

Your  
Organization  
Logo Here

# Organization XYZ E-mail Filtering Standard

## 1.0 Purpose

The purpose of this standard is to define how e-mail must be filtered at Organization XYZ.

## 2.0 Scope

This standard applies to all e-mail that traverses Organization XYZ's e-mail systems. E-mail administrators are responsible for understanding and implementing the requirements of this standard.

## 3.0 Standard

E-mail filtering has three main security objectives. One objective is to ensure the full availability of Organization XYZ's network resources. Another objective is to protect the e-mail client. The third objective is securing the e-mail content that traverses Organization XYZ's e-mail systems. The e-mail filtering process includes content filtering, virus scanning, and prevention of unsolicited e-mail. To ensure compliance with security objectives, these standards must be followed:

### 3.1 Content Filtering

Employ a content filtering mechanism that scans all incoming e-mail messages and their attachments and manages the messages depending on the results of the scan.

#### 3.1.1 Suspicious Content

Strip suspicious active content (ActiveX, JavaScript, etc.) from e-mail and forward to quarantine.

#### 3.1.2 Prohibited Words

Quarantine e-mails that contain words or phrases that indicate the e-mail is "junk" or "spam", words in the "Carlin List" and words that are racist, libelous, offensive or obscene.

#### 3.1.3 Outbound Filtering

Protect the organization from possible litigation or loss of sensitive data by implementing outbound e-mail filtering.

3.1.3.1 Quarantine outbound e-mails that contain words or phrases viewed as inappropriate for use in organizational e-mail, including hoaxes and "spam".

3.1.3.2 Quarantine outbound e-mails that contain words or phrases that indicate sensitive data is leaving the organization.

### **3.2 Malicious Code Scanning**

Employ a virus scanning mechanism that scans all incoming e-mail messages and their attachments to determine the existence of viruses or other malicious code.

#### **3.2.1 Virus Updates**

Ensure that the virus scanning mechanism uses an up-to-date list of virus and other malicious code signatures.

#### **3.2.2 Virus Cleaning and Quarantine**

Ensure that all e-mails with identified viruses or other malicious codes are stripped of the code and released or quarantined.

### **3.3 Prevention of Unsolicited E-mail**

Employ a content filtering mechanism that scans all incoming e-mail messages to determine if the e-mail is unsolicited or "spam".

#### **3.3.1 Block Specific Domains or Mail Servers**

Reject messages originating from domains or mail servers known to send unsolicited e-mails.

#### **3.3.2 Keyword Filtering**

Quarantine e-mails containing keywords in the subject line or message body that indicate the e-mail is unsolicited or "spam".

### **3.4 Monitoring**

Conduct regular monitoring of the e-mail filtering system.

#### **3.4.1 Logging and Retaining Log Files**

Ensure that all appropriate logs associated with the filtering of e-mail are enabled and configured to retain data in accordance with the System Monitoring and Logging Standard. For instance, e-mail filtering logs should show how many e-mails have been quarantined and for what reasons, etc.

#### **3.4.2 Reviewing Log Files**

Review log files to determine if the e-mail filtering system is operating effectively and to identify trends. Automated log file analysis tools may be utilized. Logs must be reviewed on a schedule in accordance with the System Monitoring and Logging Standard.

## **4.0 Responsibilities**

**4.1** E-mail administrators are responsible for understanding and implementing the requirements of this standard.

- 4.2** The Chief Security Officer is responsible for ensuring that the e-mail filtering process is monitored and is operating effectively.

## **5.0 Compliance**

- 5.1** Company officers and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this standard.
- 5.2** Failure to comply with this standard may result in disciplinary action, which may include termination of employment.

## **6.0 Definitions**

**Quarantine:** E-mail that is quarantined is sent to a special location for later administrative action instead of to the intended recipient.

## **7.0 Related Policies and Standards**

- Corporate Security Policy
- System Security Policy
- Malicious Code Policy
- System Monitoring and Logging Standard

## **8.0 Revision History**

<b>Version</b>	<b>Date</b>	<b>Revision</b>
1.0	Month Day, Year	Standard Written