STATE OF NORTH CAROLINA
DEPARTMENT OF INFORMATION TECHNOLOGY

ROY COOPER
GOVERNOR

J. ERIC BOYETTE
SECRETARY & STATE CHIEF INFORMATION OFFICER

Memorandum

To: All Agency CIOs and Security Liaisons

From: Maria S. Thompson, State Chief Risk Officer
NC Department of Information Technology

SUBJECT: Secure Cloud Storage, File Sharing and Collaboration – Phase II

Date: February 15, 2018

A. 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 comply with the Statewide Information Security Manual and meet 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, or ISO 27001.

B. POLICY

In January 2017, this office provided guidance on the use of secure cloud storage, file sharing and collaboration solutions. In that memo agencies were asked to provide feedback on all such applications in use with the intent to migrate the business needs to state approved platforms. Many of the less used providers were blocked at that time with the more common cloud solutions left open for use by state agencies

This process was identified as a multi-phased project to allow agencies sufficient time to migrate their data to approved solutions. Phase I was completed during FY 2017. The next stage of this project is now being implemented to bring the remaining cloud storage solutions under a more secure operating model. Phase II will be put into effect **April 1st, 2018**.

P O Box 17209, Raleigh, NC 27619-7209
4101 Mail Service Center, Raleigh, NC 27699-4101
Telephone: 919-754-6100

These remaining solutions are listed below. However, this list is not exhaustive of all cloud solutions. As more cloud services are identified by our monitoring systems, they will be added to the block list under Phase II:

- CLOANTO
- CloudApp
- CloudFront
- Commvault
- Coupa
- Datei.to
- deviantART
- DivShare
- dl.free.fr
- DropBox
- Elephant Drive
- NovaBACKUP
- Google Drive
- Box
- Fluxiom
- 1fichier
- 4shared
- Fileguri
- ADrive
- Amazon Cloud Drive
- Bitbucket
- ARCServe
- Backupgrid
- Backblaze
- ZipCloud
- HiveStor
- iBackup
- iCloud
- Mega
- JustCloud
- BlazeFS
- Boxnet Upload SSL
- Brothersoft
- Carbonite
- Megaupload

PROCESS

DIT intends to block access to these solutions as a general risk mitigation strategy. However, we also recognize that some agencies have programmatic or other legitimate business needs – such as working with federal partners - that require the use of some of these cloud solutions. For those needs, we will provide a technical exception for a given application and set of users. As part of their request, agencies must provide sufficient justification for use as well as detail the classification of data being stored, uploaded and shared in these solutions. The exception must detail the following:

- Business justification
- Data classification – Complete a Privacy Threshold Analysis (PTA)
- Number of users
- eDiscovery support
- Data sanitization process/plan
- Encryption capability for data in transit and at rest
- If restricted/highly restricted data is involved, account management procedures
- Validation/approval from Agency security liaison

If the exception request is approved, submitter needs to submit a Remedy Ticket referencing the exception and containing the following:

- Internet Protocol (IP) for users to be exempt – Remedy ticket must be submitted to DIT Network Operations. Note: The use of static IPs to further isolate these users is highly recommended.

Agencies that have previously submitted an exception for any of the services listed above do not need to take any action. As a note, free or public domain versions of these tools are not authorized for use with State data. These solutions typically have reduced security capabilities and do not support eDiscovery requirements or effective data sanitization at the end of business need.

For those agencies needing an exception to this policy, please communicate the need to your BRM using the attached template.

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