STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

STANDARD 560S1: Data Loss Prevention for Cloud Services

VERSION NUMBER	Standard 560S1-01
VERSION DATE	August 10, 2018
STANDARD TITLE	Data Loss Prevention for Cloud Services
GOVERNING POLICY	This standard is governed by Policy 560: Cloud Storage Services, regardless of revision.

OBJECTIVE

The objective of this standard is to state the minimum requirements for the conditions and actions of monitoring the disclosure of sensitive information outside of the user's organization by applying data loss prevention (DLP) features and strategies in a cloud storage environment.

REQUIREMENTS

Many of the features that make cloud storage services attractive can also be at odds with traditional security models and controls. The DLP technologies and strategies help close the gap between the cloud storage services and traditional security models and controls. Data loss prevention uses rules to classify and protect confidential and sensitive information from accidental or malicious sharing of information outside of the user's cloud storage organization while it is in use (endpoint actions), in motion (network traffic), or at rest (stored data).

1. **Minimum required conditions for DLP monitoring of information in a cloud storage service:**

   1.1. U.S. Personally Identifiable Information (PII):

   1.1.1. U.S. Individual Taxpayer Identification Number (ITIN)

   1.1.2. U.S. Social Security Number (SSN)

   1.1.3. U.S. Passport Number

   1.1.4. Driver's License Number

   1.1.5. Full name and date of birth

1.2. U.S. Health Information:

1.2.1. Health Insurance Claim Number (HICN)

1.2.2. PII identifiers (SSN or DEA Number) and medical terms (ICD-9-CM keyword or ICD-10-CM keyword)

1.3. U.S. Financial Information:

1.3.1. Credit card number

1.3.2. U.S. bank account number

2. **Minimum required actions for DLP monitoring of information in a cloud storage service:**

2.1. Notification to the user to help educate them of the proper disclosure of sensitive information, i.e. policy tip

2.2. Incident report sent to the agency IT division that manages and administers the cloud storage service

2.3. If sharing through email, forced secure email encryption

SUPPORTING DOCUMENTS

The following documents support this standard:

- Policy 560: Cloud Storage Services

EFFECTIVE DATE

This standard is effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

Agencies must be compliant with this standard within six months of the effective date indicated below.

SUPERSEDES

This is the initial standard and does not supersede a previous version.

The undersigned, as Acting Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this standard to be adopted as of the 28 day of August, 2018.

Jim Purcell
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
560S1-01	08/10/2018	Initial version