Cybersecurity
Policy Templates

CRF SANS

Email Management Policy

(Last Updated April 2025)

Purpose

Our Email Management Policy aims to establish a comprehensive framework for filtering and monitoring incoming and outgoing email traffic within our organization. This policy provides clear guidelines and procedures for implementing email filtering technologies to enforce security controls, protect against email-borne threats, and mitigate the risk of phishing attacks, malware infections, and data breaches. By implementing robust email filtering practices, this policy seeks to minimize the exposure to malicious emails, spam, and other potentially harmful content, ensuring the confidentiality, integrity, and availability of our systems and data. By configuring appropriate filtering rules, continuous monitoring, and regular updates, we strive to protect against emerging threats, reduce the risk of social engineering attacks, and maintain compliance with industry standards and regulatory requirements. By prioritizing email filtering, we enhance our overall cybersecurity posture, safeguard sensitive information, and maintain the trust and confidence of our stakeholders.

Scope

The Email Management Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses implementing and managing email filtering measures to protect against spam, malware, phishing attempts, and other email-borne threats. This policy covers all email communications sent or received by individuals within the organization, regardless of the email client or device used. It sets forth guidelines for configuring and maintaining email filtering technologies, such as spam filters, antivirus scanners, and content analysis systems. The policy defines procedures for blocking or quarantining malicious or suspicious emails and educating employees on recognizing and reporting potential email threats. Compliance with this policy is mandatory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for email filtering and cybersecurity governance.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

EM-01 Maintain an inventory of each of the domain names authorized to use email.

EM-02 Maintain an inventory of Mail Transfer Agents (MTAs) authorized for each of the organization's approved email domains.

EM-03 Maintain appropriate Domain Name System (DNS) records for each of the organization's approved email domains (including SPF, DKIM, and DMARC).

EM-04 Ensure that the organization's email systems require encrypted connections (TLS) between all email servers, whether internal or external.

EM-05 Ensure that the organization's email systems block emails from domains that do not utilize the appropriate Domain Name System (DNS) records (including SPF, DKIM, and DMARC).

EM-06 Ensure that the organization's email systems perform spam content filtering for all emails (received by or sent by the organization).

EM-07 Ensure that the organization's email systems perform malware content filtering for all emails (received by or sent by the organization).

EM-08 Ensure that the organization's email systems perform anti-phishing content filtering for all emails (received or sent by the organization).

EM-09 Ensure that the organization's email systems perform anti-phishing URL filtering for all emails (received by or sent by the organization).

EM-10 Ensure that the organization's email systems filter data content for all of the organization's email (received by or sent by the organization).

EM-11 Ensure that the organization's email systems perform attachment filtering for all emails (received by or sent by the organization), including utilizing sandboxes to validate each attachment.

EM-12 Maintain a file transfer portal system that is separate from the organization's email system and that the organization can use to send large files to individuals outside of the organization.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.