State of North Carolina
Copilot for Microsoft 365 Policy

Statewide IT Policy

Version 1.0

December 5, 2024

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
Dec 5, 2024	1.0	New	Policy Published	Chris Brittingham

Document Details

Department Name	NCDIT Enterprise Collaboration Services
Owner	NCDIT Enterprise Collaboration Services
Title	Copilot for Microsoft 365 Policy
Publication Date	December 5, 2024
Next Release	June 5, 2025
Document Type	PDF
Document Number	1.0
Version	1

Table of Contents

Purpose

The purpose of this policy is to establish requirements for the activation, use, monitoring, and review of Copilot for Microsoft 365 within state agencies. This policy aims to ensure that the deployment and utilization of Copilot for Microsoft 365 aligns with state regulations, enhances productivity, and maintains data governance and compliance.

Content Lead

N.C. Department of Information Technology - Enterprise Collaboration Services

Scope

The requirements summarized in this policy apply to agency leadership, agency security liaisons, and agency privacy points of contact. and selected users within state agencies who utilize Copilot for Microsoft 365 within the state of NC.

Policy Requirements

Requirements to Activate and Renew Copilot for Microsoft 365

- Agency CIOs must receive all necessary internal approvals prior to implementation of Copilot for Microsoft 365 (e.g., General Counsel, Finance, Operations, etc).
- Agencies must complete a pilot of Copilot for Microsoft 365 with select users to train and understand Copilot for Microsoft 365 use.
    - Selected users must complete Copilot for Microsoft 365 training prior to the pilot.
    - Once the pilot has been completed, agency will move to a limited deployment of Copilot for Microsoft 365.
- Agencies must procure the necessary Copilot for Microsoft 365 license through the purchase requisition process.
    - Agency CIOs are required to request licenses for Copilot for Microsoft 365 users within their agency.
- Agencies must coordinate with security liaisons and privacy points of contact to ensure that the deployment meets all state and agency security, privacy, and AI standards.
- Prior to initial Copilot for Microsoft 365 deployment, agencies are required to complete a Privacy Threshold Analysis (PTA) documenting their proposed use of Copilot for Microsoft 365.
    - A master Privacy Impact Assessment (PIA) for Copilot for Microsoft 365 will be maintained by NCDIT.
        - i. Agency PTAs will be appended to the master PIA to document Copilot for Microsoft 365 use.
    - PTAs must be renewed annually or whenever there is a substantial change in the environment or change of data use.
    - When completing a PTA, the project manager must be transparent and identify their intended use(s).
        - i. An updated PTA is required to document any changes of use or data.
        - ii. Updated PTAs must be submitted and reviewed by OPDP & ESRMO before activation or continued use.
- NCDIT can offer an adoption framework for agencies to follow, if requested.

Microsoft 365 Tenant Requirements for Copilot for Microsoft 365 Use

The Microsoft 365 Tenant Services Team is required to perform the following tasks when using Copilot for Microsoft 365. For agencies within the NCDIT Microsoft 365 tenant, these actions are performed by NCDIT.

- Tenant must designate Copilot for Microsoft 365 agency administrators to enable Copilot for Microsoft 365 for agencies within the tenant.

Agency Requirements for Copilot for Microsoft 365 Use

Agency is required to perform the following actions when using Copilot for Microsoft 365.

- Agency must assess and manage access, permissions, and roles for any user with a Copilot for Microsoft 365 license to control who can access specific data and services within the Microsoft 365 suite to prevent oversharing sensitive information. Data access should be limited to *need to know.*
- Agency must adhere to state and industry-specific policies, standards, regulations, and frameworks and configure Microsoft 365 to meet security, privacy, and AI compliance requirements and all relevant agency specific policies (e.g., North Carolina State Government Responsible Use of Artificial Intelligence Framework; Fair Information Practice Principles, Statewide Information Security Policies, Statewide Data Classification and Handling Policy).

User Requirements

- Users must adhere to all state IT policies, standards, and frameworks and relevant agency specific policies (e.g. the North Carolina State Government Responsible Use of Artificial Intelligence Framework; Fair Information Practice Principles; Statewide Information Security Policies, Statewide Data Classification and Handling Policy).
- Users must promptly report any privacy or security concerns, misuse of Copilot for Microsoft 365, or accidental data exposure to their agency security liaisons.
- Limit use of personal or confidential information to what is necessary to complete agency tasks.
- Users who discover they or others have access to personal information or confidential files that they do not have a *need to know* must report this to security liaisons and administrators for access controls review and update.
- Users are responsible for the content generated by Copilot for Microsoft 365.
- Users must complete any state or agency required Copilot for Microsoft 365 training.
  - NCDIT and the agency have the authority to mandate Copilot for Microsoft 365 specific training.

Regulations and Applicable Laws

The following reference sections in the N.C. General Statutes provide additional information with respect to compliance with state law:

- N.C.G.S.143B-1320(a)(17) – Definitions; scope; exemptions

- N.C.G.S. 143B-1321 – Powers and Duties of the Department

- N.C.G.S. 143B-1322 – State CIO Duties

- N.C.G.S. 143B-1325 – State information technology consolidated under the Department of Information Technology

- N.C.G.S. 143B-1350(a) – Procurement of information technology

- N.C.G.S. 143B-1370(a) – Communications services

- 09 NCAC 06b.0701 – Contracts Established by DIT

Enforcement

Violations of this policy, or failure to implement provisions of this policy, may result in revocation of agency or user Copilot for Microsoft 365 license(s) by the state CIO.

Policy Review Cycle

The Copilot for Microsoft 365 Policy will undergo a periodic review at semi-annual intervals, or as changes are required. Updates to the policy will be determined based upon the nature of the policy and requirements driven by need.

Any identified changes, or outdated information within the policy will be addressed promptly. This may involve revisions, additions, or removals as needed to ensure that policies remain current and relevant.

The following roles provide leadership and management over this policy in accordance with the NCDIT Policy Management Policy:

• Secretary of the N.C. Department of Information Technology and State Chief Information Officer has approval authority.

• Chief Deputy State Chief Information Officer (or delegate) has policy management responsibilities.