

White Paper:

ITAR Compliance 101: Protecting Technical Data



Understanding ITAR compliance

Compliance with the International Traffic in Arms Regulations (ITAR) is the cornerstone of safeguarding information related to the international arms trade. Enacted in 1976, ITAR governs the export and import of defense-related items and services listed in the [United States Munitions List](#) (USML). The ITAR regulatory framework is mandated by the US federal government for manufacturers, exporters, and brokers of defense articles, services, or related technical data.

The scope of ITAR compliance can extend across the entire supply chain of companies, from wholesalers and third-party vendors to hardware and software manufacturers and distributors. Its scope is massive; the Department of Defense supply chain alone includes approximately 5 million items from [more than 100,000 suppliers](#), while the broader American defense industry was worth [\\$741 billion this year](#).

In the tech and aerospace industries, ITAR significantly influences the manufacturing, sale, and distribution of products. Noncompliance can result in significant fines and potential criminal prosecution.

ITAR registration

Any entities that manufacture, sell, or distribute products on the United States Munitions List, including those serving as component suppliers, are required to be ITAR-certified. To become certified, companies must register with the US Department of State's Directorate of Defense Trade Controls (DDTC) and obtain a license to export USML-listed material, including technical data like diagrams and plans. Violations can have severe consequences, including civil fines up to \$500,000 per violation, criminal fines reaching \$1,000,000, and imprisonment for up to 10 years per violation.

Key aspects of ITAR (22 CFR 120-130)



Covers military items or defense articles



Regulates goods and technology designed for military purposes



Encompasses space-related technology due to its applications in missile technology



Includes technical data related to defense goods and services



Requires a stringent registration and certification process

2020 ITAR amendment, a.k.a. the Encryption Rule

In December 2019, the US Department of State amended ITAR to allow cloud storage for technical data under certain conditions. Effective March 2020, the amendment allows organizations to transfer certain kinds of technical data outside the United States without having to register it as an export.

Prior to the Encryption Rule, companies needed a [license to export technical data](#) — including both classified defense articles and unclassified materials — if they wanted to send or store that data outside the United States. As of March 2020, businesses may store unclassified technical data in cloud-based servers outside the US as long as that data is kept safe from unauthorized access with end-to-end encryption. This amendment presents new challenges for global corporations, which must meticulously ensure compliance when transferring or storing data related to many specific technologies.



ITAR technical requirements

End-to-end encryption

To secure unclassified technical data, ITAR requires organizations to use end-to-end encryption in order to secure data in transit from the sender to the recipient. This end-to-end encryption is defined as the provision of cryptographic protection of data, such that the data is not unencrypted between an originator (or the originator’s in-country security boundary) and an intended recipient (or the recipient’s in-country security boundary). In other words, only the sender and recipient, and no other user or system, can access data. If technical data is stored on common file systems (e.g. file servers, cloud storage platforms), that data needs to be encrypted independently from the infrastructure to ensure that no privileged user, admin, or cloud provider can access the data.

ITAR also requires that the end-to-end encryption technology leverages a FIPS 140-2 compliant module. All levels of FIPS 140-2 (Level 1 to 3) are sufficient for this purpose.

Control of the encryption algorithms

The means of decryption must not be provided to any third party, meaning that the sender must control access to the encrypted data. Unfortunately, this requirement disqualifies native encryption methods of common data storage solutions, since the encryption algorithm is tied to the infrastructure provider (e.g., the server or the service) instead of the sender or the data itself.

Stringent access controls

To meet ITAR compliance, organizations must avoid the broadly defined “unauthorized release” of technical data, which [legal experts](#) note could include scenarios where a foreign national’s user account is accidentally granted access to encrypted storage containing technical data, even if that person never actually accesses the data.

