ITAR Compliance Checklist for Data Protection

How to protect ITAR technical data from access by non-U.S. entities wherever it's shared in order to meet compliance requirements.

The International Traffic in Arms Regulation (ITAR) controls the export of defense- and military-related items to support the U.S. government's national security and foreign policy goals. The United States Munitions List (USML) contains the articles, services, and related technology that ITAR regulates, including straightforward military items like firearms, ammunition, and aircraft, but some less obvious items like personal protective equipment (e.g. hazmat suits) and IoT sensors.

Also protected is ITAR "technical data"—any information, including blueprints, documentation, schematics, flow charts, etc. needed for the design, development, manufacture, operation, maintenance or modification of items on the USML. The broad range of the USML means ITAR compliance isn't just for arms dealers but all organizations involved in the supply chain for any good or service that could be used for military and defense purposes.

The Risk of Noncompliance

Because ITAR noncompliance leads to some of the most significant consequences of all data regulations, it is not to be taken lightly and boils down to one thing: preventing non-U.S. persons from accessing ITAR technical data in the cloud. If an organization is found to be in violation of this, noncompliance penalties can result in civil fines up to $500,000, criminal fines up to $1M, 10 years imprisonment, and/or being barred from conducting any export business in the future.

ITAR Data Protection Checklist

After more than four years of deliberation, the U.S. Department of State issued a final ruling modernizing and unifying the role of end-to-end encryption in securing sensitive data and enabling cloud adoption. Effective March 23, 2020, organizations can store and share ITAR technical data in cloud environments if it is protected from access by foreign entities. Firms in manufacturing, aerospace and defense, telecommunications, defense contracting, or any other industry that handles ITAR technical data should incorporate the following data protection capabilities into their compliance programs:

- ☑ **End-to-End Encryption:** Encrypt email and files containing ITAR technical data within the client to prevent access by foreign cloud servers or personnel, effectively resolving geolocation and personnel permissions concerns.
- ☑ **Access Controls:** Set expiration and disable forwarding for additional controls that prevent unauthorized foreign access. Revoke access to reduce the risk of foreign access in event of a data breach and watermark files containing ITAR technical data to deter file-based leaks.
- ☑ **Persistent Protection:** Maintain control of attachments to prevent foreign access wherever they're shared, ensuring ITAR compliance beyond the initial email.
- ☑ **Data Loss Prevention:** Detect ITAR technical data in email and files and automatically enforce encryption and access controls.
- ☑ **Granular Audit:** View when and where ITAR data has been accessed as it's shared throughout the supply chain, and adapt controls for evolving collaboration and access requirements.
- ☑ **Key Management Capabilities:** Host your own keys so that only your authorized US personnel can access the keys protecting ITAR technical data for ultimate control.

Virtru Unlocks ITAR-Compliant Digital Supply Chain Workflows

Privacy

Prevent foreign entities from accessing ITAR technical 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.

Innovation

Unlock new collaboration workflows with partners that support new service and product innovation to drive growth.

Learn how Virtru can support your ITAR compliance programs today: virtru.com/contact-us.