databerg Report](#), compiled by Veritas Technologies, found that 33% of globally stored or processed data is either redundant, noncritical, or obsolete. 52% of stored or processed data has not been assessed for value and is referred to as 'dark' data.

The remaining 15% is data that has been identified as critical or useful to business operations. This relatively small amount of data though can have drastic consequences if leaked for businesses and connected individuals (employees, clients, contractors, etc.).

For example, an insurance business collects data on clients to assess risk and build profiles through proprietary algorithms. The individual pieces of data (particularly if they are anonymized) will not present a large risk if exposed. However, if the data is not separated from user identities or if entire algorithms or risk profiles are leaked, the business operations could be severely impacted. A major consequence could be that consumers decide the business is not trustworthy or competent.

When we expand our notion of compliance in this way to consider both external and internal forces, we can recognize that compliance is an integral element of building business value through secure, responsive content management. Compliance is a mechanism that serves to harden business security and improve business resilience and flexibility in the market.



Rules	FileCloud Configuration	Enable	Effective Date
ITAR Part 120 - Purpose and Definitions			
120.6	Choose a metadata set for classifying defense articles.	<input checked="" type="checkbox"/>	30/08/2021
120.10	Choose a metadata set for classifying technical data.	<input type="checkbox"/>	
120.13	Choose a DLP rule that allows logins from within the US only.	<input type="checkbox"/>	
120.15	Enable this rule as confirmation that all users are US residents.	<input checked="" type="checkbox"/>	30/08/2021
120.17	Choose a DLP rule that only allows private sharing.	<input type="checkbox"/>	
120.25	Promote at least one user to an Admin role with access to the Compliance Dashboard.	<input checked="" type="checkbox"/>	30/08/2021



Compliance on an International Scale

It's one matter to attain compliance with domestic government regulations. It's quite another when a company operates on an international scale (as many do).

By crossing sovereign boundaries, companies are susceptible to a myriad of compliance standards that will impact how they handle data and deliver value to consumers. These regulations quickly form an inscrutable and potentially clashing web of compliance requirements.

With the advent of global business, cloud technology, and remote operations, it is fair to say that many if not most medium and large-scale organizations operate internationally. This is particularly true as digital business and online markets continue to grow. The boundaries of nations and states are less apparent to the average consumer while seeking goods and services.

Though expanding a business across domestic boundaries means incurring more risk and regulations, it also provides access to a greater pool of consumers, as well as more efficient supply chain or logistics partners. Consider the example of the textile industry:

A simple, white t-shirt can be designed in the United Kingdom by a clothing brand. However, the raw cotton may be sourced from the United States, sent to Columbia to be cleaned and turned into yard, then to India to change yarn into fabric, then to Thailand for cutting and stitching into a piece of clothing.

Only then might it finally arrive in the United Kingdom to be sold to a consumer. This example doesn't even factor in more complicated clothing designs or dyeing processes. If the original company operates an online business, it's also possible the T-shirt could travel still further afield to reach its new owner.

In this example, blurring the boundaries of countries enables garment companies to reduce operating overhead while competing for a larger share of the market without being restricted to the location of headquarters or work sites.

However, the further their supply line spreads and the more consumers they reach, the more the business becomes entangled with a variety of different regulatory requirements.

These boundaries have become even more ephemeral with the COVID-19 pandemic. Businesses all around the world of all sizes were forced to shift to remote operations or forced to close down to slow the spread of the disease and save lives. These challenging conditions cracked open new opportunities to explore international markets while testing the limits of cloud technology and digital collaboration tools.

All this to say that businesses can never really know with 100% certainty all the different borders and boundaries they cross, which invites a level of ambiguity into compliance objectives. Companies must be ready to respond to a shifting landscape of internal and external compliance requirements to compete effectively in our modern international markets.



“I Didn’t Know”

Though international business and remote/cloud technology makes it easier to streamline business operations and reach wider markets, the web of compliance may curb enthusiasm. Regulatory bodies are not forgiving, and penalties for failed compliance can be steep.