Metadata obfuscation

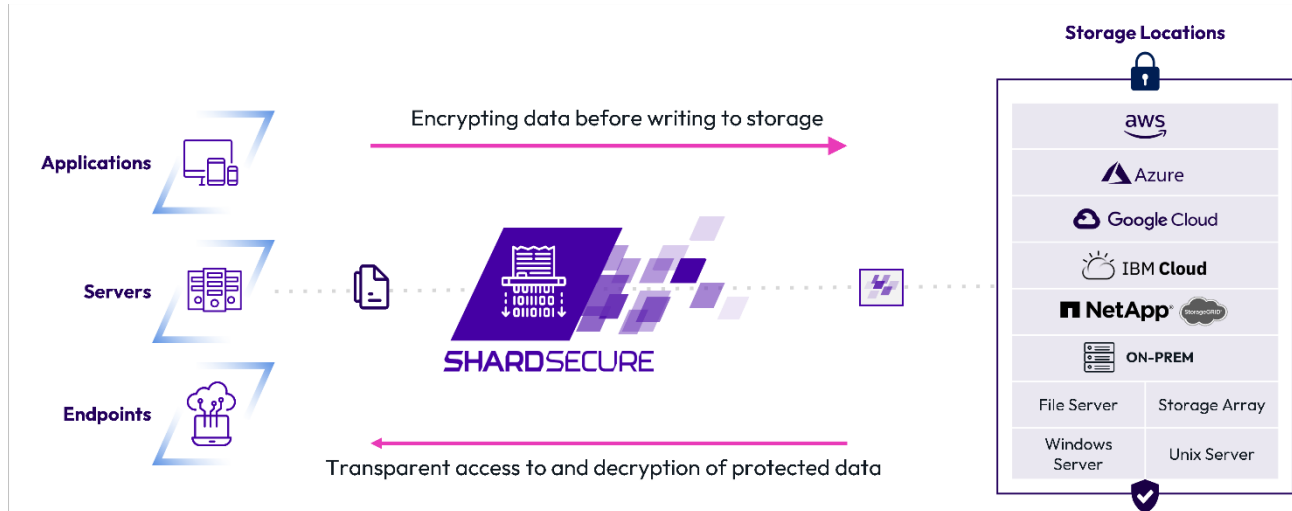
ITAR requires that end-to-end encryption technologies protect entire files, not just parts of them. This means that both the file content and its metadata, including the file name, must be obfuscated if they are transferred or stored outside the US. Unfortunately, traditional encryption solutions commonly provide obfuscation or encryption for only the file content, not the name, size, or author of the file. This adds an additional challenge to complying with the metadata obfuscation requirement.

Requirements	
	Encrypt/Decryption of Data
	User Management
	Metadata and content needs to be encrypted
	Dynamic Data residency

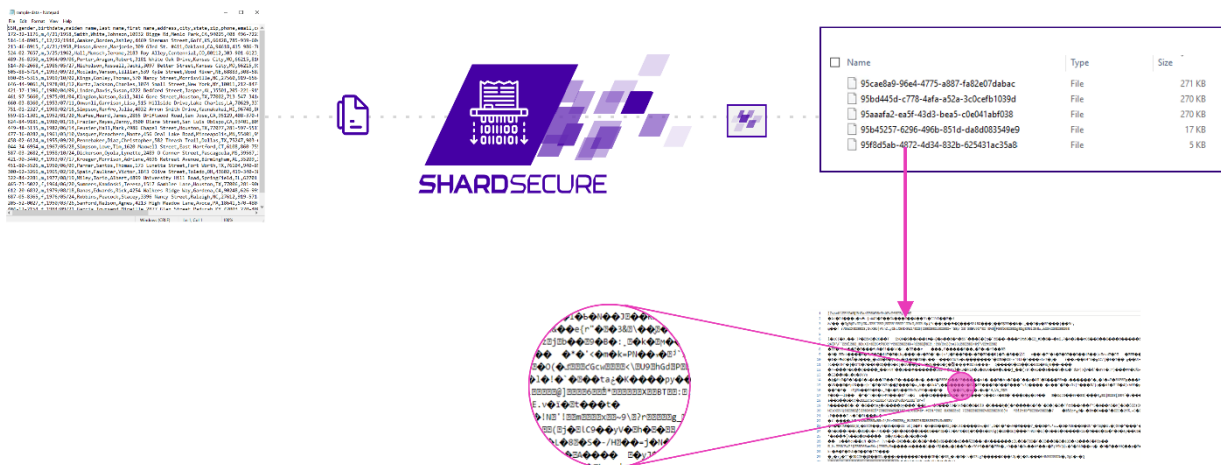


ShardSecure enables data security for ITAR compliance

ShardSecure offers a robust, agentless end-to-end encryption solution for ITAR regulated data, enabling ITAR compliance without the need for installation or distribution of encryption agents. Data protected using the ShardSecure platform can be accessed via the platform's API and/or UI to fulfill a variety of use cases.



