Protect Technical Data and Support ITAR Compliance

Virtru's end-to-end encryption, enforceable security settings, granular access controls, and customer-hosted key management capabilities prevent foreign access to technical data in the cloud.

Enable ITAR Compliant Sharing and Storage of Technical Data

The ITAR Encryption "Carve Cut" Rule states that:

- Cryptographic protection must be applied prior to data being sent outside of the originator's security boundary and remain undisturbed until it arrives within the security boundary of the intended recipient. This means encrypting data prior to emailing or sharing it.
- Encryption must be certified by the U.S. National Institute for Standards and Technology (NIST) as compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2), or meet or exceed a 128-bit security strength.
- Information that can be used to decrypt (access) the technical data may not be shared with a third party.

FedRAMP

Virtru hosts everything in the U.S., uses encryption algorithms that comply with FIPS 140-2, is FedRAMP authorized at the moderate impact level, and adheres to the security controls defined by NIST SP 800-53. Virtru cannot access your protected data at any time.

Unlock ITAR Compliant Digital Supply Chain Workflows

True Privacy

Prevent foreign entities, hackers, cyber-spies, and cloud vendors from accessing data or the keys protecting it with end-to-end encryption and customer-hosted keys.

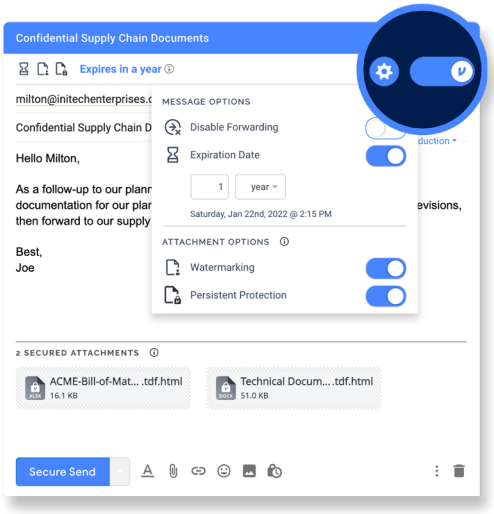
Secure Sharing

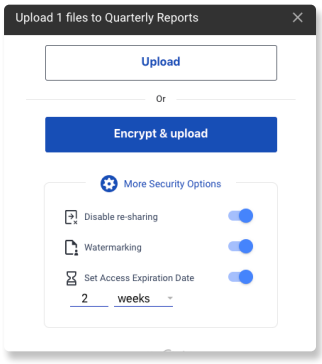
Keep ITAR technical data protected wherever it's shared throughout cloud-based supply chain workflows and maintain persistent control and visibility at all times.

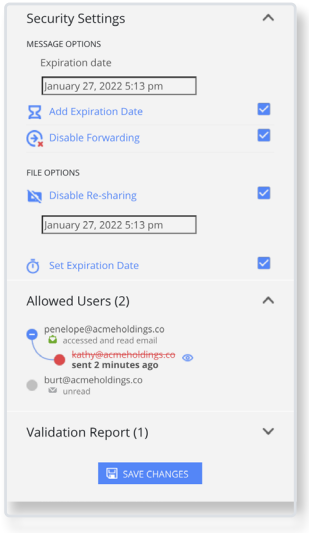
Expanded Innovation

Create limitless collaboration workflows with partners that support new service and product innovation to drive growth while you maintain ITAR compliance.

Seamless Data Protection and Control for the Infrastructure, Software, and Devices You Use Today







Ability to Set Mandatory Encryption & Access Control

Prevent human error by automatically adding encryption for users who handle ITAR-protected data to protect emails and files (including drafts). Revoke messages, disable forwarding, set expiration, watermark files, and maintain persistent control of files. Designate “encrypt & upload” as the only option for adding documents in Google Drive.

Support Data Governance Through Granular Audit Trails

View when and where messages and files have been accessed and adapt controls for evolving workflows and supply chain requirements.

Proven Platform to Support ITAR Compliance with Google and Microsoft

Trusted Data Format

US government approved data protection standard that binds encrypted data to policies and metadata to protect technical data.

Software Development Kit (SDK)

Embed data protection and access controls into the apps and systems that power your sensitive, digital supply chain workflows.

Key Management

Host your own keys so unauthorized parties can never access your data. Integrate with existing processes and Hardware Security Modules.

More than 6,000 organizations trust Virtru to collaborate with confidence

verizon Kubota Tower Semiconductor CLARK CONSTRUCTION

virtru

Learn how Virtru helps you meet ITAR compliance with an affordable, all-inclusive subscription that also supports your organizational goals for data protection: **virtru.com/contact-us**