Internal Revenue Service – Publication 1075

FILECLOUD
WWW.GETFILECLOUD.COM

Note: This white paper is intended to provide an overview and is not intended to provide legal advice. For more comprehensive information on regulations and their implications, please consult your legal counsel.

Introduction to IRS Publication 1075

By 2022, 50% of midsize and large organizations in mature regional markets will use a content collaboration (previously known as Enterprise Sharing and Sync - EFSS) platforms to implement document workflows and improve collaboration and productivity.

Strategic Assumption in Gartner's Magic Quadrant for Content Collaboration 2018

For the Third Consecutive Year, Gartner Peer Insights Recognizes CodeLathe's FileCloud as "Voice of the Customer" CCP Customers' Choice

The overview of Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies states:

This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of Federal Tax Information (FTI).

Enterprise security policies address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to implement all applicable security controls. This document contains the managerial, operational, and technical security controls that must be implemented as a condition of receipt of FTI.

The guidelines outlined herein apply to all FTI, no matter the amount or the media in which it is recorded. FTI must be afforded the same levels of protection regardless of it residing on paper or electronic form. Systematic, procedural, or manual security policies must minimize circumvention.

A mutual interest exists in our responsibility to ensure that FTI is disclosed only to persons authorized and used only as authorized by statute or regulation. The IRS is confident of your diligence in this area and believes that this publication will be a helpful resource.

Conforming to these guidelines meets the safeguard requirements of IRC 6103(p)(4) and makes our joint efforts beneficial.

Requirements throughout this document apply to all organizational segments of an agency receiving FTI. It is the agency's responsibility to ensure all functions within the agency, including consolidated data centers and contractors (where allowed by federal statute) with access to FTI, understand and implement the requirements in this publication.

This publication provides the preliminary steps to consider before submitting a request to receive FTI, requirements for proper protection, expectations from the IRS, and considerations that may be helpful in establishing a program to protect FTI. The exhibits in this publication are provided for additional guidance as well as giving credit and background it helps people who want to read the original know where to find it:

This table summarizes the requirements stated in Sections 9.3 and Section 9.4 of the Computer System Security section of Publication 1075.

IRS Publication 1075 - Section 9 Computer System Security				
Sub-sections	**Requirement**	**Details**	**Responsibility**	**FileCloud**
9.3.1	**Access Control**	• Access Control Policy and Procedures (AC-1) • Account Management (AC-2) • Access Enforcement (AC-3) • Information Flow Enforcement (AC-4) • Separation of Duties (AC-5) • Least Privilege (AC-6) • Unsuccessful Logon Attempts (AC-7) • System Use Notifications (AC-8) • Session Lock (AC-11) • Session Termination (AC-12) • Permitted Actions without Identification or Authentication (AC-14) • Remote Access (AC-17) • Wireless Access (AC-18) • Access Control for Mobile Devices (AC-19) • Use of External Information Systems (AC-20) • Information Sharing (AC-21) • Publicly Accessible Content (AC-22)	Shared	Yes
9.3.2	**Awareness and Training**	• Security Awareness and Training Policy and Procedures (AT-1) • Security Awareness Training (AT-2) • Role-Based Security Training (AT-3) • Security Training Records (AT-4)	Customer	Not Applicable
9.3.3	**Audit and Accountability**	• Audit and Accountability Policy and Procedures (AU-1) • Audit Events (AU-2) • Content of Audit Records (AU-3) • Audit Storage Capacity (AU-4) • Response to Audit Processing Failures (AU-5) • Audit Review, Analysis, and Reporting (AU-6) • Audit Reduction and Report Generation (AU-7) • Time Stamps (AU-8) • Protection of Audit Information (AU-9) • Audit Record Retention (AU-11) • Audit Generation (AU-12) • Cross-Agency Auditing (AU-16)	Shared	Yes
9.3.4	**Security Assessment and Authorization**	• Security Assessment and Authorization Policy and Procedures (CA-1) • Security Assessments (CA-2) • System Interconnections (CA-3) • Security Authorization (CA-6) • Continuous Monitoring (CA-7)	Customer	Not Applicable
9.3.5	**Configuration Management**	• Configuration Management Policy and Procedures (CM-1) • Baseline Configuration (CM-2) • Configuration Change Control (CM-3) • Security Impact Analysis (CM-4) • Access Restrictions for Change (CM-5) • Configuration Settings (CM-6) • Least Functionality (CM-7) • Information System Component Inventory (CM-8) • Configuration Management Plan (CM-9) • Software Usage Restrictions (CM-10) • User-Installed Software (CM-11)	Customer	Not Applicable

