Insert the organization logo by clicking on the image icon

Email Security Policy Template

Date:

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Title:** | Email Security Policy Template | | |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  | |
| **Publish Date:** |  | | |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 3](#_Toc97461801)

[2. Scope 4](#_Toc97461802)

[3. Policy 4](#_Toc97461803)

[3.1 Email Usage 4](#_Toc97461804)

[3.2 Email System 5](#_Toc97461805)

[4. Policy Enforcement 5](#_Toc97461806)

# Objective

The purpose of this policy is to outline the best practices of using the email system and ensure that users are aware of acceptable and unacceptable uses of its email system. The policy highlights the minimum requirements for secure use of email within the <entity name> Network.

# Scope

This policy applies to all <entity name> employees, contracted personnel, trainees, third party's representatives who have been provided access to the Email system at <entity name>. This policy covers all information systems (Environments operated by the IT team).

# Policy

* 1. Email Usage

1. Email usage should be in accordance with policies and procedures governing ethical conduct, safety, legal compliance, and proper business practices.
2. Users should use email for business purposes only, personal communication is permitted on a limited basis.
3. All classified messages and attachments in email must be protected according to the should be in accordance with Law No. (16) 2014 concerning state secrets law.
4. Users should not open attachments from unknown or untrusted sources. A virus scan must be performed on all materials being sent or received.
5. Users should not send non-business-related attachments that contains large files graphics and multimedia using the <entity name> email account.
6. Users are prohibited to for forwarding emails to third-party email system automatically.
7. Users are prohibited from using third-party email systems and storage servers to conduct business.
8. Users can use reasonable number of resources for personal emails. however, non-work-related email shall be saved in a separate folder from work related email such as, sending jokes, or chain letters using business email is prohibited.
9. Users shall not forward messages to individuals “chain mail”, that may unnecessarily utilize system resources or interfere with the work of others.
10. Users shall have no expectation of privacy of their email uses. Such as, data being stored, messages sent or received on the <entity name> email system.
11. Users must not provide other unauthorized individual with their E-Mail account and password.
12. Users should not distribute internal mailing list to un-authorized individuals.
13. Users must not install any programs, upgrades or patches being received via email, unless it is approved by IT security team.
    1. Email System
14. The <entity name> email system shall not contain or used for distribution of any disruptive or offensive messages. Such as, race comments, gender, hair colour, disabilities, age, pornography, religious beliefs and practice, political beliefs, or national origin.
15. The <entity name> email system should not be used to transmit confidential messages such as trade secret or copyrighted materials, legal or contractual agreements, technical information related to the <entity name> operations or security, unless it is digitally signed and encrypted communication.
16. Messages received from unsecured email account shall not considered secured or private, unless it is digitally signed and encrypted.
17. The <entity name> email system and information must be monitored and reviewed for any legitimate purposes. This will help to ensure compliance, prevent unauthorized uses of the system, and troubleshooting.
18. All distributed email accounts must not contain active link to Internet website unless it is approved by IT security team.
19. Email system must be backed up and available for recovery purposes for 7 days.
20. Email system should limit the attachments size by file compression utilities before sending them, non-business-related attachments greater than 3MB are restricted by external gateway.
21. IT team should implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards to minimize the chance of spoofed or modified emails from valid domains.
22. IT team shall block unnecessary file types entering the <entity name> email gateway/system.
23. IT team should deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.

# Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-