ShardSecure addresses the metadata obfuscation requirements for ITAR technical data by obfuscating not only the file content but also its associated metadata, including names, tags, extensions, timestamps, file size, authors, and versions. Once ShardSecure encrypts a file, attackers are not able to identify which ciphertext belongs to which file.



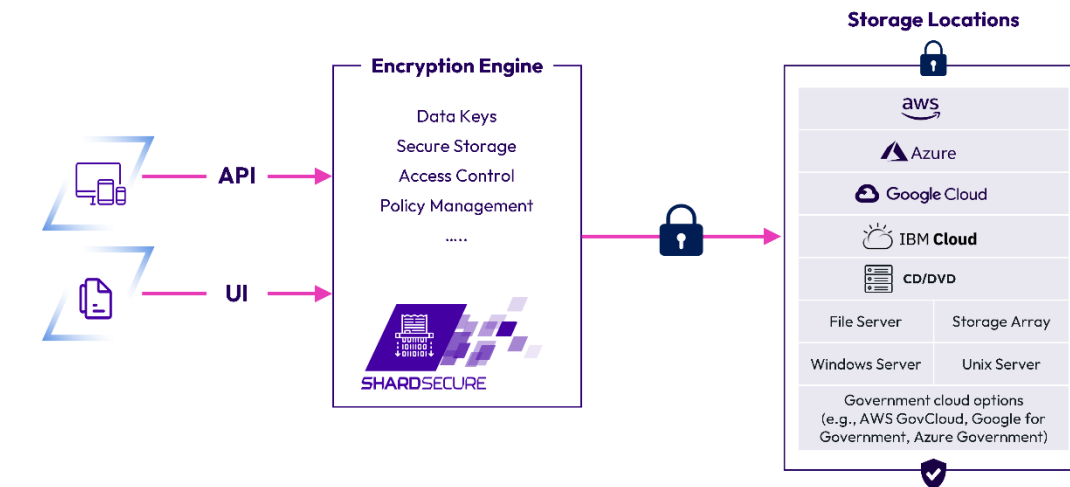
Advanced data protection and privacy

The ShardSecure platform uses agentless end-to-end encryption to maintain the security and privacy of unstructured data on-premises, in the cloud, and in hybrid- and multi-cloud environments. The platform keeps data safe from unauthorized users, separating infrastructure administrator and cloud service provider access from sensitive data. This is crucial for ITAR compliance, which requires that technical data not be subject to unauthorized release to any third party.

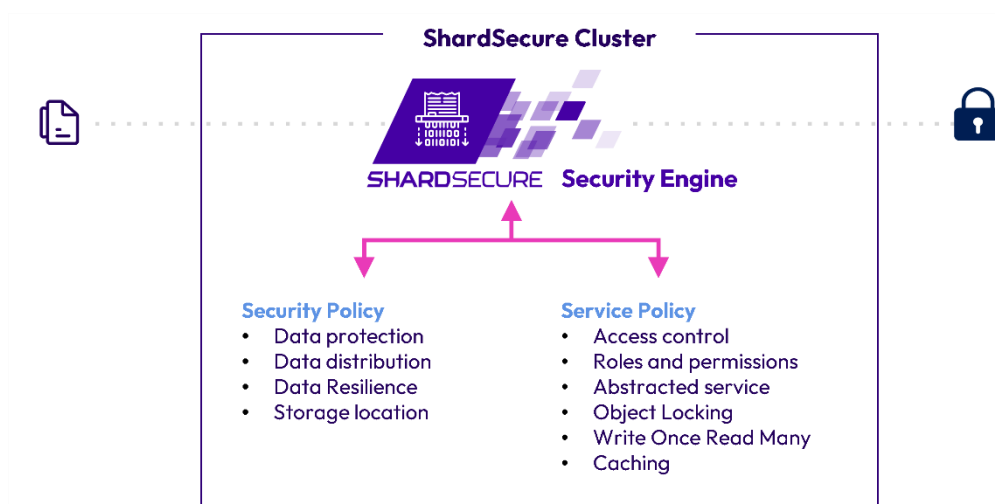
Traditional agent-based solutions can slow performance and drain security team resources. They are often difficult to manage at scale and may be incompatible with newer workloads and cloud services. The ShardSecure platform offers an innovative alternative, allowing companies to secure their data from internal and external threats while reducing complexity.

