ITAR Compliance Best Practices Guide

Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

Table of Contents

Executive Summary & Overview 3

Data Security Best Practices 4

About Aurora® 10

Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

Executive Summary & Overview:

International Traffic in Arms Regulations (ITAR) is a set of US Government regulations that deals with the export and temporary import of defense articles and services.

ITAR regulations dictate that information and material pertaining to defense and military related technologies, including technical data may only be shared with U.S persons. This includes but is not limited to technology pertaining to satellites and launch vehicles, software developed for the management and use of military applications. Basically, ITAR governs the people, data and systems involved in arms and defense manufacturing and contracting.

Penalties for ITAR Violations include: Criminal fines for corporations or individuals of up to $1 million per violation and/or imprisonment of up to ten years for willful violations. Civil penalties for corporations and individuals include fines up to $500,000 per violation relating to unauthorized exports of defense articles/defense services and Debarment from export of defense articles or defense services.

Being ITAR compliant is really about having a good data security strategy and defensive technology implementation in place. On a basic level, this strategy will address the access requirements (Only U.S persons can have access to ITAR information), the exporting or transmitting limitations (Defense information cannot be exported or transmitted to non-authorized personnel without explicit permission from the Federal Government) and the internal security requirements (ITAR governed businesses need to do due diligence and invest in the security of ITAR regulated information).

Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

ITAR Compliance Data Security Best Practices:

What can organizations do to protect data with regards to ITAR compliance? We listed a short, summarized list below that can help organizations with ITAR compliance through some data security best-practices. It is important to understand that data security is not an end result, but a continuous journey in protecting your information assets. We implement solutions, test and validate our security by third parties and constantly fine tune our security posture, while enabling business units to function optimally. Sound more like an art form than a science? It can be.

We've listed a few best-practices below that can help you get started on your journey:

Security Policies & Incident Response Procedures:

An ITAR specific security policy is the foundation of a data security practice and strategy. However, this is not a check box or one time deliverable, but a living, breathing document--as the business environment changes, so do the policies and the strategy. These policies should address physical and network security considerations as well as incident response procedures. The best-intentioned security measures cannot guarantee that we will not be breached. However, in the event of a breach, a good incident response program can be the difference between a quick remediation or a costly data breach. The policies and incident response procedures should be tested and validated annually. Lastly, the policy documents also function as a baseline for employee security awareness training, also a critical component to ITAR compliance and addressed in more detail further in this guide.

Next Generation Firewall:

Attackers are getting more and more sophisticated. Several of them are now organized and sponsored by nation states. Smart, agile perimeter security is vital for ITAR compliance and for protection from savvy hackers and ever changing threat vectors. Traditional firewalls are a thing of the past. Perimeter firewalls today have to provide advanced threat defense from malware, viruses, and zero day attacks as well as provide traditional firewall functionality. Some of the new functionality to look for is sandboxing (for Malware protection), IPS/IDS functionality,

Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

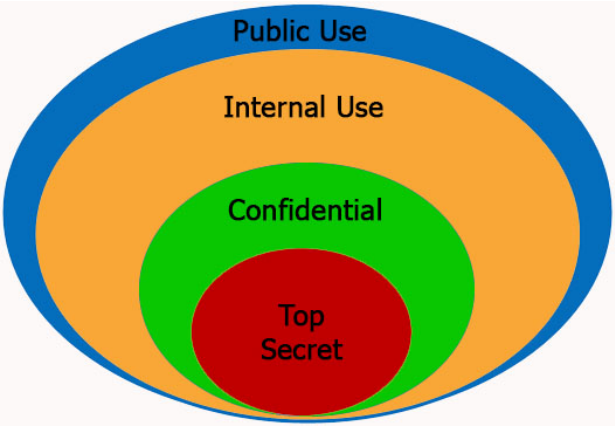
some SIEM (Security Identity and Event Management) functionality, Application Protection, an easy GUI based management and easy incident response capability. If our security team cannot easily identify, manage and respond to attacks, a highly complex firewall can truly work against

us. Look for complexity in functionality, but ease in ongoing management of next generation firewalls.

