IT Shared Services Standard: Electronic Mail Standard

For South Carolina State Agencies
Version 1.0
Effective: August 8, 2018

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Revision History:

Date	Authored by	Title	Ver.	Notes
08.08.2018	Security and Architecture Review Board	Standards	1.0	Recommended by the Executive Oversight Group. Standard finalized.

Contents

Electronic Mail

Rationale

Effective email communication is a vital element in the support of South Carolina's citizens. It supports internal agency communications, and it enables external messaging among state agencies and between agencies and the state's citizens. Email is an effective means of communicating and collaborating, providing a flexible messaging platform and a documented record of the communication. The exchange of messages supports individual-to-individual and individual-to-group communications. Messages can be centrally stored and archived. Archival capabilities provide a complete history of the communication including replies, message forwarding, and file attachments.

Agency Exception Requests

Agencies that need to deviate from the standard, and/or technologies specified in this standard, may request an exception from the Technology Work Group (TWG). In such a case, the agency must submit a written statement of their business needs to their Agency Relationship Manager in the South Carolina Department of Administration Program Management Office. The exception request must demonstrate current quantitative performance baselines, or any regulatory compliance required in their business solution. All exceptions must be approved prior to the agency pursuing procurements, deployments, or development activities related to technologies that are not compliant with this standard.

Current State

Currently, there are 44 agencies that have already adopted Microsoft's Exchange Online solution for their electronic mail system. South Carolina is not the only state to move in this direction, 40 other states have a commercially-provided cloud-based email system in use, with more than 80% of those utilizing the Microsoft Exchange Online services. Of the nine states which do not currently offer commercially-provided cloud-based email, four have active projects underway to develop a cloud-based email offering in the near future. Two of the remaining five states currently have private state-provided cloud offerings using Microsoft Exchange.

Purchasing

The state of South Carolina has made a significant investment in Microsoft technologies over the last several years. As such, agencies have far more experience with Microsoft solutions as an email technology and its integration with other office applications. Microsoft Exchange Online is deployed in 44 of the 75 agencies subject to 2017 SC Act No. 97, Part 1B, Section 117.121 and is therefore the State's *de facto* standard.

The administrative and security tools that align with the named Microsoft branded products and/or suites in support of Exchange Online are mentioned only to establish the salient characteristics desired for the various solutions to address compatibility with Exchange Online and currently

deployed solutions and is not intended to limit competition. Complete descriptive literature and all conversion costs must accompany equivalent bids.

Maintenance

Email solutions must be deployed and maintained at a level appropriate for the system, based on the solution's requirements; the manufacturer's best practice guidelines; and security and regulatory compliance standards. Maintenance on software goes beyond fixing "bugs," which is one of the four types of software changes. Updating the software environment, reducing its deterioration over time, and enhancing features to satisfy user requirements are all examples of maintenance work. Core system updates will be the responsibility of the vendor to ensure that their equipment is patched on a regular basis. Major application update changes will be performed by the vendor with a notification to the agency. **Agencies may not remain on software versions that are no longer maintained or supported by the manufacturer.**

An email solution must have a maintenance schedule for patches and hotfixes to be applied per vendor recommendations and release dates. All patches must pass through a test process prior to production distribution.

Further, the maintenance plan should include a summary report on the following:

1. Resources needed to ensure the maintenance cycle can be administered as designed.
2. Estimate time (per week/month/year) needed to perform maintenance.
3. Training plans to develop the necessary skills for support personnel.

Should an agency need assistance designing a maintenance plan tailored to their specific needs, they can request this assistance from the Security and Architecture Review Board (SARB).

Service Level Agreements

Microsoft Exchange Online Service Level Agreement (SLA)[1] offers a 99.9 percent availability, additional outages will have financial impact to vendor. Microsoft defines "downtime" as, "Any period of time when users are unable to send or receive email with Outlook Web Access. There is no Scheduled Downtime for this service."[2] The table below shows the Service Credit amount based upon service availability as defined in the SLA.