Encryption with least-privilege access

The ShardSecure platform allows authorized users to easily encrypt and copy files to a central storage location. Its encryption engine handles everything related to encryption and access controls while simplifying workflows.



Shardsecure's policy engine enables organizations to not only design data access rules but also define different rule sets for different types of data protected by the platform. The policies and rule sets include information about data protection, encryption, residency, and storage as well as policies related to lifecycle, such as versioning, object locking, immutability, and write once read many.



ShardSecure is FIPS 140-2 Level 1 compliant. It also offers integration with market leaders of Hardware Security Modules (HSMs) to achieve FIPS 140-2 Level 3. While ITAR defines any FIPS 140-2 level as sufficient, ShardSecure enables its customers to achieve FIPS 140-2 Level 3 compliance, if required.

Seamless data sharing and user access

Most organizations have data sharing requirements to enable data exchange between different systems. ShardSecure's API makes it possible to not only share data in an ITAR-compliant manner but also facilitate the introduction of automated workflows for data sharing between organizations. ShardSecure provides a powerful REST API as well as SDKs for most common programming languages, allowing companies to effectively secure ITAR data without impacting existing data and user workflows.

```

import os
import boto3
from botocore.exceptions import NoCredentialsError

ACCESS_KEY = os.getenv('SS_ID')
SECRET_KEY = os.getenv('SS_secret')
SHARDSECURE = 'https://poc-jw.poc.aws.shardsecure.com'

def upload_to_aws(local_file, bucket, s3_file):
    s3 = boto3.client('s3', endpoint_url=SHARDSECURE, aws_access_key_id=ACCESS_KEY,
                      aws_secret_access_key=SECRET_KEY)

    try:
        s3.upload_file(local_file, bucket, s3_file)
        print("Upload Successful")
        return True
    except FileNotFoundError:
        print("The file was not found")
        return False
    except NoCredentialsError:
        print("Credentials not available")
        return False

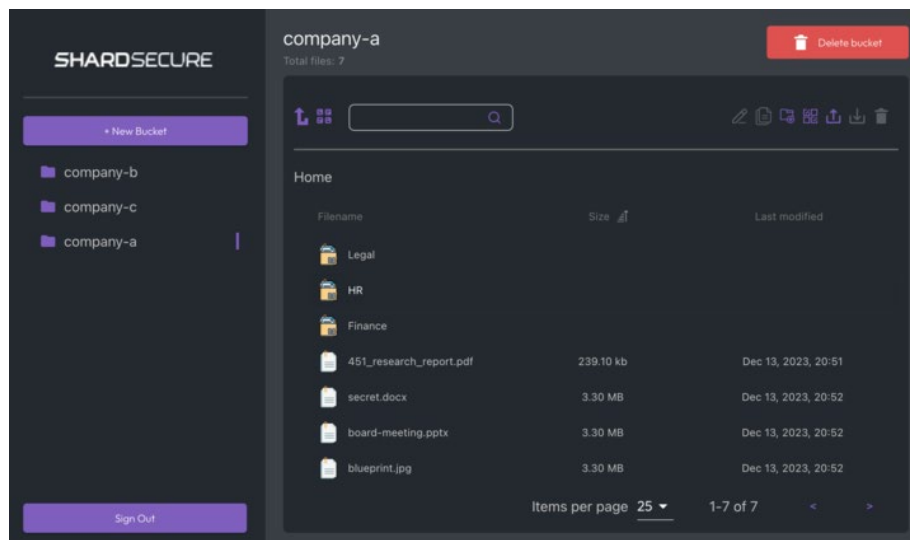
uploaded = upload_to_aws('pii.txt', 'python', 'pii.txt')

