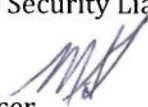


January 4, 2017

MEMORANDUM

TO: State CIOs and State Security Liaisons

FROM: Maria S. Thompson 
State Chief Risk Officer

SUBJECT: Secure Cloud Storage, File Sharing and Collaboration

A. OVERVIEW:

Cloud services and related storage solutions have become ubiquitous across the IT industry and on the surface offer the promise of low-cost methods for storing and processing data. However, the effective and secure deployment of this technology depends on careful application of appropriate security controls, well-established governance and management visibility. Absent such controls cloud services can result in increased risk of unauthorized disclosure. **This memo asks each State agency to provide an inventory of current cloud solutions and where appropriate, a plan to migrate cloud data to a more secure and supported platform as described in paragraph 2 below.**

B. BACKGROUND:

N.C.G.S. 143B-1376 requires that the State CIO ensure compliance of all State data stored in non-State facilities. Data stored in these facilities must receive approval from the State CIO prior to the data being stored offsite. Additionally, these solutions must be in compliance with the Statewide Information Security Manual, and meet the requisite protection and privacy requirements based on the classification of the data.

The State Continuous Monitoring Plan, in support of N.C.G.S. 143B-1376 requires that all cloud vendors annually report and document their compliance posture. These vendors include those providing Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). The State recognizes the following independent assessment reports as suitable mechanisms to support this requirement: Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, SSAE 16 or ISO 27001.

C. POLICY:

1. All State agencies MUST ensure that State data is stored on approved onsite or offsite solutions that meet the intent of the above policies and State law. Personal cloud storage, file sharing and collaboration solutions such as Dropbox, iCloud, Google Drive, IDrive, OpenDrive, Adobe and others are strictly prohibited for cloud storage or internal/external file sharing due to concerns regarding security and data sovereignty.

Use of these services does not provide the State with the ability to audit the security controls in place and therefore significantly increases the risk of a data breach that could result in the following:

- Loss of competitive advantage;
- Loss of business relationships;
- Unauthorized disclosure of personal information;
- Reputational damage.

Agencies who have procured these solutions using State funds must begin the process of migrating State data to a State approved solution **no later than 01 March 2017**. Agencies must develop a migration plan and submit it to the Department of Information Technology (DIT) prior to this due date. The plan should include the following requirements:

- Data type and classification
- Type/Name of solution
- Contract number and expiration date
- Cost of the Contract
- Anticipated migration date (when all data will be moved from Cloud to State approved service)
- Date of data sanitization. Vendor must provide support for the residual data stored in the environment

2. **State Approved Solutions.** The State has purchased Microsoft OneDrive for Business and SharePoint to support secure file sharing and collaboration. Additionally, Citrix ShareFile is available for purchase on State contract for those agencies requiring additional security features to meet requirements such as Payment Card Industry – Data Security Standards (PCI-DSS).

OneDrive for Business and SharePoint inherently provide a level of security for data at rest and data in transit as provisioned within the Microsoft Government Cloud. Agencies are cautioned, however, to refrain from using these solutions for processing, storing or sharing of data classified as “Restricted or Highly Restricted” as defined in the *Statewide Data Classification and Handling Policy*. These actions are strictly prohibited due to the current lack of technical measures in place to prevent unauthorized or inadvertent disclosure of sensitive data.

3. A migration plan template is being provided for your use and your Agency Business Relationship Managers (BRMs) is available to assist you in this effort. All migration plan submissions must be sent to the BRM email address at brm@lists.nc.gov. Once received, DIT will facilitate the deployment of solutions to meet your storage requirements.

DIT is developing processes to enforce the use of Data Leak Prevention (DLP) technologies in order to curtail unsanctioned actions within OneDrive and other Microsoft suite of tools. Other preventative measures such as the use of Rights Management and Mobile Device Management is recommended, in order to further reduce the risk of inadvertent disclosures. Once technical measures have been implemented, the Enterprise Security and Risk Management Office (ESRMO) will reassess the risk to the enterprise and provide update to this policy.

The point of contact (POC) for this correspondence is the State Chief Risk Officer, Maria Thompson, maria.s.thompson@nc.gov (919) 754-6578.