# STATE OF ALABAMA

**INFORMATION TECHNOLOGY STANDARD**

| Standard 540S1: Email Security Configuration | | |
|---|---|---|
| Document/Version: 540S1-01 | Version Date: 03/05/2021 (draft) | Effective Date: TBD |

OBJECTIVE

Define practices for securing the environments around state email systems in an effort to reduce the risk of system, data, and user credential breaches.

AUDIENCE

Email security configuration requirements are intended for agencies that host an email system, or are responsible for a third-party hosted email system, and the administrators of those systems.

.

REQUIREMENTS

Despite the robust security features built into most email systems, email is still the most commonly used channel for both opportunistic and targeted attacks putting sensitive data at risk. Email users often store or transmit sensitive data without fully understanding the risk to the organization. Administrators of email systems must take proactive measures to combat these challenges by implementing, as applicable, the following security standards.

1. SECURE EMAIL GATEWAY FOR SECURE MAIL FLOW

1.1. Use Transport Layer Security (TLS) 1.2 or higher. TLS uses an encrypted channel to protect message transfers from man-in-the-middle attacks. Earlier TLS versions are not as secure.

1.2. Configure the anti-spam, anti-phishing, anti-virus, and anti-malware options of the Secure Email Gateway to update as frequently as possible and block the messages containing violations of these features.

1.3. Inspect embedded URLs at the time of delivery. If a URL links to a known malicious or phishing site, block the message.

1.4. Block or quarantine executable files and files with macros or other embedded code. This includes Office and other documents that have embedded code, executable files, software installer files, scripting files, PowerShell files, batch files, registry files, Microsoft Management Console files, HTML application files, and program information files.

1.5. Enforce data loss prevention (DLP) rules to prevent outbound email with sensitive data from being accessed by unauthorized users.

1.6. Implement a rule that tags the subject line or the message body of all inbound email from the Internet with "[External]" or similar indicator of the message source.

2. EMAIL AUTHENTICATION FOR PROTECTION AGAINST SPOOFING

2.1. Implement Sender Policy Framework (SPF) records. SPF records standardize the way a sending domain identifies and asserts the authorized mail sender for a given domain.

2.2. Implement Domain Keys Identified Mail (DKIM). DKIM is the mechanism for eliminating the vulnerability of man-in-the-middle content modification by using digital signatures generated from the sending mail server.

2.3. Implement Domain-based Message Authentication, Reporting and Conformance (DMARC). DMARC allows email senders to specify policy on how their mail should be handled, the types of security reports that receivers can send back, and the frequency those reports should be sent.

2.4. Enforce DMARC on inbound email to protect internal users from receiving spoofed external messages from domains that have implemented DMARC in rejection mode.

3. AUDITING AND REPORTING

3.1. Enable mailbox audit and message trace settings. Audit logs and message traces provide valuable visibility into geographic locations of logins, access of mailbox delegates, the service used to login (OWA, SMTP, etc.), creation of new messages, deletion of messages, movement of folders, sending of messages, whether objects or attachments were viewed, sending IP addresses, and number of recipients of any given message.

3.2. Enable system reporting features. Regularly reviewing reports of the email system will provide insight of the effectiveness of the security configuration of the system.

4. DISABLED SERVICES AND FEATURES FOR THE ENTERPRISE EMAIL SYSTEM

4.1. Disable Internet Message Access Protocol (IMAP) and Post Office Protocol (POP3). IMAP and POP3 protocols allow login over unencrypted connections, transmitting login credentials across the network in clear text.

4.2. Disable auto-forwarding rules. The use of client-side forwarding rules to exfiltrate data to external recipients is a commonly used vector for attackers. To preclude inadvertent transmission of inappropriate information onto the Internet, auto-forwarding shall not be used to send state email to an Internet, public, or private email address.

## SUPPORTING DOCUMENTS

This document is governed by:

- Policy 540: Email and Directory Services

Additional supporting documents:

- Standard 560S1-01: Data Loss Prevention for Cloud Services
- Standard 660S1: User Rules of Behavior

The following special publication (SP) of the National Institute of Standards and Technology (NIST) supports this standard and may aid in its implementation:

- NIST SP 800-177: Trustworthy Email



## DOCUMENT CHANGE HISTORY

| Version | Version Date | Comments |
|---|---|---|
| 540S1-01 | 03/05/2021 | Initial version (DRAFT) |
| | | |
| | | |