```

SDKs for:

- Command Line Interface
- .NET
- C++
- Go
- Java V2
- JavaScript
- PHP V3
- Python
- Ruby V3

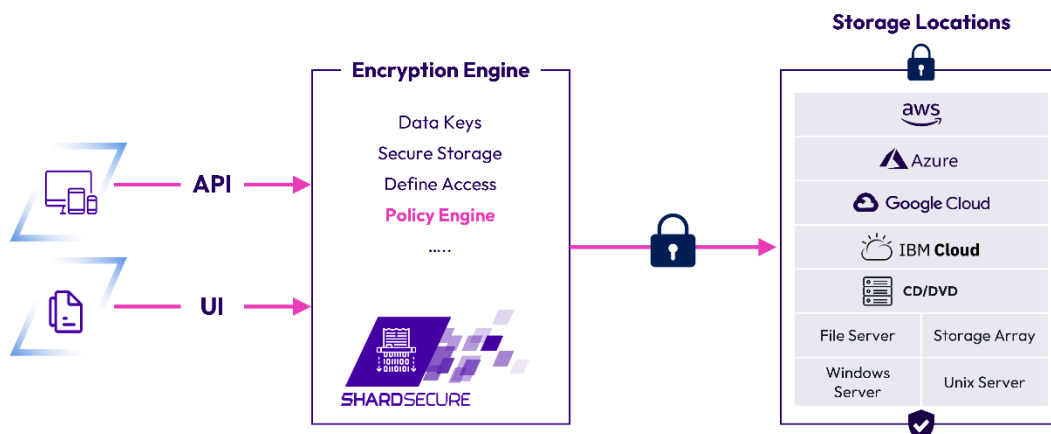
ShardSecure's web interface enables users to have a seamless user experience when sharing data with third parties. The innovative UI also enables users to encrypt/decrypt files regardless of size.



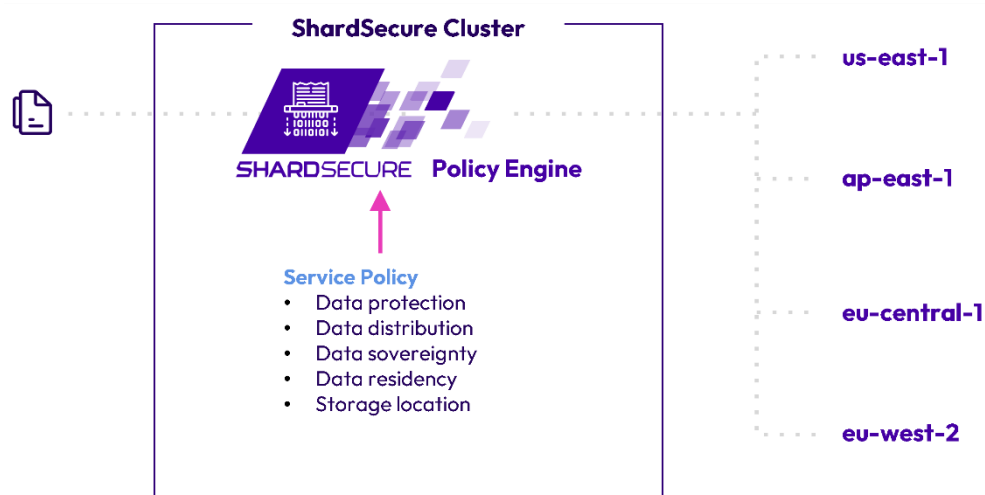
These API and UI capabilities enable different business units and organizations to utilize end-to-end encryption to meet ITAR requirements without negatively impacting existing business processes or user experience.

Embedded controls for data residency

The ShardSecure platform keeps organizations in control of their data, addressing data sovereignty and residency concerns. Companies can utilize the cloud and on-premises storage providers of their choice, in the geographic locations and jurisdictions of their choice, to mitigate data transfer risks.