Data Classification:

All data is truly not created equal. We are all concerned about Data theft, be it credit card information, healthcare (PHI) information or private and confidential employee data or trade secrets. In recent cases, we have heard a lot about corporate espionage and hacking threats from competing nation states. Well, how do we go about protecting our information assets from data thieves?

In most cases, a combination of Data Classification, Data Leakage Prevention and Encryption will get you there. Data classification is a pre-requisite to a successful Data Leakage Prevention (DLP) implementation. Before we can protect our data from leaking, we need to classify information into some iteration of the below four categories: 1) Public Use, 2) Internal Use Only, 3) Confidential and 4) Top Secret.



In order to accomplish this task:

- We usually scan the environment (**data discovery**) for key words and phrases and content that the business unit deems confidential and at risk.

Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

- This information is identified and **consolidated** initially. It's a lot easier to safeguard assets in 1-5 locations, rather than if they were spread out all across the network.

- Once the data is consolidated, appropriate protection and **data security** (data at rest encryption for example) measures can be applied to the data or the devices it resides on.

From that point on, all the information assets can be tagged appropriately (Example: Public Use, Internal Use Only, Confidential and Top Secret). The organization can then set policies for *data in use* and *data in motion*. A Data Leakage Prevention (DLP) solution can then follow the policies we set to protect data from leaving the organization or getting into the wrong hands internally as well.

In conclusion, for an effective data security strategy, we really have to lay the foundation through a data classification exercise, and then follow it up with data security measures like DLP and Encryption.

Data Leakage Prevention:

There are three employee scenarios that a properly implemented DLP solution can protect you against:

- The well-meaning insider: This is the accidental leak. The innocent employee who made a mistake. Someone emailing themselves, or taking data home to work on it, mentioning what they do or worked on their social media page, leaving a USB device or smart phone at the coffee shop, etc.

- Malicious Insider: The employee that didn't get the promotion he/she thought they deserved, or just a trouble maker trying to leak information, or someone working for the competition or a foreign state (in the case of ITAR specifically).

- Malicious Outsider: Competitors, enemy states, corporate espionage, hackers, etc fall into this category.

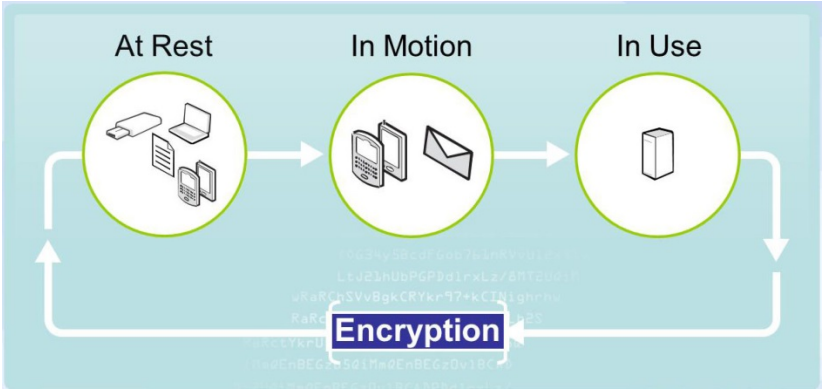
Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

Once data is appropriately tagged, we can then have DLP protect it from all three scenarios listed above. Lastly, if sensitive data does need to leave the organization for valid business reasons, it needs to be encrypted.

Data Encryption:

Encryption policies must be in place to effectively secure all types of data including:

- Data at Rest (Laptops, desktops, USB Devices, Offsite Backup, Databases, etc.)
- Data in Motion (Emails, File Transfers, Web Traffic, etc.)
- Data in Use (SharePoint, Private Cloud, File & Application Servers, Database, etc.)

