Heimdal®

Email Security Policy Template

Overview

Email at [COMPANY-NAME] is to be treated as an essential and crucial resource. Therefore, we are implementing this policy to:

1. Develop sensible and appropriate guidelines for using information resources.
2. Inform users about their duties related to the utilization of these resources.
3. Set up a timeline for the retention and archiving of emails.

Purpose

The purpose of this Email Security Policy is to ensure the integrity, confidentiality, and availability of [COMPANY-NAME]'s email services. This policy outlines the standards and procedures by which all employees must abide to safeguard [Company Name]'s electronic communications.

Scope

This policy applies to all employees, contractors, and third-party representatives of [COMPANY-NAME] who have access to the company's email system. It encompasses all hardware and software, as well as any associated services, used to conduct company business via email.

Policy Details

Privacy and ownership of information

Notice of waiver: Users relinquish any expectation of privacy for materials they produce, store, send, or receive using [COMPANY-NAME]'s computer systems.

[COMPANY-NAME] reserves the right to monitor communications, such as emails, without prior notification. Furthermore, all content—including personal emails, files, and documents—are the property of [COMPANY-NAME], may be accessed per company policy, and could be subject to public records requests.

Email security measures

Vigilance against malware:Emails must be handled with extreme caution to mitigate information security risks. An antivirus tool is employed to detect and manage malicious codes or files.

All incoming emails undergo filtering to check for viruses, malicious codes, or spam, which will be isolated for user review. Introducing malware into [COMPANY-NAME]'s systems can severely disrupt business operations. Any detected security threats must be reported to IT immediately.

Anti-spoofing efforts: Procedures are in place to detect spoofed emails. Employees are expected to identify and report suspected email spoofing to IT promptly.

Safe handling of email attachments: Emails are screened for malicious attachments. Files with extensions known to harbor malware or pose a significant risk are removed before email delivery.

Blocking malicious senders: Emails from domains or IP addresses linked to known malicious entities are automatically blocked. Misbehaving email accounts, especially those sending out spam, will be deactivated and investigated.

Proper use of email

Business communication standards: Email should be used solely for business-related purposes and must mirror the professionalism expected in other business communications.

Outgoing attachments are automatically scanned for malware. Improper use of email can damage both the recipient's system and [COMPANY-NAME]'s reputation.

Prohibited activities:

- Sending intimidating, harassing, or offensive emails.
- Using email for personal matters.
- Engaging in unauthorized promotional activities.
- Violating copyright laws.
- Sending emails from another user's account without permission.
- Creating a false identity or forging email messages.
- Disabling security features, such as automatic scanning.
- Circumventing email security protocols.
- Sending joke emails, chain letters, or engaging in spam-like activities.
- Sending overly large emails or attachments.
- Distributing emails containing viruses.

Email confidentiality and security

Data encryption: Any confidential or sensitive [COMPANY-NAME] information sent outside the company’s network must be encrypted. Passwords or decryption keys should never be transmitted via email.

Security precautions: Email is inherently insecure; therefore, sensitive information like passwords, social security numbers, and personal identifiers should not be emailed to external parties without encryption. All user activity on {COMPANY-NAME}'s systems is logged and subject to monitoring.

Representation restrictions: Users must avoid giving the impression they are speaking on behalf of [COMPANY-NAME] unless they have explicit or implicit authorization.

Use of non-[COMPANY-NAME] email accounts: Confidential or sensitive company information must not be sent, forwarded, or received through non-[COMPANY-NAME] email accounts.

Users employing non-[COMPANY-NAME] issued devices must comply with the Personal Device Acceptable Use and Security Policy.

Incidental use policy

Guidelines for personal use: Incidental personal use of [COMPANY-NAME]'s email systems is permitted for approved users only and must not extend to family members or acquaintances. Such use should not incur any direct costs to [COMPANY-NAME] nor interfere with an employee’s regular duties.

Content restrictions

Employees must not send or receive files or documents that could expose [COMPANY-NAME] to legal liability or cause embarrassment. The storage of personal files within [COMPANY-NAME]'s IT systems should be kept to a minimum.

Email retention practices

Retention period: All emails are retained in the system for a period of 36 months. Emails that exceed this age will be automatically purged from the system.

Purging policy: Both deleted and archived emails are automatically purged after the retention period. Similarly, appointments, tasks, and notes older than 36 months will also be purged.

Email archive access

- **Access rights:** Only the mailbox owner and the system administrator are granted access to email archives.
- **Archive maintenance:** Emails stored in the online archive will be deleted 36 months from their original send or receive date, consistent with the general email retention policy.