Service Credit:

Monthly Uptime Percentage[3]	Service Credit
< 99.9%	25%

[1] Service Level agreement information regarding up time comes from the Service Level Agreement for Microsoft Online Services May 1, 2018 Online.

[2] *Ibid*

[3] Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

Monthly Uptime Percentage[3]	Service Credit
< 99%	50%
< 95%	100%

Security

Electronic messaging (email) systems must be implemented with the appropriate security and privacy controls. Controls will be identified through a combination of regulatory and/or statutory requirements; classification of agency data privacy[4] restrictions; and agency operational needs. At a minimum, all email systems must be compliant with the relevant security controls established in SCDIS-200. Specific controls are defined by an agency's security policies. Security policies with a direct impact on email are:

1. Access Control
2. Data Protection & Privacy
3. Mobile Security
4. Threat & Vulnerability Management

An agency may have additional security, privacy, and operational policies that require security and privacy controls beyond those found in the SCDIS-200 security framework[5]. Each agency must define what these controls are for themselves. Email systems must support these additional controls. Agencies must confirm that all required security and privacy controls are implemented within an email system prior to the agency's use of it.

Multifactor authentication is a requirement for connection to remote systems. If an agency already has multi-factor authentication deployed, then the cloud-based email solution will integrate with that capability. If an agency does not use multi-factor authentication and is moving email services to one of the cloud-enabled environments, then part of the transition must include implementing vendor provided multi-factor authentication.

$$\frac{User\ Minutes\ -Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

[4] Data classification is determined in accordance with the State of South Carolina Data Classification Schema. Agencies should consult their respective Privacy Liaisons when assigning classification levels. Assistance is also available from the Department of Administration's Enterprise Privacy Office.

[5] Examples of additional security and privacy requirements are IRS Publication 1075, the Criminal Justice Information Services (CJIS) Security Policy, and the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. Agencies having data falling under such documents must apply the appropriate controls in their use of any email system.

Data Protection

In addition to the security and privacy policies and controls discussed above, this standard establishes requirements for underlying technologies which support email, or which add confidence to the overall function of the system. The method by which the agency accomplishes the protection is not defined by the standard, but the protection is required.

1. Agencies must protect against unwanted email (spam). This may be accomplished through native functionality within the email system or through other security technologies that the agency deploys.
2. Agencies must deploy advanced threat protection (ATP) as part of their email system to add protection against such threats. This may be accomplished through native functionality within the email system or through other security technologies that the agency deploys.
3. Agencies must implement technologies that take advantage of recent updates in the underlying Domain Name System (DNS) to validate sender domains[6]. These technologies include:
    a. Domain Name System Security Extensions (DNSSEC)
    b. Sender Policy Framework (SPF):
        i. A system to declare and verify who can send e-mails from a given domain
    c. Domain Keys Identified Mail (DKIM)
        i. An e-mail authentication system based on asymmetric cryptographic keys.
    d. Domain based Message Authentication, Reporting and Conformance (DMARC)
        i. An e-mail authentication system that helps in determining what to do when messages fail SPF or DKIM checks.
4. Agencies must deploy a secure email system which supports exchanging, processing, viewing, editing, and storing encrypted email and any attachments send therewith.

Encryption

At a high level, encryption is the process of encoding data (referred to as plaintext) into cipher text that cannot be used by people or computers unless and until the cipher text is decrypted. Decryption requires an encryption key that only authorized users have. Encryption helps ensure that only authorized recipients can decrypt content, such as email messages and files.

[6] These security components were taken from the following standards documents:

- SCDIS-200
- NIST SP 800-45 v2 Guidelines on Electronic Mail Security
- NIST SP 800-177 Trustworthy Email
- NIST SP 800-81-2 Secure Domain Name Service (DNS) Deployment Guide
- NIST SP 800-53 r4 Security & Privacy Controls for Federal Information Systems and Organizations

Encryption by itself does not prevent content, such as files, email messages, calendar entries, and so on, from getting into the wrong hands. Encryption is part of the overall information protection strategy that agencies adopt. Encryption helps ensure that only those who should be able to use encrypted data are able to.

