Enabling IRS 1075 Compliance with Virtru

What is IRS 1075?

Internal Revenue Service (IRS) Publication 1075, also known as IRS 1075, provides guidance for U.S. government agencies on how to protect federal tax information (FTI).

IRS 1075 asserts that these agencies protect personal and financial information against unauthorized use, inspection, or disclosure. Additionally, the policy requires other Federal, State, and local authorities that receive FTI directly from either the IRS or from secondary sources must also have adequate security controls in place to protect the data received.

Who does IRS 1075 affect?

IRS 1075 affects any Federal, State, or local government agency that shares FTI. Non-agency organizations and individuals that receive FTI directly from these agencies – or from the IRS – may also be subject to the publication, such as:

- Certified public accountants / accounting firms
- Corporate controllers
- Corporate counsel
- Banks and credit unions
- Credit lending and monitoring services

Many personal indicators, often included in individual tax returns, fall under the definition of FTI that the publication seeks to protect. Some examples include:

- Taxpayer's identity (i.e., Social Security and bank account numbers)
- Personal income details (i.e., nature, source, or amount)
- Tax deductions and receipts
- Withholding information

Since IRS 1075 covers so many different types of data, it's particularly important to understand the specific expectations regarding encryption and data protection.

What Are the Encryption Requirements? How Does Virtru Help?

Although much of IRS 1075 spans beyond encryption, the publication submits a list of encryption-related controls as a baseline for compliance.

Although the IRS does not publish an official designation or certification for 1075 compliance, Virtru helps customers protect FTI shared via email by providing encryption, key management, and authentication capabilities that meet or exceed IRS expectations and protect data no matter where it travels:

Topic	Requirements	Relevant Virtru Features
Email Encryption	Under the circumstances where there is an agency business requirement to use e-mail to transmit FTI, both the FTI data and message itself must be encrypted to protect the confidentiality of FTI.	Client-side encryption with network data protection option
Cryptographic Module Authentication	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, regulations, standards, and guidance for such authentication.	AES-256 bit encryption; Virtru platform libraries certified for FIPS 140-2 compliance
Transmission Integrity	The information system protects the integrity of transmitted information.	Persistent, client-side encryption; customer-managed encryption keys

Topic	Requirements	Relevant Virtru Features
Transmission Confidentiality	The information system protects the confidentiality of transmitted information.	Persistent, client-side encryption; customer-managed encryption keys; Virtru Customer Key Server (CKS)
Cryptographic Key Establishment and Management	When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	Key management and other cryptographic functions automated by Virtru's SaaS server or CKS
Use of Cryptography	Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked.	Virtru platform libraries certified for FIPS 140-2 compliance
Mobile Encryption	All FTI maintained on mobile media shall be encrypted with FIPS 140-2 validated data encryption and, where technically feasible, user authentication mechanisms.	Client-side mobile apps for iOS and Android

Going Beyond the Requirements

In addition to these requirements, Virtru provides other valuable security and control capabilities for organizations looking to comply with IRS 1075:

- **Persistent Access Control –** Revoke access to FTI shared inadvertently, or set message expiration periods when communicating with recipients who do not require long-term access to tax return information.
- **Message Audit –** See when messages are forwarded and revoke access at any point to ensure that only authorized recipients can access FTI.
- **Search and E-Discovery –** Unlike S/MIME and PGP, Virtru's client-side encryption keeps message content searchable and exportable in the event of an audit, Freedom of Information Act (FOIA) request, or other e-discovery requirement.
- **Customer-Hosted Encryption Keys –** Virtru's Customer Key Server (CKS) allows agencies and other organizations to choose where their encryption keys are located. As a result, they can ensure that keys stay within the United States, while also preventing third party cloud providers from ever accessing their unencrypted data.

Have more questions about IRS 1075 encryption requirements?

Contact sales@virtru.com today to speak with one of our compliance experts.

More Than 6,000 Organizations Have Made the Switch to Virtru