The EU’s General Data Protection Regulation (GDPR) is one such example. The authorities that evaluate and penalize companies for GDPR violations have the power to **impose fines** up to €20 million or 4% of a company’s worldwide turnover for the preceding financial year – whichever is higher. Many **major tech companies** have already been fined for violations, including Amazon, Google, Twitter, WhatsApp, and Meta. Amazon has been hit with the highest penalty to date, at €746 million.

External regulations put into place by nation states and governing bodies often build in grace periods. Laws establishing a certain regulation may be passed, but penalties are not levied immediately. This provides some time for companies to identify and implement solutions to meet requirements.

However, once this grace period has passed, enforcement can be swift and uncompromising. For these regulatory bodies, “I didn’t know” is not an acceptable excuse. Even for regulations that are tens or hundreds of pages long with little precedent, the onus remains on the company to discern how the regulation will affect their operations and to implement a solution that will meet requirements.

On a positive note, companies have the freedom to seek out innovative solutions that fit their business needs, thus feeding into long-term business strategy while demonstrating compliance. The developing market of compliance solutions creates a scalable array of options that can do as little as meet the minimum standard of compliance or as much as future-proof a company’s operations.

Typically, these flexible, scalable solutions will provide better value in the long run since they will be worked into the business’ operational strategy. However, for companies just beginning their compliance journey, a smaller solution may provide the necessary compliance coverage while granting insights for future business value.

There is no magic bullet for content compliance that will meet every business’ needs or respond to every current regulation. Just as regulations and digital boundaries continue to shift, so too do content compliance solutions.



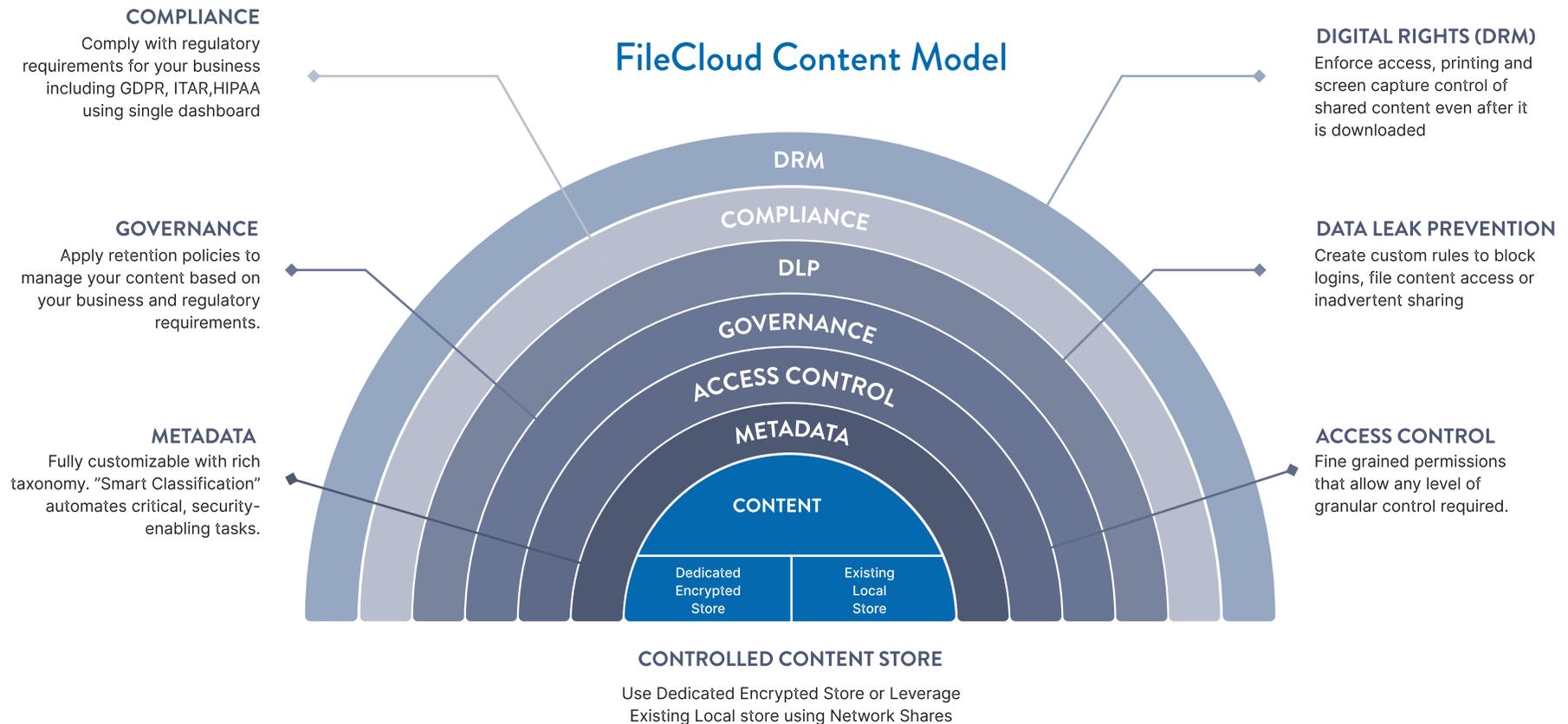
FileCloud provides all the tools users need for document management, records retention, content classification, and file sharing.



