State of North Carolina

Microsoft 365 - Agency Requirements for Email and Collaboration Services Policy

N.C. Department of Information Technology

Version 1.0

January 24, 2024

Document Information

Revision History

Date	Version	New or Revised Policy	Description	Author
January 24, 2024	1.0	New	Policy Published	Srinivas Sunkara

Document Details

Department Name	NCDIT Internal Operations – Enterprise Operations – Microsoft 365 Services
Subject Matter Expert	Srinivas Sunkara (NCDIT Microsoft 365 Service Director); Karen Mann
Title	Microsoft 365 - Agency Requirements for Email and Collaboration Service Policy
Publication Date	January 24, 2024
Document Type	PDF
Document Number	
Version	1.0

Table of Contents

Purpose

This policy summarizes the State requirements for Microsoft 365 email and collaboration services in an independently managed tenant. The below items represent the requirements that any executive branch agency within the State of North Carolina must perform.

For those agencies that reside within the NCDIT shared Microsoft 365 email and collaboration tenant, these requirements are managed by the NCDIT Microsoft 365 tenant services.

Content Lead

North Carolina Department of Information Technology (NCDIT) – Microsoft 365 Subject Matter Experts

Scope

The requirements summarized in this policy apply to agencies supported by NCDIT inside of the State of NC shared Microsoft 365 tenant, as well as those agencies who are separated into a dedicated and independently managed Microsoft 365 tenant.

Requirements

Compliance and Records Management

Agency is required to maintain the following, at a minimum:

- Agency is required to name a compliance lead for their tenant.
- Agency is required to own appropriate licensing to meet statewide security, compliance, and data privacy requirements.
- Agency must perform annual Compliance Optimization* with Microsoft in conjunction with their annual Security Assessment and share the results with State CIO and ESRMO.
- Agency must define and enforce an internal Data Loss Prevention (DLP) policy. At a minimum, the DLP policy must include the following:
    - Configuration settings to be shared with agency security liaison.
    - Scanning controls to monitor and alert when medium or high-risk data, as defined by the Data Classification and Handling Policy, is shared externally (SSNs, credit card #s, PII, etc).
    - A process to document and share security violations with the agency security liaison and ESRMO, when requested.
- Agency must enforce an eDiscovery agency policy with restricted access to authorized staff to perform eDiscovery searches for litigation, personnel, or other searches.
- Agency must align data retention requirements with statewide records retention schedule defined and managed by Dept. Of Natural and Cultural Resources (DNCR).

Agency is recommended to maintain the following:

- Agency should adopt the Statewide Data Classification and Handling Policy* or document agency specific data classification policy and enforce applicable controls.
- Agency should enforce email retention controls as defined by E-Mail Retention and Archiving Policy*.
- Agency should implement airgap and immutable data protection as a backup and recovery solution for all email accounts.

**See References*

Cybersecurity

Agency is required to maintain the following, at a minimum:

- Agency is required to name a compliance lead for their tenant.
- Agency must utilize a tenant that is in the Government Community Cloud (GCC) which is FedRAMP certified.
- Agency must perform annual Security Optimization Assessment (SOA)* engagement and annual Purview Compliance Assessments* from Microsoft and provide results to State CIO and ESRMO.
- Agency must maintain email and Microsoft 365 service security controls (i.e. Proofpoint, Cisco Email Security, Microsoft Defender).
- Agency must maintain a Cloud Access Security Broker (CASB) solution to provide monitoring and alerting.
- Agency must maintain an email phishing best practices training and testing program.
- Agency must require Multi-Factor Authentication (MFA) for administrator and user accounts.
- Agency must establish privileged identity management (PIM) for Microsoft 365 IT administrators to provide "just-in-time" administrative access.
- Agency must be prepared to send logging of incident and security event correlation and analysis to ESRMO, upon request.

Agency is recommended to maintain the following:

- Agency should enforce restricted administrative access controls to allow for admin access from managed devices only.
- Agency should maintain Government domain security protections using DMARC, DKIM and SPF.
    - DMARC should be set to a "reject only" posture.
- Agency tenant should comply with all applicable security controls identified in NIST 800-171.

**See References*

Microsoft 365 Services

Agency is required to name a compliance lead for their tenant and document agency specific governance for all Microsoft 365 Services. Services include, but are not limited to:

- Exchange Email
- Defender
- Purview
- SharePoint & OneDrive
    - External & Internal Sharing
- Teams
- Endpoint Mgmt. (if applicable)
- Power Platform/Dynamics (if applicable)
- Power BI

Agency must submit all Third-Party Apps to ESRMO for review and approval.
Agency must track SharePoint sites that will be set for external access.
Agency must track and have approval for allowing sensitive forms of PII on SharePoint sites.

- Approval requires an approved PTA from ESRMO

If applicable, agency must create and update Power Platform Enterprise Data Gateways for PowerBI.

- If an agency is publishing state data externally, the agency must utilize a data gateway to ensure access and security management.

Agency is recommended to maintain the following:

- Agency should allow External and Guest to communicate with other agencies.
- OneDrive for Business controls should be configured so that external access is not allowed.

Regulations and Applicable Laws

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

- N.C.G.S.143B-1320(a)(17)
- N.C.G.S. 143B-1321
- N.C.G.S. 143B-1322
- N.C.G.S. 143B-1325
- N.C.G.S. 143B-1350 (a)
- N.C.G.S. 143B-1370 (a)
- 09 NCAC 06b.0701

Policy Review Cycle

The Microsoft 365 - Agency Requirements for Email and Collaboration Service Policy will undergo a periodic review at bi-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.

Definitions and Acronyms

Cloud Access Security Broker

A Cloud Access Security Broker (CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.

DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email authentication protocol that is designed to give email domain owners the ability to protect their domain from unauthorized use.

DKIM

DomainKeys Identified Mail (DKIM) is an authentication method designed to detect forged sender addresses in email.

SPF

Sender Policy Framework (SPF) is an email authentication method which ensures the sending mail server is authorized to originate mail from the email sender's domain.

Acknowledgment of Policy

Written acknowledgment of this policy must be provided by an Agency Head or Delegate.

I have read, understand, and will abide by the above Microsoft 365 - Agency Requirements for Email and Collaboration Services Policy and the specific terms of this policy. I further understand that governance of these requirements will be managed by agency leads in my tenant. I understand that failure to execute or enforce any terms of this policy may result in revocation of the ability to operate in an independently managed tenant.

Name

Date

Signature of Agency Head or Delegate

References

Statewide Data Classification and Handling Policy

E-Mail Retention and Archiving Policy

Office 365 Security Optimization Assessment

Microsoft Compliance Optimization Manager