



Compliance Component

DEFINITION

| | |
|--------------------|---|
| <i>Name</i> | E-mail Server System Design |
| <i>Description</i> | This component addresses best practices for State of Missouri e-mail systems design, specifically those criteria related to e-mail servers. Referred to as the Mail Transport Agent (MTA), an e-mail server is a software program that routes computer-based messages across local, regional and global networks. E-mail server design specifications include protocols and standards, as well as redundancy/failover capability, operations, administration, and application integration criteria. |
| <i>Rationale</i> | Standards compliant e-mail servers are required for efficient and effective delivery of electronic messages. The E-mail Server System Design Compliance defines the required feature sets for E-mail Server interoperability and baseline functionality. |
| <i>Benefits</i> | <ul style="list-style-type: none"> • Efficient communication with electronic messages. • Improves interoperability. • Encourages the use of open standards. |

ASSOCIATED ARCHITECTURE LEVELS

| | |
|---|--------------------------|
| <i>Specify the Domain Name</i> | Application |
| <i>Specify the Discipline Name</i> | Electronic Collaboration |
| <i>Specify the Technology Area Name</i> | E-mail Architecture |
| <i>Specify the Product Component Name</i> | |

COMPLIANCE COMPONENT TYPE

| | |
|---|-----------|
| <i>Document the Compliance Component Type</i> | Guideline |
| <i>Component Sub-type</i> | |

COMPLIANCE DETAIL

| | |
|---|--|
| <i>State the Guideline, Standard or Legislation</i> | <p>E-mail System Design Criteria</p> <p>State of Missouri E-mail Servers shall be based on products and procedures that meet the checklist of criteria detailed in the following service areas.</p> <ol style="list-style-type: none"> 1. <u>Implementation Requirements</u> <ol style="list-style-type: none"> 1.1. Must support redundancy/failover to ensure high availability; all components of the system must be capable of running concurrently on multiple servers operating in a load-balanced configuration. 1.2. Must be easily scalable. 1.3. Must allow staggered upgrades to individual servers without requiring system outages. |
|---|--|

- 1.4. Must support standard Internet protocols, including: SMTP, POP3, IMAP4, or LDAP where appropriate.
- 1.5. Must support HTTP to provide "webmail" access to e-mail services, where appropriate.
- 1.6. Must support the use of an LDAP directory to look up local delivery addresses.
- 1.7. Must run on multiple platforms and support multiple access channels (including hand held devices).
- 1.8. Should support secure connections between individual e-mail servers.
- 1.9. Should support SMTP authentication as defined in RFC 2554.
- 1.10. Should support secure mailbox access via dial-up access (remote clients).

2. Operations and Administration Requirements

- 2.1. Must support user proxy access.
- 2.2. Must support remote administration of all components of the system via secure login or secure browser connections (SSL).
- 2.3. Must support integrated administration, i.e., the addition, deletion, or modification of a user account must be automatically reflected in all affected components of the system, and must not require duplication of administrative effort for individual components of the system.
- 2.4. Must support mass change and update functionality.
- 2.5. Must support delegation of administrative authority – transition of authority in someone's absence.
- 2.6. Must support hard mailbox quotas.
- 2.7. Must support virus-scanning of all incoming and outgoing SMTP traffic.
- 2.8. Must allow the control of the size of both incoming and outgoing e-mail messages.
- 2.9. Must Support E-mail Retention including support for:
 - 2.9.1. Sunshine Act / Freedom of Information Act implications.
 - 2.9.2. Searchable / Archival mailbox copies available.
 - 2.9.3. Keeping permanent server-based copy of mailboxes.
- 2.10. All externally exposed mail servers:
 - 2.10.1. Must provide native anti-relay and anti-spam features.
 - 2.10.2. Must support interfaces with SPAM and content filtering for both incoming and outgoing e-mail traffic.
 - 2.10.3. Must be configurable to reject messages from hosts with no reverse DNS (RDNS).
 - 2.10.4. Must provide complete control over blocking e-mails with attachments that contain specific file extensions or file names.
 - 2.10.5. Must be configurable to pass the Network Abuse Clearinghouse relay test.
 - 2.10.6. Must support DNS-based "blacklists", such as MAPS, for spam blocking.
 - 2.10.7. Must support the use of a local "blacklist"; must be able to block by host or domain name presented on the SMTP HELO command, IP address, IP net block,

RFC 822 sender address ('return-path' address), and username portion of RFC 822 sender address.