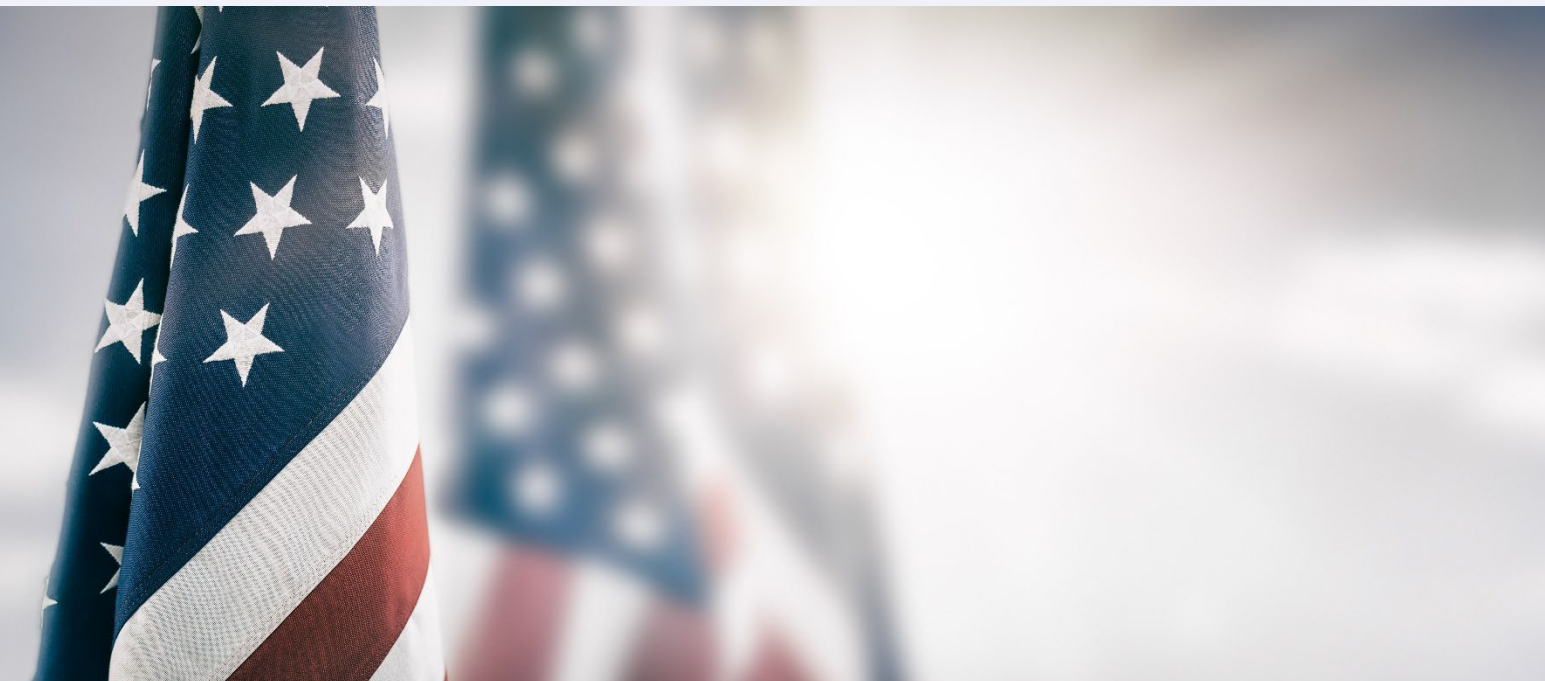
The built-in policy engine can be configured to ensure that data resides within predefined jurisdictions, ensuring compliance with jurisdictional requirements. Dynamic data routing happens automatically based on metadata, tagging, and policy.



Conclusion

A comprehensive understanding of ITAR compliance is crucial for companies handling defense materials and technical data. The consequences of noncompliance are severe, so businesses must ensure they meet the strict standards imposed by the US Department of State. This includes not only registering with the DDTC and obtaining necessary licenses but also implementing strong end-to-end encryption solutions to control access to sensitive information.


ShardSecure's enhanced data protection simplifies ITAR compliance for organizations involved in the defense, aerospace, and tech sectors. To learn more about our technology, [visit us online](#) or [book a demo](#).



 @ShardSecure

 @ShardSecure

 @ShardSecure

 101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

 info@shardsecure.com

**SHARD
SECURE**