FileCloud: a Scalable Compliance Solution that Builds Business Value

FileCloud was developed out of and informed by cloud collaboration technology and the international compliance frontier. As a highly acclaimed Content Collaboration Platform (CCP), FileCloud offers a helping hand to ease the burden of compliance through our shared responsibility model. The hyper-secure platform, combined with flexible and powerful data governance tools, makes FileCloud compliance-friendly, with infrastructure that clients and users can trust.

With its focus on hyper-security and collaborative access, FileCloud strikes an intelligent balance to offer an adaptive platform that meets a variety of compliance and operational needs. The user-friendly interface, fine-tuned admin controls, and granular access settings empower clients to make the most of their content. Deployment options, data governance and audit tools, remote access, and collaboration integrations establish FileCloud as a powerful and adaptive content compliance solution.



FileCloud Compliance Features

Flexible Deployment Options

Flexible deployment means that FileCloud can be operated as a stand-apart solution or integrated with an existing IT infrastructure. FileCloud Server can be run on your own servers and behind your company's firewalls to maintain absolute control over your data and meet stringent compliance requirements for data residency or sovereignty.

If your company needs a lighter weight solution, FileCloud Online can be run with a public cloud service such as Azure or AWS. For maximum flexibility, FileCloud ServerSync can be deployed as a hybrid cloud to leverage the best of both on-premises and public cloud options. For companies that run multiple businesses or sites, FileCloud can also be deployed as a multi-tenant solution, complete with custom branding options for each site.



Hyper-Security

FileCloud was designed from the ground up with security in mind; this foundation ensures that the FileCloud platform is capable of responding to current threats, as well as potential cybercrime strategies that have yet to be launched.

