NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Third-Party Cloud Service Risk Authorization & Management

Statewide Information Security Manual Supplement

Version 1.0

February 2026

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
Feb. 25, 2026	1.0	New	Policy Creation	

Table of Contents

Introduction

The State of North Carolina is committed to protecting the confidentiality, integrity, and availability of information assets through a comprehensive risk authorization and management program. Cloud Service Provider (CSP) continuous monitoring practices are integral to this program, enabling ongoing assessment and mitigation of potential risks throughout the system lifecycle. The State of North Carolina will utilize the GovRAMP security framework to ensure that all third-party cloud services adhere to stringent security standards and are authorized for use.

Scope

This policy supplement applies to third-party external cloud services utilized by the State of North Carolina. This document is not applicable to the following use cases:

- On-premises systems and solutions

Purpose

This supplement establishes a standardized process and requirements for authorizing and managing risks associated with the selection of CSPs and the ongoing use of cloud services.

Determination of Information Sensitivity

When considering the acquisition of a cloud service, State Agencies shall determine the appropriate data classification level (high water mark) consistent with the *Statewide Data Classification & Handling Policy*. State data is classified into four categories (Public, Internal, Confidential, and Restricted) based on the potential impact of unauthorized access, loss, theft, or corruption of data systems to the State, an agency, or a constituent.

Based on the data classification level, State Agencies will select the appropriate GovRAMP status required for the procurement. The Agency Security Liaison or delegate is responsible for verifying that the chosen GovRAMP status aligns with the information processed in the cloud service as described in the sections below. For cloud services procured through the Statewide Information Technology Procurement (SITP) process, the North Carolina Department of Information Technology (NCDIT) will validate the appropriate GovRAMP status and approve the service for use. For cloud services procured outside of this process, State Agency Security Liaison validation and approval is sufficient.

Public Data (Formerly Low Risk)

Public data includes data that is open to public inspection according to state and federal law, state policy, or readily available through public sources (e.g., information on publicly accessible websites, work email addresses, etc.).

For third-party cloud services where the highest category of information to be processed is public data, State Agencies are responsible for validating the applicable GovRAMP Security Snapshot Score (GSSS) prior to contract award. Then, for the duration of the contract term, State Agencies must review an updated GSSS annually to validate that the CSP is meeting or exceeding their original contracted score. For cloud services procured through the SITP process, NCDIT will also participate in the annual review and validation.

Internal Data (Formerly Part of Medium Risk)

Internal data is information that most State Agency employees would have access to, but that is not meant to be shared with the public (e.g., draft documents that have not yet been published, employee work schedules and duty assignments, internal newsletters, training materials, etc.).

For third-party cloud services where the highest category of information to be processed is Internal data, State Agencies must validate that the CSP has either achieved the status of GovRAMP Core prior to award, or that the CSP has agreed to achieve GovRAMP Core status within an interim time period, no later than twelve (12) months from the effective date of the contract. For cloud services procured through the SITP process, NCDIT will also participate in review and validation.

If the CSP does not hold GovRAMP Core status prior to contract award and chooses to utilize the interim time period, please refer to the *Interim GovRAMP Monitoring Requirements* section below for additional information.

Confidential Data (Formerly Part of Medium Risk)

Confidential data includes information that is limited to a small audience with a need-to-know or legitimate business case (e.g., State employee personnel records, trade secrets, student records, sensitive public security information, etc.). If exposed to unauthorized parties, data from this category will cause high impact consequences such as regulatory fines, inability to recruit talent, loss of confidence, and/or damage to vendor relationships.

For third-party cloud services where the highest category of information to be processed is Confidential data, State Agencies must validate that the CSP has either achieved a status of GovRAMP Ready, or has agreed to achieve GovRAMP Ready status no later than fifteen (15) months from the effective date of the contract. For cloud services procured through the SITP process, NCDIT will also participate in review and validation.

If the CSP does not hold GovRAMP Ready status prior to contract award and chooses to utilize the interim time period of 15 months, please refer to the *Interim GovRAMP Monitoring Requirements* section below for additional information.

Restricted Data (Formerly High Risk)

Restricted data represents the highest risk to the State, State Agencies, and constituents if it is disclosed or compromised. This information is likely to be regulated by State or Federal law, and access to it is restricted to a limited audience (e.g., State and Federal Tax Information [FTI], Payment Card data, Protected Health Information [PHI], Criminal Justice Information [CJI], Social Security Administration-provided information, etc.)

For third-party cloud services where the highest category of information to be processed is Restricted Data, State Agencies must validate that the CSP has either achieved a status of GovRAMP Authorized, or has agreed to achieve GovRAMP Authorized status no later than twenty-one (21) months from the effective date of the contract. For cloud services procured through the SITP process, NCDIT will also participate in review and validation.

