STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

STANDARD 560S2: System Security Standards for Office 365

VERSION NUMBER Standard 560S2-01

VERSION DATE August 10, 2018

STANDARD TITLE System Security Standards for Office 365

GOVERNING POLICY This standard is governed by Policy 560: Cloud Storage Services, regardless of revision.

OBJECTIVE The objective of this standard is to establish minimum security requirements for Office 365 Cloud Storage Services: Exchange Online, OneDrive, and SharePoint. These requirements must be applied by the administrators of Office 365 tenants.

REQUIREMENTS As organizations adopt Office 365, they often start with Exchange Online and discover that Microsoft bundles OneDrive and SharePoint. Entities exploring all the services offered by Office 365 face many data security, compliance, and governance challenges. Despite the robust security features built into Office 365, high-risk user behavior can still put sensitive data at risk. It is not uncommon for employees to upload sensitive data to cloud-based file sharing services without fully understanding the risk posed to the organization. Administrators of Office 365 services shall take proactive measures to combat these challenges by implementing the security standards listed below.

1. **Security Standards for Exchange Online:**
   - 1.1. Implement the following countermeasures to combat spoofing and phishing:
     - 1.1.1. Security Policy Framework (SPF)
     - 1.1.2. Domain Keys Identified Mail (DKIM)
     - 1.1.3. Domain-based Message Authentication, Reporting and Conformance (DMARC)
   - 1.2. Secure Mail flow rules:
     - 1.2.1. Set anti-spam options.
     - 1.2.2. Set anti-malware options.

1.2.3. Set extension blocking – executables, program files, scripts, shortcuts, macros, registry files.

1.3. Apply data loss prevention (DLP) rules to prevent emails with sensitive data from being accessed by unauthorized users and set up appropriate remediation actions. Refer to Standard 560S1: Data Loss Prevention for Cloud Services.

1.4. Enable audit logging:

1.4.1. Enable all audit settings.

1.4.2. Turn on reporting features.

1.4.3. Review audit log reports.

1.5. Ensure individuals who are no longer employed have their access terminated immediately.

2. Security Standards for SharePoint Online and OneDrive for Business:

2.1. Allow users to share with authenticated external users only.

2.2. Links should be direct for specific people, and never public.

2.3. The default link permission should be *view*.

2.4. External users should be prevented from sharing files, folders, and sites they do not own.

2.5. External users must accept sharing invitations using the same account where invitations were sent.

2.6. Apply data loss prevention (DLP) rules to prevent emails with sensitive data from being accessed by unauthorized users and set up appropriate remediation actions. Refer to Standard 560S1: Data Loss Prevention for Cloud Services.

2.7. Enable audit logging:

2.7.1. Enable all audit settings.

2.7.2. Turn on reporting features.

2.7.3. Review audit log reports.

2.8. Ensure that individuals who are no longer employed have their access terminated immediately.

SUPPORTING DOCUMENTS

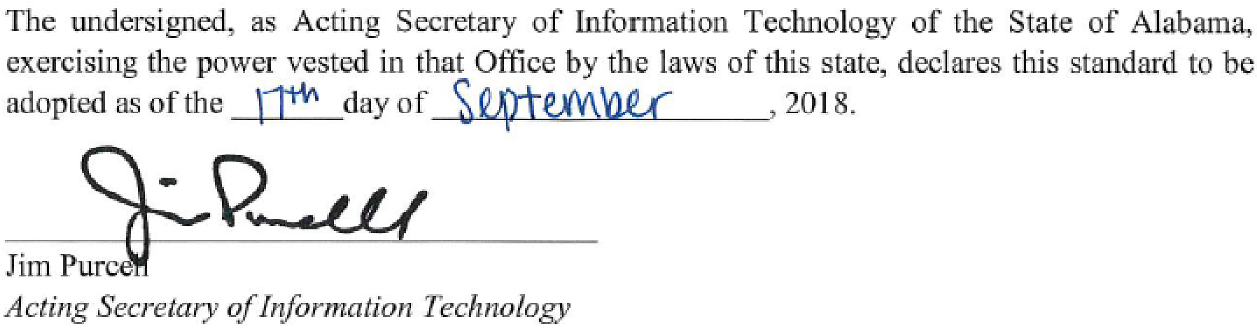
The following documents support this standard:

- Policy 560: Cloud Storage Services
- Standard 560S1: Data Loss Prevention for Cloud 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.

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 17th day of September, 2018.

Jim Purcell
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
560S2-01	08/10/2018	Initial version