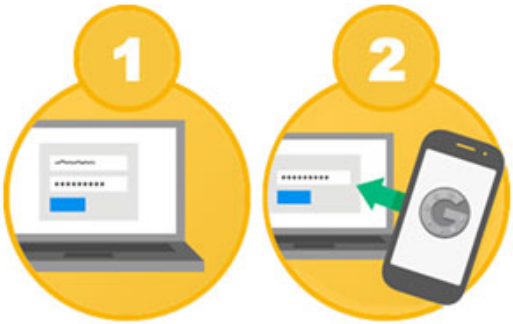


Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

Encryption can usually work in conjunction with DLP to provide holistic data security and policy enforcement. Once we've determined that ITAR data needs to legitimately leave the organization, and we confirm that it is going to the intended U.S person, we can enforce encryption of the data, so only the intended recipient can access and read the information.

Multi-Factor Authentication:

Something you know (password) and something you have (token, soft token, smart phone, etc.). At some point in the near future, all sensitive online accounts will require multi-factor authentication. From our online banking institutions to our ITAR applications at work; Multi-factor authentication makes it much harder for a hacker to access sensitive and top secret information. It's possible to steal credentials in the form of static and weak passwords but a random generated token for 2-factor authentication makes hacking just ones password useless. These token can now be received on phones, so we no longer need to carry physical tokens with us and risk losing them.



Two Factor Authentication

Identity & Access Management (IAM):

Identity is the 'Who' – who needs to have access to this information and from which authorized systems. In the IT world, we refer to this combination of people and systems as your digital identity. Now we know who you are and where you're accessing the information from.

Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

Access is the 'What' – what information do they need to access. It includes the individual's role, permissions and security restrictions come into play as well. The correct combination of *Identity* and *Access* Management can help a great deal with ITAR compliance.

We can ensure that only the authorized U.S individuals are accessing information that they need to have access to, from pre-authorized systems, and nothing more. IAM paired with multi-factor authentication can make it very difficult for a hacker to access ITAR governed information solely by compromising an employee's network password.

End User Security Awareness Training:

You are as secure as your weakest link. And that unfortunately is us – people, employees, end users, execs, managers, bosses – whatever our role may be in the organization. Invest in end user training, annually if you can, biennially if you have budgetary restrictions. Onsite, live, interactive training is usually the most beneficial. The trainee gets the opportunity to ask questions, delve deeper into a specific topic if needed, and it helps with overall attention span. Online trainings are also available for new employees, but not as an alternate to the live ones. A trained employee can help avoid a data breach which can cost millions. End user training can be effective towards proactive security versus reactive security which again is much more costly. Prevention is truly the best option here, and end user training is a huge step in that direction.

In conclusion, this is not a guide for 100% ITAR compliance. However, the goal is to build a security foundation to protect against ITAR violations and security breaches. The threat landscape changes every second and our goal is to provoke thought and to provide an easy to understand checklist to get us started. If some of the above foundational security elements are not in place, it would make it very difficult for us to prove that we did our due diligence to be ITAR compliant or to prevent a data breach from occurring.

Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com

About Aurora®

For over 20 years, security-conscious companies have turned to Aurora® Enterprises' professionals for support of their business critical applications. Our experienced team of security experts helps our clients to conquer the complex challenges of data security. Aurora's Services, Sales and Software teams combine to uniquely position the company as a single source, full service solutions provider to enterprises and government agencies.

Aurora® is a national *8(a) certified and Disadvantaged /Minority Business Enterprise (DBE/MBE)*, for information security software, hardware and consulting services. Aurora® provides enterprise-class security consulting services at a mid-market price. Our security assessment services are centered on Application Security, Network Security and Endpoint Security. From quick Vulnerability Assessments to deep dive Security Strategy Development, our security professionals include practical recommendations with a holistic approach to information privacy. Aurora® specializes in implementing solutions that cover Web Security, Email Security, Application Security and Data Encryption. We protect both the network as well as the Endpoint, providing our customers end-to-end security and easy management.

Aurora® currently holds 11 state contracts for IT products and services. Aurora® is a security cleared entity with a focus on helping our Federal Government in their cyber security initiatives. We are especially proud to have both Civilian and Department of Defense agencies as customers. All our current contracts and certifications can be viewed and downloaded at http://www.aurorait.com/government/

Email: Sales@Aurorait.com
Phone: (888) 282-0696
Website: www.Aurorait.com