

Overview

All campus E-mail service providers must meet the following minimum standards. E-mail service providers are defined as systems that both send and receive e-mails and support business or individual users accounts.

E-mail Management

1. Installation and operation of an e-mail system must be approved by the Information Security Office.
2. The system owner is responsible for ensuring that the requirements of these standards are met.
3. The department or unit responsible for the e-mail system shall bear the costs of ensuring compliance with this standard.
4. One or more support person(s) must be identified. Current and accurate contact information for the support person must be maintained and communicated to the Information Security Office.
5. The support person(s) must be appropriately classified and demonstrate appropriate knowledge of the e-mail system.
6. The system owner must adopt data retention guidelines and procedures.
7. The system owner must adopt access control guidelines and procedures. The authorization process must be through a documented, auditable process.
8. The system owner must create a disaster recovery plan. The disaster recovery time for a complete system failure must be twelve hours or less.
9. The system owner must provide 'equitable' access to all users of the e-mail system. Equitable is defined by the current campus e-mail system standard service (SacLink.) Equitable access includes but it not limited to:
 - a. User accounts must provide at least 500 MB of storage with the ability to increase capacity to reasonable accommodate the user's business needs.
 - b. Accessible 24/7 from standard web browsers.
 - c. Meets Accessible Technology Initiative requirements.

System Hardening

1. The system owner and support person(s) must ensure that all security patches for the operating system, application and database are evaluated and applied on a timely basis.
2. The e-mail system is run on dedicated hardware or dedicated virtual machine (i.e. not also running file share or FTP services).
3. The support person(s) will implement a well defined host based firewall. Firewall configuration must be provided to the Information Security Office for review.
4. The support person(s) will comply with the Information Security Office vulnerability scanning program.
5. Responsibility for remedy rests with the e-mail system owner.
6. The support person(s) should install and enable rootkit detection and update the signature file at least daily.

Message Handling

1. All incoming messages must be scanned for spam and viruses using current technologies.
2. All outgoing messages must be sent through the campus e-mail gateway (MTA).
3. Secure POP and secure IMAP are the preferred protocols. A business case must be made to support insecure protocols and provide to the Information Security Office.
4. Message relaying must be disabled or properly configured to only relay from known good sources.

Access Control

1. Remote management must be restricted to authorized support person(s) and use strong authentication over an encrypted and secured connection.
2. The equipment must be housed in a physically secured location with a climate controlled environment and protected power. The location access must be auditable.
3. All user access must be authenticated to use e-mail resources.
4. Users are provisioned with individual accounts. Generic accounts are acceptable only if one person is assigned access at any one time.
5. Remove or disable all 'anonymous' and 'guest' accounts.
6. Change passwords on all required default accounts to strong unique passwords.
7. System must enforce strong passwords
8. User accounts on the local host and within application and databases are implemented with the least privilege. Administrative accounts are kept to a minimum.
9. Backup media should be treated as confidential and private. It must always be stored and handled securely. Offsite backup media must be encrypted using a generally accepted strong industry cipher.

Monitoring

1. Security event logging must be enabled and security log files retained for three months.
2. A schedule and procedures must be created to review logs.
3. Any detected or suspected breach of information must be promptly reported to the Information Security Office.

Compliance

1. E-mail systems must be reviewed annually for compliance to this standard.
2. System owners must complete and present a self-assessment to the Information Security Office annually.
3. System owners must document non-compliant systems issues, plans and timeline to remediate the issues.
4. Non-compliant systems without a completed self-assessment will be removed from the network.
5. Non-compliant systems that do not have an adequate remediation plan or timeline will be removed from the network.

Required Documentation

System Owner

1. Procedures for e-mail usage, administration, ownership and maintenance.
2. Documentation of all security measures (corrective, detective and preventative) regarding malicious software (viruses, Trojan horses, spam filtering) at the sever level.
3. Documentation of security provisions to minimize e-mail spoofing and prevent message relaying.
4. Procedures for reporting malicious events and other misuse of e-mail.
5. Procedures for the management and security of e-mail servers.
6. Procedures for controlling information leakage via e-mail and other communications (i.e., restrictions on transmitted file types and/or size).

Information Security Office

1. E-mail standards.
2. Listing of all approved e-mail systems utilized by the campus.