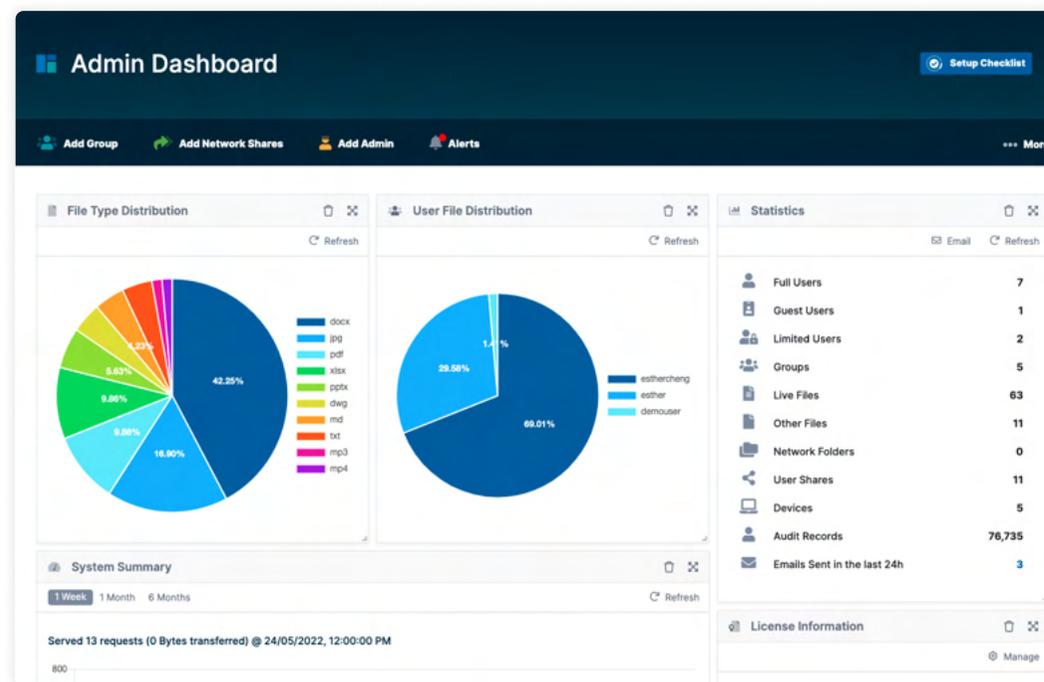
Data at rest is protected with 256-bit AES encryption, and data in transit is encrypted with the latest SSL/TLS protocols. User authentication can be secured and streamlined with options such as Single Sign-on (SSO), SAML integration, and two-factor authentication (2FA). For companies wishing to utilize established directories, FileCloud can be integrated with ADs and LDAPs. Windows NTFS permissions can also be carried over into your FileCloud environment.

Admins have a full, bird's eye view of all file and user activity thanks to comprehensive audit trails, which can be exported for ease of internal and external audits. Custom reports and file analytics can also be set up to provide more insights into storage, file and user activity, and shared data.

Antivirus scanning upon file upload ensures data already in storage is protected from threats. Unlimited file versioning and automatic file backup minimize the risk of data loss in the event of ransomware or malware threats.



A [2020 study](#) conducted by Cybersecurity Ventures found that global cybercrime costs will reach \$10.5 trillion by 2025 (up from \$3 trillion in 2015). For perspective, [Statista](#) found that the global estimated economic loss from natural disasters worldwide in 2021 came up to \$343 billion.



Content and Metadata Management

FileCloud recognizes that limits on storage or file size can severely impact businesses, which is why we support large file size uploads. This ensures users have access to the files they need when they need them. Users can also secure files for more efficient collaboration by locking or checking out files to prevent duplication or overwriting.

Team Folders create a collaborative workspace for teams and departments. Users can also leverage integrations with their preferred applications, including OnlyOffice, Microsoft 365, and Google Docs. Workflow automation removes the burden of (and risk of human error from) repetitive file tasks.

For users on the go, concerns over access or data loss are eliminated thanks to FileCloud's mobile and client applications for online or offline access. Endpoint backup ensures all files are synced with the FileCloud environment, regardless of the device or access point.

Users are also empowered with metadata; default metadata sets come with FileCloud, but admins can also create custom sets to identify files with labels relevant for their business use case. The Content Classification Engine is supported by these default and custom metadata sets so files can be automatically classified upon upload.

Metadata, file comments, and activity streams provide information on active files and folders to support a more informed workspace. Full text and pattern search is available to users based on metadata tags, file names, content, and other variables. This extensive organization ensures users, leadership, and auditors can access necessary information without struggle.

