# NCPROTECT™

# ITAR & EAR COMPLIANCE IN MICROSOFT 365® & SHAREPOINT®

## Executive Summary

International Traffic in Arms Regulations (ITAR), are issued by the United States government to control the export and import of defense-related articles and services on the United States Munitions List (USML). In short, the U.S. Government requires all manufacturers, exporters, and brokers of defense articles, defense services or related technical data to be ITAR compliant. The Export Administration Regulations (EAR) are issued by the United States Department of Commerce to control the export of items which are designed for a commercial purpose which could have military applications, such as computer hardware and software (Commerce Control List).

ITAR and EAR violations can pose a huge risk for impacted companies. Defense contractors have been fined tens of millions of dollars for failing to control access to EAR and ITAR regulated data. Furthermore, they can impact more than just the bottom line – criminal penalties of 10 to 20 years in prison, depending on the regulation, are also possible.

## KEY BENEFITS

- Supports Microsoft 365 apps and SharePoint on-premises
- Uses attribute-based access control (ABAC) to determine access, usage and sharing rights
- Adds multi-label classification capabilities to augment Microsoft Purview Information Protection
- Prevents the deletion of an ITAR document based on the published date or a shipment date for retention requirements.
- Tracks a document's full chain of custody and policy changes

## MEETING ITAR AND EAR COMPLIANCE IN MICROSOFT 365 AND SHAREPOINT

If your company needs to comply with ITAR or EAR regulations and you are using SharePoint Online in Microsoft 365 or GCC High, or SharePoint on-premises to grant access to product development plans, hardware specifications, source code, and other sensitive information, then you need to implement security controls in these applications to ensure compliance. The rules apply to any internal and external users or groups that have access to regulated content in the U.S. and in many other countries as defined in the requirements.

It is one of the most complex access management issues to solve. To be compliant, multiple factors must be considered before sharing regulated content including:

- User clearance level and caveats
- User citizenship
- Document/item clearance level (i.e. top secret, confidential, etc.)
- Device (i.e. browser or OS such as iPad, Android, tablet or other mobile device)
- Geography and access locations

Trying to define access using item permissions or roles would require the creation of thousands of security groups, and if using inheritance thousands of sites or libraries and folders. You also run the risk of exceeding the limit of allowed security scopes on a list. The complexity of these security schemes greatly expands the likelihood of multiple single point defects in individual user or document permissions – any of which constitute an export breach.

NC Protect provides a simple approach using dynamic access and identity management in M365 and SharePoint Server.

## NC PROTECT FOR ITAR AND EAR COMPLIANCE

The NC Protect approach to ITAR and EAR is simple.

NC Protect's zero trust methodology uses attribute-based access control (ABAC) to determine access, usage and sharing permissions at the item level — without the need to create additional groups and independent of item permissions. Organizations define policies and dynamically define groups, permissions and access based on user and file attributes including classification.

With NC Protect access controls and information protection are applied to individual files, chats and messages in real-time, so sensitive content can be safely stored, shared and collaborated in Microsoft 365 apps (SharePoint Online, Office and Exchange) and SharePoint Server—regardless of user membership, unlike solutions that secure or encrypt at the app or location level. This approach also controls the proliferation of sites to support individual collaboration scenarios.

# NC PROTECT CAPABILITIES FOR ITAR & EAR COMPLIANCE

NC Protect secures content in compliance with ITAR and EAR regulations without adding complexity in M365 and SharePoint Server with the following key capabilities:

- Uses simple, but powerful dynamic attribute-based access and sharing rules
- Utilizes standard metadata fields and/or Microsoft Purview Information Protection (MPIP) sensitivity labels
- Supports multi-label classification. Tag individual documents with more than one label to support complex taxonomies.
- Works with any user claim provider and any user property list or database.
- Compares multiple document metadata values against multiple user claims to deny access including:
  - Sensitivity Ranking (Top Secret, Secret, Classified, Confidential, etc.).
  - Restrict access based on the users' citizenship and Releasability classification of documents (US, AU, UK, etc.).
  - Restrict access to particular membership of a project, department or company.
  - Caveats can require that a user has all token values before providing access.
  - Access can change based on the age of the document.
- Documents not classified, compared to UNCLASSIFIED, can be restricted until classified.
- Users can only 'see' documents they are allowed access to, no matter where the document resides - even if all security levels have access to one folder/library.
- An agentless Secure Reader allows provides secure, read-only access to PDF files, Office documents (Word, Excel, PowerPoint & Visio), CAD files and OCR documents to prevent users from copying, modifying or redistributing controlled content.
- Adds a secure user-specific watermark that incorporates custom attributes such as the user's name, email, time and date of access, creating a digital thumbprint that travels with the document for security and auditing purposes.
- A user traveling outside the US can be denied access to classified documents or restricted to read only access and be prevented from downloading or emailing the document.
- Documents in draft can be edited by authorized collaborators, however, when published the edit rights can be automatically restricted or removed entirely without defining complex workflows or moving the document.
- NC Protect will prevent the deletion of an ITAR document based on the published date or a shipment date to help enforce ITAR document retention policies.
- Can apply FIPS 140-2 compliant encryption to protect information at rest or in motion.
- Tracks the entire chain of custody of sensitive documents including user access to documents and actions taken with them.

## LET'S GET THE CONVERSATION STARTED

Contact us to discuss your ITAR and EAR compliance needs.


## ADVANTAGES OF DYNAMIC, ATTRIBUTE BASED ACCESS AND CONTROL

**archTIS' granular data-centric approach to security enables conditional access control down to the item-level using both data and user attributes. Since access and information protection are applied to individual files and email messages, as compared with solutions that secure or encrypt at the app or location level, sensitive content can be safely stored, shared and collaborated in supported Microsoft apps, regardless of user membership. This approach also controls the proliferation of sites to support individual collaboration scenarios.**

archTIS

archTIS.com | info@archtis.com Australia | United States | United Kingdom