2.10.8. Must support the use of locally-written heuristic rules.

2.10.9. Should support the use of a local "whitelist" to override DNS-based and local "blacklists", and allow the acceptance of messages which would normally be blocked by a general rule. This feature could be used to accept all messages addressed to "postmaster" or "abuse", regardless of the source, or to accept all messages from a specific host or sender within a blocked domain or net block.

2.10.10. Must support e-mail address rewrite (intelligent rewrite).

2.11. Should support "live" backup of the message store, i.e., it must not be necessary to halt the system in order to backup the message store.

2.12. Should provide warnings to users whose mailbox usage exceeds a specified threshold (percent of quota).

2.13. Should support the generation of usage reports. Information which might be required includes, but is not necessarily limited to:

2.13.1. Number of messages sent, received, blocked, delivered to message store.

2.13.2. Message size statistics.

2.13.3. Delivery time statistics.

2.13.4. Number of POP3 and IMAP4 logins; number of login failures.

2.13.5. Quota usage reports.

2.13.6. Message statistics by Agency/Department.

3. User Services Requirements

3.1. Must support browser access to client mailbox via a webmail interface.

3.2. Must not require clear-text transmission of passwords.

3.3. Must be capable of deferring to a third-party authentication service, such as LDAP.

3.4. Must support user-controlled forwarding (auto forwarding rules).

3.5. Must support user-controlled auto-reply (out of office reply).

3.6. Must support system-wide address books and distribution lists including:

3.6.1. Addresses from both internal and external sources.

3.6.2. The ability to store contact information, and provide for easy retrieval in a form that can be used by other programs and applications.

3.6.3. Must support the creation of aliases.

3.7. Must enable the establishment/set-up of auto-responders, such as "out of office notification" or "we received your request and are looking into it".

3.8. Should support strong encryption for secure connections from e-mail and browser clients.

3.9. Should support native authentication (single sign-on).

3.10. Should support concurrent auto-reply, forwarding, and local

| | | |
|--|---|--|
| | <p>delivery.</p> <p>3.11. Should support user-configured server-side rules and filters which are applied when messages are delivered to the user's mailbox.</p> <p>3.12. Webmail interface should meet the W3C Web Content Accessibility Guidelines. This will enable users with visual disabilities to use the webmail service to send and receive messages.</p> | |
| <i>Document Source Reference #</i> | <p>Network Abuse Clearinghouse Relay Test - http://www.abuse.net/relay.html</p> <p>MAPS Blacklist - http://mail-abuse.org/</p> | |
| Compliance Sources | | |
| <i>Name</i> | <i>Website</i> | |
| <i>Contact Information</i> | | |
| <i>Name</i> | <i>Website</i> | |
| <i>Contact Information</i> | | |
| KEYWORDS | | |
| <i>List Keywords</i> | POP3, SMTP, IMAP, LDAP, MIME, PKI, Mail Transport Agent, MTA, distribution list, address book, attachment, virus, spam, filter, alias, SSL, DNS, RDNS, real time blacklist, RBL, whitelist, proxy, Sunshine Law, HIPAA | |
| COMPONENT CLASSIFICATION | | |
| <i>Provide the Classification</i> | <input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i> | |
| <i>Sunset Date</i> | | |
| COMPONENT SUB-CLASSIFICATION | | |
| Sub-Classification | Date | Additional Sub-Classification Information |
| <input type="checkbox"/> <i>Technology Watch</i> | | |
| <input type="checkbox"/> <i>Variance</i> | | |
| <input type="checkbox"/> <i>Conditional Use</i> | | |
| Rationale for Component Classification | | |
| <i>Document the Rationale for Component Classification</i> | | |
| Migration Strategy | | |
| <i>Document the Migration Strategy</i> | | |
| Impact Position Statement | | |
| <i>Document the Position Statement on Impact</i> | | |
| CURRENT STATUS | | |
| <i>Provide the Current Status</i> | <input type="checkbox"/> <i>In Development</i> <input type="checkbox"/> <i>Under Review</i> <input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i> | |

AUDIT TRAIL

| | | | |
|-----------------------------|-----------|---------------------------------|-----------|
| <i>Creation Date</i> | 6/24/2003 | <i>Date Approved / Rejected</i> | 7/18/2003 |
| <i>Reason for Rejection</i> | | | |
| <i>Last Date Reviewed</i> | | <i>Last Date Updated</i> | |
| <i>Reason for Update</i> | | | |