STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY

STANDARD 560S3: End-User Security Standards for Office 365

VERSION NUMBER	Standard 560S3-01
VERSION DATE	August 10, 2018
STANDARD TITLE	End-User 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 end-user operation of Office 365 cloud storage services: Exchange Online, OneDrive, and SharePoint.

REQUIREMENTS

As organizations adopt Office 365, they often start with Exchange Online and discover that Microsoft bundles OneDrive and SharePoint. Entities exploring Office 365 can face many data security, compliance, and governance questions. 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. By following the security requirements below, end-users can minimize the risks of unauthorized disclosure of sensitive information.

1. End-User Security Standards for Exchange Online:
   - 1.1. Comply with all federal, state, and local rules applicable to email use.
   - 1.2. Ensure the device operating system and software are up to date.
   - 1.3. Ensure the device is up to date with antivirus and malware protection.
   - 1.4. Ensure the device is protected by a strong password
   - 1.5. Do not click on links or open attachments from unknown senders.
   - 1.6. Do not respond to spam email.

1.7. If an email is from a known sender, verify it came from that person and double check the spelling of the link or attachment.

1.8. If sending sensitive information, encrypt the message by inserting “[ENCRYPT]” in the subject line.

2. End-User Security Standards for OneDrive and SharePoint:

2.1. Comply with all federal, state, and local rules applicable to file sharing use.

2.2. Ensure the device operating system and software are up to date.

2.3. Ensure the device is up to date with antivirus and malware protection.

2.4. Ensure the device is protected by a strong password.

2.5. Encrypt files containing sensitive information at rest and in transit.

2.6. Do not share files with the *everyone* group; share files only with individuals or groups who are authorized to access the files.

2.7. Use folders to share groups of files with others online.

2.8. Be careful sending links to shared folders because links can be forwarded to individuals who should not be provided access.

2.9. Remember that once a file is shared with someone, the file can be download and shared with others.

2.10. Routinely review permissions on shared files and folders and remove individuals when they no longer need access.

3. Connecting to Office 365 over public Wi-Fi or unsecured Internet connection is not recommended. The preferred method of remote access to state information system resources is through a centrally managed Virtual Private Network (VPN) connection that provides encryption and secure authentication.

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 28 day of August, 2018.

Jim Purcell
Acting Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
560S3-01	08/10/2018	Initial version