

# NC PROTECT™

## ADVANCED INFORMATION PROTECTION FOR MICROSOFT TEAMS®

### Executive Summary

Ensure your organization's business-critical data is used and shared in accordance with your business regulations and policies.

NC Protect enables secure collaboration of sensitive information in Microsoft Teams. It provides conditional access control without the overhead of complex user permissions, poorly applied at-rest encryption, or the need to create multiple channels to limit access to files. It ensures your information is protected in real time across all collaboration scenarios.

### Key Benefits

Enable secure file sharing in Teams channels with a Secure Document Library that enables you to:

- Automatically adjusts access and protection based on file and user attributes
- Hide sensitive content from unauthorized users
- Automatically encrypt data when the scenario requires it
- Supports a broad range of file types, including Office files, PDF, CAD, images, and more

### GREAT FOR COLLABORATION, PROBLEMATIC FOR DATA SECURITY

The ability to quickly share information through built-in chat and file-sharing features has made Microsoft Teams a crucial collaboration tool for organizations. However, the speed and ease of creating new teams pose challenges for IT and security departments, which must ensure that business-critical information is adequately protected. User-managed tools like Teams complicate efforts to control data access and maintain compliance with business sharing and usage policies. Whether through over-permissioned channels or unintentional file sharing, sensitive information can easily be exposed in Teams.

### DYNAMICALLY SECURE FILE SHARING IN MICROSOFT TEAMS

NC Protect enables you to dynamically secure file sharing in Teams Channels in accordance with your access and sharing policies. NC Protect's Secure Document Library augments the file-sharing tab in a Teams channel, enabling secure, policy-enforced access control and data protection. Dynamically adjust access to and protection of files shared in Teams and control what users can see, how they can share information, and with whom.

### Fine-grained Access Control and Data Protection

NC Protect enhances security by not only controlling access to sensitive data but also applying data-centric protections, such as read-only access, user-specific watermarks, and dynamic encryption. It can even hide files from unauthorized users.

### Attribute-based Flexibility & Precision

Attribute-based access control (ABAC) policies utilize both data and user attributes from Microsoft Purview, Entra ID, SharePoint properties, and other sources to determine access rights and apply file protection in real time. With NC Protect's fine-grained access controls, a user who shouldn't have access to a file will be blocked from accessing it, regardless of Team membership.

### Centrally Manage Policies Across M365

Centrally manage access and protection policies across Teams and SharePoint Online using the same rule sets to reduce admin overhead and resources needed to manage sites and applications.

### Implement with Confidence

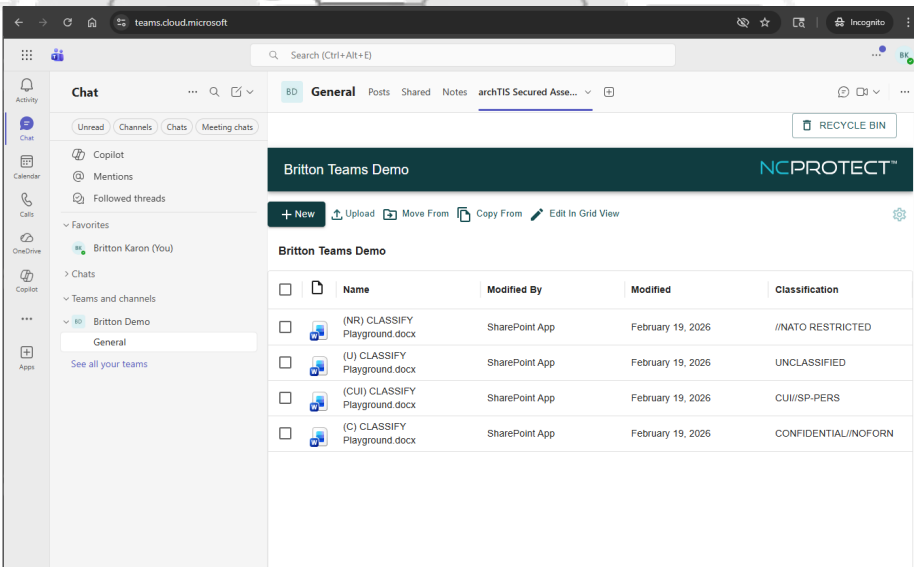
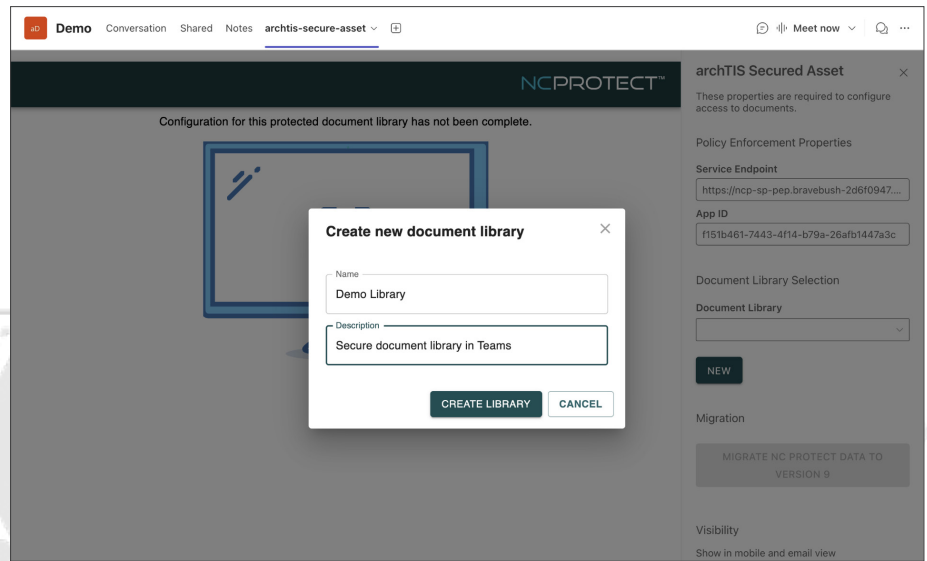
NC Protect requires no additional client-side application, reducing IT overhead and the risks associated with implementing new cloud services or BYOD policies. NC Protect's seamless integration with the Microsoft suite is vetted by the Microsoft Intelligent Security Association.



# SECURE FILE SHARING IN MICROSOFT TEAMS

Create a Secure Document Library and apply access control and protection policies right from a Teams Channel with just a few clicks.

Easily add a Secure Document Library right from an existing Teams channel using the Add a Tab function.



Once your library is created and policies are applied, you're ready to start securely sharing files.

SEE HOW WE ENHANCE AND SIMPLIFY FILE SHARING IN MICROSOFT TEAMS.

Contact Us



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



Member of  
Microsoft Intelligent  
Security Association