IRS Publication 1075 - Section 9 Computer System Security				
Sub-sections	**Requirement**	**Details**	**Responsibility**	**FileCloud Server**
9.3.6	**Contingency Planning**	• Contingency Planning Policy and Procedures (CP-1) • Contingency Plan (CP-2) • Contingency Training (CP-3) • Contingency Plan Testing (CP-4) • Alternate Storage Site (CP-6) • Alternate Processing Site (CP-7) • Information System Backup (CP-9) • Information System Recovery and Reconstitution (CP-10)	Customer	Not Applicable
9.3.7	**Identification and Authentication**	• Identification and Authentication Policy and Procedures (IA-1) • Identification and Authentication (Organizational Users) (IA-2) • Device Identification and Authentication (IA-3) • Identifier Management (IA-4) • Authenticator Management (IA-5) • Authenticator Feedback (IA-6) • Cryptographic Module Authentication (IA-7) • Identification and Authentication (Non-Organizational Users) (IA-8)	Shared	Yes
9.3.8	**Incident Response**	• Incident Response Policy and Procedures (IR-1) • Incident Response Training (IR-2) • Incident Response Testing (IR-3) • Incident Handling (IR-4) • Incident Monitoring (IR-5) • Incident Reporting (IR-6) • Incident Response Assistance (IR-7) • Incident Response Plan (IR-8)	Shared	Yes
9.3.9	**Maintenance**	• System Maintenance Policy and Procedures (MA-1) • Controlled Maintenance (MA-2) • Maintenance Tools (MA-3) • Non-Local Maintenance (MA-4) • Maintenance Personnel (MA-5)	Customer	Not Applicable
9.3.10	**Media Protection**	• Media Protection Policy and Procedures (MP-1) • Media Access (MP-2) • Media Marking (MP-3) • Media Storage (MP-4) • Media Transport (MP-5) • Media Sanitization (MP-6)	Customer	Not Applicable
9.3.11	**Physical and Environmental Protection**	• Physical and Environmental Protection Policy and Procedures (PE-1) • Physical Access Authorizations (PE-2) • Physical Access Control (PE-3) • Access Control for Transmission Medium (PE-4) • Access Control for Output Devices (PE-5) • Monitoring Physical Access (PE-6) • Visitor Access Records (PE-8) • Delivery and Removal (PE-16) • Alternate Work Site (PE-17) • Location of Information System Components (PE-18)	Customer	Not Applicable

IRS Publication 1075 - Section 9 Computer System Security				
Sub-sections	**Requirement**	**Details**	**Responsibility**	**FileCloud Server**
9.3.12	**Planning**	• Security Planning Policy and Procedures (PL-1) • System Security Plan (PL-2) • Rules of Behavior (PL-4)	Customer	Not Applicable
9.3.13	**Personnel Security**	• Personnel Security Policy and Procedures (PS-1) • Position Risk Designation (PS-2) • Personnel Screening (PS-3) • Termination (PS-4) • Personnel Transfer (PS-5) • Access Agreements (PS-6) • Third-Party Personnel Security (PS-7) • Personnel Sanctions (PS-8)	Customer	Not Applicable
9.3.14	**Risk Assessment**	• Risk Assessment Policy and Procedures (RA-1) • Risk Assessment (RA-3) • Vulnerability Scanning (RA-5)	Customer	Not Applicable
9.3.15	**Systems and Services Acquisition**	• System and Services Acquisition Policy and Procedures (SA-1) • Allocation of Resources (SA-2) • System Development Life Cycle (SA-3) • Acquisition Process (SA-4) • Information System Documentation (SA-5) • Security Engineering Principles (SA-8) • External Information System Services (SA-9) • Developer Configuration Management (SA-10) • Developer Security Testing and Evaluation (SA-11) • Unsupported System Components (SA-22)	Customer	Not Applicable
9.3.16	**System and Communications Protection**	• System and Communications Protection Policy and Procedures (SC-1) • Application Partitioning (SC-2) • Information in Shared Resources (SC-4) • Denial of Service Protection (SC-5) • Boundary Protection (SC-7) • Transmission Confidentiality and Integrity (SC-8) • Network Disconnect (SC-10) • Cryptographic Key Establishment and Management (SC-12) • Cryptographic Protection (SC-13) • Collaborative Computing Devices (SC-15) • Public Key Infrastructure Certificates (SC-17) • Mobile Code (SC-18) • Voice over Internet Protocol (SC-19) • Session Authenticity (SC-23)	Shared	Yes