It is possible to have multiple layers of encryption in place at the same time. For example, both the email messages sent, and the communication channel used to transmit the message can be encrypted at the same time using the same or different encryption protocols. In Microsoft's government cloud offering of Exchange Online, data is encrypted at rest and in transit using several strong encryption protocols and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES).

Retention

The South Carolina Public Records Act [SCPRA][7] established the responsibility to protect and ensure the availability of the public records created by government entities. The act identifies public records as all records created by public bodies, regardless of physical format[8] (). Therefore, records created or formatted electronically, including email, must be covered by approved retention schedules.

Retention schedules are produced in conjunction with, and are approved by, the South Carolina Department of Archives and History. Retention schedules dictate the minimum amount of time a public record must be accessible. Each state agency has a records officer who works with the Department of Archives and History to establish retention schedules. Each state agency must coordinate with the Department of Archives and History to ensure all agency emails are covered by approved retention schedules.

Policy Requirements for Electronic Mail

- Each agency must have a defined policy and process for email retention.
- Each agency must have a defined policy and process for FOIA requests.
- Each agency must have a defined policy and process for legal holds.
- Each agency must perform business continuity planning and testing.

Disaster Recovery

Agencies must develop disaster recovery functionality for their email system. Disaster recovery may be accomplished through native functionality within the email system or through other data protection technologies that the agency deploys, either on-premise at the agency's DR site; with a managed service provider; or in the cloud. In cloud-based email implementations, this functionality may be laid upon the cloud service provider if they are able to provide the necessary functionality.

[7] Code of Laws of South Carolina, 1976, Section 30-1-10 – Section 30-1-170
[8] Code of Laws of South Carolina, 1976, Section 30-4-20(c)

Some cloud service providers do not provide data protection as a standard service, but they may provide it as an extra offering. It is also important to note that while cloud-based solutions have higher overall resiliency than on premise systems, this is not the same as a true data protection schema or disaster recovery functionality. It is always the agency's responsibility to ensure that their data is adequately protected against loss. The method by which the agency accomplishes the protection is not defined by the standard, but the protection is required.

Email Architecture

This section describes the different architectures currently in use for email systems in the state. **Agencies must move to the strategic standard shown in the Technology Adoption section below on their next service renewal date if they are not currently using the architecture described there.**

Software as a Service Electronic Mail

Software as a Service (SaaS) Electronic Mail is a vendor-hosted system in which the vendor provides and maintains the infrastructure, middleware, application software and the application data. The vendor may also offer full administration of the system as well, but SaaS email systems also allow agency administration of the system. System security may be supplied by the vendor, or it may be shared between the vendor and the agency. Software as a Service is a key component of cloud-based solutions. Thus, this is a cloud architecture. Users would connect to this service using the internet or a dedicated peering connection. The solution must meet all the requirements laid out in this standard. Examples of SaaS email systems are Microsoft's Exchange Online, part of Office 365 and Google's Gmail offerings.

Infrastructure as a Service Electronic Mail

Infrastructure as a Service (IaaS) Electronic Mail is a different flavor of cloud-based email than is Software as a Service. IaaS does not in itself provide email. Rather, email is delivered via an IaaS implementation. In this architecture, the vendor provides the physical infrastructure, server operating system and storage components. The agency is responsible to provide the application software. A vendor may provide backups, replication, and recovery services as part of their IaaS offering. Basic physical and operating system level security are provided by the vendor, but the overall system and security configuration of the servers, storage, and application tiers of the email system lies with the agency. Administration of the email system would also be an agency responsibility. The solution must meet all the requirements laid out in this standard. There are any number of cloud platforms that are able to provide IaaS for email systems.

On Premise Electronic Mail

An On-Premise Electronic Mail system is a traditional architecture. The agency hosts an email solution at their location and stores email locally. The agency is responsible for all services, features, and operation of their email solution. The burden for securing the platform falls completely on the individual agency.