Access Control and Governance

Ensuring only authorized users can read, write, or share secured files is a major element of content compliance. This is why FileCloud enables granular folder, sub-folder, and file sharing through private, public, and time-limited share links.

With role-based access controls (RBAC), admins can adjust internal permissions based on user, group, or global policies. Admins can also manage user access, regardless of the device used, through the remote device management dashboard. In the event of suspicious activity (observed by the admin directly or flagged by an integrated SIEM solution), admins can remotely wipe a device or block a user.

Another key element of governance involves content lifecycle management through retention policies. These policies automate record retention to remove the burden from an admin or admin-user, reducing inefficient manual retention duties (and consequently the risk of human error). FileCloud's hierarchical retention policies ensure content is appropriately retained or decommissioned based on classification, content, user or file activity, and other factors. These policies may block specific actions on files and folders and/or specify what occurs when the policy expires.



FileCloud's Hierarchical Retention Policy Types

Legal Hold:



Freezes digital content to aid discovery or legal challenges. Once legal hold is applied, file deletion or modifications are not allowed.

Trash Retention:



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

Retention:



Identifies digital content to be maintained for an unlimited amount of time before deletion or release.

Archival:



Moves and stores old organizational content over the long term. No deletion is allowed until a specified time period is reached. After this time, content is 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.

DLP, Compliance, and DRM

Fine-tuned controls over data access and sharing ensure that compliance requirements are met while securing data assets for the company, employees, and consumers. Data Leak Prevention (DLP) is one major element to this control. DLP rules can be set to block access based on explicit factors including metadata. These rules override any share permissions or policies to protect data from accidental or malicious user activity.

FileCloud's integrated Compliance Center is another element that addresses content compliance for international business. Configurations for ITAR, HIPAA, and GDPR connect compliance requirements with FileCloud's wide array of tools, policies, and settings, all in one easy dashboard. Compliance rules are regularly checked within the system to scan for potential violations and issues. These rules can also be enabled or disabled as needed to account for external compliance measures enacted by the company.



DLP, Compliance, and DRM

For additional compliance needs, FileCloud also provides support for FIPS 140-2 encryption, CMMC, FINRA, FDA Title 21/Part 11, Sarbanes-Oxley Compliance-Sections 302/404, and CJIS, among others. Whitepapers and checklists provide valuable resources to empower clients to set up FileCloud, so their environment meets their compliance and governance needs. The best-in-class support team is also available to provide additional guidance on how to leverage FileCloud's features.

For maximum control over data, even when it leaves the FileCloud system, clients can take advantage of Digital Rights Management (DRM). This powerful feature maintains control over data through several layers. Granular share settings and the secure document viewer/container can be configured to:



Limit the number of downloads.



Restrict unauthorized sharing, screenshot capture, and printing.



Redact protected text and limit the amount of visible information on the opened file (content is revealed as the user scrolls).



Establish password-secured access for multiple file types (PDF, docx, xlsx, ppt, jpeg, and png).



Revoke shares at any time – if access is revoked and the recipient tries to open the document, the file will be locked.

Conclusion

Content compliance for international business can be complicated, messy, and intimidating. The frontier of globalized markets offers a massive incentive for businesses; yet it also poses additional regulatory burdens that can tangle operations and lead to hefty fines and penalties for non-compliance.

FileCloud is here to simplify the process and provide real ROI for long-term business success, no matter your industry. Through powerful security features and governance tools, FileCloud is an adaptive system that can be launched as an independent solution or integrated with existing IT infrastructure. Secure access and easy-to-use collaboration tools make FileCloud a user-friendly solution that can provide support to meet your compliance needs and beyond.



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.



13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

support@filecloud.com
<https://www.filecloud.com>



1M+
USERS



3000+
ENTERPRISES



100+
RESELLERS



90+
COUNTRIES



US Army Corps
of Engineers



Deloitte.

Copyright Notice

© 2022 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.