IRS Publication 1075 - Section 9 Computer System Security				
Sub-sections	**Requirement**	**Details**	**Responsibility**	**FileCloud Server**
9.3.17	**System and Information Integrity**	• System and Information Integrity Policy and Procedures (SI-1) • Flaw Remediation (SI-2) • Malicious Code Protection (SI-3) • Information System Monitoring (SI-4) • Security Alerts, Advisories, and Directives (SI-5) • Spam Protection (SI-8) • Information Input Validation (SI-10) • Error Handling (SI-11) • Information Handling and Retention (SI-12) • Memory Protection (SI-16)	Shared	Yes
9.3.18	**Program Management**	• Senior Information Security Officer (PM-2) • Additional Computer Security Requirements	Customer	Not Applicable
9.4.1	**Cloud Computing Environments**	• Notification Requirement • Data Isolation • SLA • Data Encryption in Transit • Data Encryption at Rest • Persistence of Data in Relieved Assets • Risk Assessment • Security Control Implementation	Customer	Not Applicable

IRS Publication 1075 - Section 9 Computer System Security			
Sub-sections	**Requirement Details**	**Responsibility**	**FileCloud Server**
9.4.2	**Data Warehouse**	Customer	No Applicable
9.4.3	**Email Communications**	Customer	No Applicable
9.4.4	**Fax Equipment**	Customer	No Applicable
9.4.5	**Integrated Voice Response Systems**	Customer	No Applicable
9.4.6	**Live Data Testing**	Customer	No Applicable
9.4.7	**Media Sanitization**	Customer	No Applicable
9.4.8	**Mobile Devices**	Customer	No Applicable
9.4.9	**Multi-Functional Devices and High-Volume Printers**	Customer	No Applicable
9.4.10	**Network Protections**	Customer	No Applicable
9.4.11	**Systems and Services Acquisition**	Customer	No Applicable
9.4.12	**System and Communications Protection**	Customer	No Applicable
9.4.13	**System and Information Integrity**	Customer	No Applicable
9.4.14	**Program Management**	Customer	No Applicable
9.4.15	**Cloud Computing Environments**	Customer	No Applicable
9.4.16	**Data Warehouse**	Customer	No Applicable
9.4.17	**Email Communications**	Customer	No Applicable
9.4.18	**Fax Equipment**	Customer	No Applicable

References: Internal Revenue Service. (n.d.). *Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies*. Publication 1075 (Rev. 11-2016). https://www.irs.gov/pub/irs-pdf/p1075.pdf.

References:

Internal Revenue Service. (n.d.). Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies.

Publication 1075 (Rev. 11-2016).

https://www.irs.gov/pub/irs-pdf/p1075.pdf.

By 2022, 50% of midsize and large organizations in mature regional markets will use a content collaboration (previously known as Enterprise Sharing and Sync - EFSS) platforms to implement document workflows and improve collaboration and productivity.

Strategic Assumption in Gartner's Magic Quadrant for Content Collaboration 2018

For the Third Consecutive Year, Gartner Peer Insights Recognizes CodeLathe's FileCloud as "Voice of the Customer" CCP Customers' Choice

About Us

FileCloud is used by thousands of customers around the world including Global 2000 enterprises, government organizations, educational institutions, and managed service providers.

"We liked FileCloud's pricing, comprehensive feature set (branding, encryption) and the responsive support."

Stewart

FileCloud Server is the commercial off the shelf software solution that helps businesses securely share, manage, and govern enterprise content.

FileCloud software provides the necessary capabilities for organizations to comply with IRS Publication 1075 under the shared responsibility model.

Note: The end-user is responsible for utilizing suitable FileCloud capabilities as well as managing and maintaining the environment where FileCloud is being hosted to ensure the requirements of IRS Publication 1075 are being met.

13785 Research Blvd,
Suite 125 Austin TX
78750

Email: sales@codelathe.com

Website: www.getfilecloud.com

Phone: +1 (888) 571-6480

Fax: +1 (866) 824-9584