Technology Adoption

This section lays out the technology roadmap *vis-à-vis* email for the state while recognizing that not all agencies are currently at the same place technologically. When procuring and/or implementing new or upgraded email systems, agencies must adopt the Strategic Technology Tier. Agencies must also be preparing their infrastructure and systems to move towards the Emerging Technology Tier since that technology is expected to become the Strategic Technology within the next five (5) years, the length of a normal technology lifecycle. Agencies which find themselves in the Contained or Obsolete Technology categories must begin planning now to adopt the Strategic Tier no later than when their next technology refresh is scheduled to take place[9].

Emerging Technologies

This tier of technology adoption represents a future state in the overall technology path of modernization. Email systems possessing or enabling the following technologies are considered in the Emerging Technologies category. Many of the features in this tier are currently available, and they are needed to address both security and business operational requirements. Therefore, agencies should begin adopting and deploying the features within this tier as soon as they are able to do so. All features listed must be adopted and enabled for the deployed system to meet the Emerging Technologies standard.

- Government-class service provides Email, Archive, and data protection services with the rich and familiar Outlook experience users are accustomed to. Users can access these services from their desktop web browser using Outlook Web Access(OWA) and mobile devices.
- Shared calendars let users see when others are free or busy throughout all agencies.
- Collaboration tools such as Skype for Business[10], share presence and connect with other users via instant message.
- Participation in the state's Unified Global Address list
- Adoption of an email address sub-domain under sc.gov
- Domain Name System Security Extensions (DNSSEC)
- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain based Message Authentication, Reporting and Conformance (DMARC)
- Email logging interoperability with the state's SOC SIEM devices
- Information Rights Management

[9] Agencies may be required to begin planning their move to the Strategic Tier earlier than the scheduled date of their next technology refresh depending on whether required security features are supported or not.

[10] This standard address only the instant messaging and share presence functions of Skype for Business. Audio/video conferencing technologies are out of scope of this standard. Agencies are directed to consult the state's telecommunications contracts documents for guidance on audio/video conferencing.

Strategic Technologies

This tier of technology adoption represents the current minimum set of technologies a system must support. This is the current standard for system adoption. It is not required that all features must be enabled, but they all must be available in the deployed system.

Software as a Service (Email) - Microsoft Exchange Online

- Specific government cloud segregation from public cloud[11]
- Integration with agency domain validation and authentication mechanisms
- Multifactor authentication
- Anti-malware
- Protection against unwanted email (SPAM)
- Data Loss Protection
- Auditing
- Importing
- Archiving
- Encryption at rest and in transit
- Legal hold
- eDiscovery
- Email logging
- Advanced Threat Protection

Contained Technologies

This tier of adoption represents older technology that does not align with the current course of industry or with the strategic direction of the state. No new implementations of these technologies will be approved. Agencies may continue to operate the architectures below at this time, but they must move into the Strategic Tier at their next system hardware lifecycle refresh point or at the time of a version upgrade of their email software.

Infrastructure as a Service and On-Premise Architectures are classified as Contained Technology, even if they can meet strategic guidelines.

Additionally, the technologies listed below have been available for some time, and they must be deployed in an agency's email solution currently to continue to operate it as a Contained Technology. Agencies, without the below technologies implemented in their email system, must begin the process of adopting the Strategic Technology tier within six months of the publication of this standard If these technologies are not immediately deployed.

[11] State agencies eligible for educational cloud hosting for their offices/units possessing educational certification may use educational clouds insofar as the cloud offering meets the agency's security requirements. Educational institutions outside Proviso 117.121 are not affected by this standard.

- Integration with agency domain validation and authentication mechanisms
- Anti-malware
- Protection against unwanted email (SPAM)
- Email logging
- Multifactor authentication

Obsolescent/Rejected Technologies

This tier of technology represents technology that is no longer approved for state use.

Any system fitting any of the following descriptions:

- Incompatible with internet email.
- Commercial Internet Service Provider email services
- Public cloud deployments

Any agency whose email falls into any of these categories must begin adopting the Strategic Technology tier within three months of the publication of this standard.