

[COMPANY NAME] Email Usage and Retention Policy

Purpose

When email goes out from [COMPANY NAME] the general public will tend to view that message as an official policy statement from the [COMPANY NAME]. This policy is to govern the method which email is used to prevent tarnishing the public image of [COMPANY NAME], to prevent unauthorized disclosure of proprietary information, and inappropriate use of email. The policy is defined so when a breach of protocol is alleged there is standard which all users of email have accepted and remediation methods are known.

Proper email usage and security is a team effort involving the participation and support of every [COMPANY NAME] employee. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Scope

This policy covers appropriate use and retention of any email sent from a [COMPANY NAME] email address and applies to all employees, vendors, and agents operating on behalf of [COMPANY NAME].

Policy

1. Prohibited Use

The [COMPANY NAME] email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any [COMPANY NAME] employee should report the matter to their supervisor immediately.

Inappropriate email is classified but limited to:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

2. Personal Use

Using a reasonable amount of [COMPANY NAME] resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a [COMPANY NAME] email account is prohibited. Virus or other malware warnings shall only be sent from [COMPANY NAME] Information Security Team or authorized third party email security vendor. Mass mailings from [COMPANY NAME] shall be approved by [COMPANY NAME] on a per project basis. These restrictions also apply to the forwarding of mail received by a [COMPANY NAME] employee.

3. USENET Postings

Posting to USENET newsgroups is strictly prohibited unless authorized by your supervisor and the information security team. The necessity of posting to a USENET group should be a rare event and limited to the information technology group looking for help or guidance. Postings by employees from a [COMPANY NAME] email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of [COMPANY NAME], unless posting is in the course of business duties.

4. Monitoring

[COMPANY NAME] employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system. [COMPANY NAME] may monitor messages without prior notice. [COMPANY NAME] is not obliged to monitor email messages.

5. Email Retention Policy

This policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

| | |
|--|----------------------------|
| Email Retention Categories - Email information is categorized into four main classifications with retention guidelines: | |
| Administrative Correspondence | 4 Years |
| Fiscal Correspondence | 4 Years |
| General Correspondence | 1 Year |
| Ephemeral Correspondence | Retain until read, destroy |

Email Retention Categories Definitions

Administrative Correspondence

Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox admin@[COMPANY NAME] has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

Fiscal Correspondence

Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@[COMPANY NAME] has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

General Correspondence

General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

Ephemeral Correspondence

Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

5. Encrypted Communications

Encrypted communications should be stored in general in a decrypted format. The encryption should be used to protect the transport of the message not the storage. The security controls that protect the network will also protect the storage of the email. Encrypted email should be used when sensitive information is sent to non company email addresses.

6. Recovering Deleted Email via Backup Media

[COMPANY NAME] maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Email

The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical clients include Eudora and Microsoft Outlook.

Forwarded email

Email resent from an internal network to an outside point.

Chain email or letter

Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Sensitive information

Information is considered sensitive if it can be damaging to [COMPANY NAME] or its customers' reputation or market standing.

Virus warning

Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

Unauthorized Disclosure

The intentional or unintentional revealing of restricted information to people, both inside and outside [COMPANY NAME] who do not have a need to know that information.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here...]. If you have a business need to use other mailers contact the appropriate support organization.

Encryption

Secure [COMPANY NAME] sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

Spam

Unauthorized and/or unsolicited electronic mass mailings.

Special thanks to The SANS Security Policy Project
(<https://www.sans.org/resources/policies/?portal=298306d377f45c9efa8cf59885c1c44b>)

This policy was developed by merging policies from the SANS project, mixed with industry experience, and then tailored for small-medium business.