FILECLOUD

ITAR Compliance for High-Security Sectors

FileCloud Provides Seamless ITAR Compliance for Defense, Engineering, Architecture, Aerospace, and Construction

User-Friendly UI
An intuitive Compliance Center dashboard means FileCloud admins can view all ITAR configurations at a glance. Recommendations on best practices are also provided, allowing for seamless implementation, as well as troubleshooting of any configuration problems.

Compliance Center
The FileCloud Compliance Center maps ITAR requirements to FileCloud security settings that, once activated, ensure adherence. These include SSL, encryption, customized metadata, DLP, and smart content classification.

Network Protection
FileCloud's security capabilities allow you to monitor and control your network traffic. These include encryption of data in transit and at rest, SIEM integration, 2FA with policy control, ICAP integration, detailed audit logs, and more.

AWS GovCloud
Retain full control over data that falls under ITAR by hosting FileCloud on AWS GovCloud. This cloud storage solution includes ransomware protection, FIPS 140-2 encryption, end-to-end encryption, and more.

Record-Keeping
All ITAR-related activities are subject to stringent record-keeping rules. Records must be maintained for five years from the date of the relevant transaction in a format readily available to the US government. Retention policies let you seamlessly automate ITAR record keeping. Export reports and logs can be archived for auditing purposes.

Data Leak Prevention
Entities that fall under ITAR are obliged to prevent data leaks to civilians, criminals, or organizations that may be a threat to national security. Unlike many other file-sharing products, FileCloud's Smart DLP allows for ITAR compliance in a local network or the cloud.

Four Pillars of ITAR

Pillar 1 USML	This contains many obvious defense-related items, such as firearms, explosives, and naval vessels. However, a wide range of commercial products and services that can be used for military purposes are also covered. These include: ✓ Training ✓ Electronics ✓ Chemicals ✓ Satellites ✓ Software ✓ Information (such as drawings and manuals)
Pillar 2 Technical Data	Technical data has a broad definition in ITAR. It not only includes sending a physical package containing data, or transmitting data electronically, but also travelling abroad to provide data. Disclosing data in a speech to foreign nationals, or even in a private conversation, also falls under the definition of data export. Exporting technical data is considered just as egregious as exporting physical products, and in some cases worse. This is because technical data can enable hostile actors to manufacture products on a large scale. It is a serious export violation that can threaten the integrity of the defense supply chain and national security, as well as potentially costing lives.
Pillar 3 Services	The provision of services related to an item on the USML falls under ITAR. Services can include installation, repair, troubleshooting, engineering, training, and consulting. Items requiring such services, for example, could include certain flight control systems, UAVs, and protective clothing.
Pillar 4 Parts & Components	If an item is on the munitions list, parts and components that are specifically designed for an item on the USML are also subject to ITAR. However, parts and components are sometimes listed instead on the Commerce Control List and regulated under the Export Administration Regulations (EAR) instead of ITAR.

Contact Us

Frequently Asked Questions About ITAR

What is ITAR?

The International Traffic in Arms Regulations (ITAR) is a U.S. export control law. It applies to entities that manufacture, export, or temporarily import defense products or services.

What is Covered by ITAR?

A broad range of products and services are covered, including imaging systems, satellites, body armor, spacecraft, and training. The full array of products and services regulated by ITAR is found on the United States Munitions List (USML).

Who Must Adhere to ITAR?

Entities that are part of the military supply chain must adhere to ITAR, whether they are manufacturers, wholesalers, distributors, software vendors, vendors, contractors, or third-party suppliers.

What is the Regulatory Body for ITAR?

ITAR is regulated by the U.S. Department of Defense Directorate of Defense Trade Controls (DDTC).
The main mission of the DDTC is to ensure that foreign policy objectives and national security are not compromised by the export of products, services, and technical data.

Why is ITAR Important?

The USML contains products and services that, if exported by unauthorized channels, could affect national security and, potentially, human life. Violations of ITAR can result in serious civil and criminal sanctions.

There are also restrictions under ITAR on the transfer of controlled technology and data to foreign nationals within the U.S.

Which Sectors are Affected by ITAR?

Sectors affected by ITAR include defense contractors, aerospace, architecture, satellite and space, military equipment, telecommunications, aviation and avionics, construction, and the maritime industry.

Any entity that deals with defense-related goods, services, or technical data should carefully evaluate whether ITAR compliance applies to them.

"FileCloud is a great platform for those looking to have an ITAR compliant solution for file storage and sharing. Very secure and well thought out piece of software."

– Defense and Space professional