If the CSP does not hold GovRAMP Authorized status prior to contract award and chooses to utilize the interim time period of twenty-one (21) months, please refer to the *Interim GovRAMP Monitoring Requirements* section below for additional information.

Change in Information Sensitivity

Once a cloud services contract is awarded, it is the responsibility of the State Agency to ensure that the sensitivity of information placed in the cloud service does not rise above the approved level.

If the State Agency identifies a business need to place a higher level of information into a cloud service than what was originally approved, it is the State Agency's responsibility to ensure that the CSP can meet the new standard of protection detailed above (to include contract modification) prior to any transfer, storage, or processing of the higher level of information by the cloud service.

Interim GovRAMP Monitoring Requirements

If a chosen CSP does not hold the required GovRAMP status prior to contract award, the CSP has the option to achieve that status within a set interim time period. For these use cases, there are additional monitoring requirements to ensure State data is appropriately protected. For cloud services procured through the SITP process, NCDIT will also participate in all review and validation actions described within this section.

- Prior to contract award, State Agencies are responsible for reviewing the applicable GSSS.
- Once the contract is awarded, State Agencies must confirm enrollment in the GovRAMP Progressing Snapshot Program (PSP) PRIOR to any non-Public State data being transferred to, stored in, or processed by the cloud service.
- For cloud services processing Confidential and/or Restricted information, State Agencies are responsible for validating Progressing Snapshots quarterly in accordance with existing data handling requirements.

If the CSP is not able to obtain the required authorization within the given interim time period, extensions may be granted at the discretion of the purchasing State Agency, provided that the Security Liaison has reviewed the most recent Progressing Snapshot and has validated that the appropriate mitigations are in place to protect State data. Extensions may not exceed six (6) months.

In the event that the CSP is in the authorization queue for the appropriate GovRAMP status but has not yet been formally authorized, State Agencies may accept a letter from the GovRAMP Project Management Office (PMO) indicating that the product is currently in the process of being reviewed for a verified status of Core, Ready, Authorized, or Provisionally Authorized.

Federal Risk and Authorization Management Program (FedRAMP) Authorization

If the cloud service holds a FedRAMP Rev. 5 authorization at time of award, this authorization can be accepted in lieu of a GovRAMP authorization. Authorizations obtained via the FedRAMP 20x Pilot Program will not be permitted. State Agencies are responsible for validating at least annually via the FedRAMP Marketplace or equivalent attestation that the cloud service's FedRAMP authorization is in good standing. For cloud services procured through the SITP process, NCDIT will also participate in review and validation.

State Agencies may identify a business need to require a cloud service to enroll in the GovRAMP Fast Track program. When this is required, State Agencies are responsible for validating that the CSP has enrolled in the GovRAMP Fast Track program to achieve a status of GovRAMP Authorized or Provisionally Authorized.

Non-Cloud Professional Services Processing State Data in the Cloud

State Agencies may require services from vendors who are not CSPs, but who will process, transmit, or store State data within a cloud service to enable the fulfillment of their professional services. Prior to contract award, State Agencies are responsible for validating that the protection requirements listed above are met or exceeded for cloud services processing sensitive State data. This may include confirmation of the cloud service's GovRAMP or FedRAMP authorization.

GovRAMP Continuous Monitoring

NCDIT and designated State agency staff shall utilize GovRAMP's Continuous Monitoring portal to review the monthly, quarterly, and/or annual reports for cloud service products. Continuous Monitoring for GovRAMP Core, Ready, Provisionally Authorized, and Authorized can be requested for either Standard Access or Elevated Access and requests for access should be approved by the vendor within fourteen (14) days of contract award, and seven (7) days of any subsequent status changes.

- Standard Continuous Monitoring Access: For cloud services with a Low or Moderate security category, service providers will upload packages to the GovRAMP Box Portal. Documents include:

    a. POA&Ms (Plan of Action and Milestones)
    b. An updated inventory workbook
    c. OS, DB, and web application vulnerability scans
    d. Deviation Request Form to support POA&M Risk Adjustments, Operational Requirements, and False Positives
    e. Executive summary of the above items

- Elevated Continuous Monitoring Access: Includes all documentation included in Standard Access and access to a product's System Security Plan (SSP), Security Assessment Plan (SAP), and/or Security Assessment Report (SAR).

Additional Resources

- GovRAMP Website
- GovRAMP Baseline Controls Matrix and Guidance
- GovRAMP Authorized Product List
- GovRAMP Fast Track Program
- FedRAMP Authorized Product List (Marketplace)