

The banner features a dark blue background with a glowing circuit-like pattern. On the right side, there are several overlapping rectangular panels with labels: 'PUBLIC', 'INTERNAL', 'SENSITIVE', and 'RESTRICTED'. The 'SENSITIVE' panel has a lock icon, and the 'RESTRICTED' panel has a crossed-out circle icon. The text 'NC PROTECT™' is at the top in a light blue and white font, 'CONNECTOR FOR ISEC7 CLASSIFY' is below it in white, and 'ISEC7' is at the bottom in a large white font with a small red square to its right.

NC PROTECT™

CONNECTOR FOR ISEC7 CLASSIFY

ISEC7

Executive Summary

archTIS has partnered with ISEC7, a global leader in data classification, to offer robust classification and dynamic data protection for joint Defense and industry customers looking to implement data-centric zero trust security to protect sensitive information.

ISEC7 CLASSIFY integrates seamlessly with Microsoft 365 apps and ISEC7 MAIL. Enterprises and organizations can cover all scenarios when working with classified information, regardless of device or location.

Joint customers can now use ISEC7's robust classification capabilities and pair them with NC Protect's dynamic access and data-centric protection policies to safeguard sensitive data.

Integration Benefits

- Classify data based on multiple dimensions of sensitivity and dissemination.
- Add ABAC-based policies to restrict access and protect data based on a file's classification.
- Use policies in combination with multiple classifications, including ISEC7, Spirion and Microsoft Purview Information Protection.
- Assists with U.S. and global regulatory compliance requirements for data classification and protection, data privacy regulations, and more.

FLEXIBLE CLASSIFICATION & DATA PROTECTION FOR MICROSOFT APPLICATIONS

The protection of sensitive data is critical for government and defense agencies and suppliers. IT and security teams are seeking ways to implement data-centric attribute-based access control (ABAC) capabilities that align with a modern zero trust approach, without compromising existing technology investments and classification processes.

The integration between NC Protect and ISEC7 CLASSIFY offers a seamless solution. Joint customers can enhance sensitive data labeling and dissemination capabilities with dynamic access and protection policies to meet government, defence and enterprise regulatory compliance needs.

The NC Protect ISEC7 CLASSIFY Connector provides organizations using ISEC7 CLASSIFY with the ability to:

- Control access to data based on the file's classification.
- Implement dynamic data protection policies to restrict the usage and sharing of sensitive files based on their classification.
- Add Controlled Unclassified Information (CUI) categories and limited dissemination controls to documents and files.
- Utilize a Bring Your Own Classification (BYOC) model to enhance existing data security and compliance processes.

TAKE CONTROL OF YOUR SENSITIVE DATA WITH NC PROTECT AND ISEC7 CLASSIFY

Combining the classifications embedded by ISEC7 CLASSIFY with NC Protect's ABAC capabilities delivers customers an outstanding solution to meet complex regulatory and security requirements for appropriately handling and disseminating sensitive unstructured data.

ISEC7 CLASSIFY's classification metadata can be used by NC Protect in combination with user and security attributes, to seamlessly apply dynamic ABAC policies to prevent unauthorized access to information on a per-file basis, as well as apply unique data protection capabilities. NC Protect adds additional security capabilities including dynamic watermarks, CUI markings, secure read-only access, and more based on the file's sensitivity and the user's context at the time of access.

The ISEC7 CLASSIFY integration is part of NC Protect's 'Bring Your Own Classification' model. It allows customers to use NC Protect's classification engine, leverage existing classifications, or a combination of the two, as part of the attributes used for enacting the product's dynamic ABAC policies. NC Protect's fine-grained ABAC policies evaluate attributes including document, user and environment values against defined policies to control who can access information and under what conditions. Supports DOD365-SEC and Microsoft 365 apps, including SharePoint Online, Microsoft Teams and Office 365.

EASILY CONNECT AND USE ISEC7 CLASSIFICATIONS IN NC PROTECT'S DYNAMIC ACCESS AND PROTECTION POLICIES

NC Protect can use ISEC7 classifications as one of the many data attribute types used when building and applying its dynamic access and protection policies.

Edit Condition

Change the attribute and value of the condition

Type
attribute

Attribute Condition
Allows for evaluation of attributes against static values.

Attribute
data Classification (string)

Operator
in

Values
//NATO RESTRICTED
CONFIDENTIAL//NOFORN

Cancel Save

	Modified By	Modified	Created	Classification
Playground.docx	Terence Johnson-A	February 19, 2026	February 19, 2026	
(C) CLASSIFY Playground.docx	Terence Johnson-A	February 19, 2026	February 19, 2026	CONFIDENTIAL//NOFORN
(U) CLASSIFY Playground.docx	Terence Johnson-A	February 19, 2026	February 19, 2026	UNCLASSIFIED

NC Protect can use ISEC7 classifications to control access and apply file protection in the Secure Document Library.

SUPPORTS THESE M365 APPLICATIONS



SharePoint Online



Microsoft Teams



Office 365



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

