Email Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated*

1 Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

2 Purpose

The purpose of this email policy is to ensure the proper use of <Company Name> email system and make users aware of what <Company Name> deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within <Company Name> Network.

3 Scope

This policy covers appropriate use of any email sent from a <Company Name> email address and applies to all employees, vendors, and agents operating on behalf of <Company Name>.

4 Policy

4.1 All use of email must be consistent with <Company Name> policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

4.2 <Company Name> email account should be used primarily for <Company Name> business-related purposes; personal communication is permitted on a limited basis, but non-<Company Name> related commercial uses are prohibited.

4.3 All <Company Name> data contained within an email message or an attachment must be secured according to the *Data Protection Standard*.

4.4 Email should be retained only if it qualifies as a <Company Name> business record. Email is a <Company Name> business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

4.5 Email that is identified as a <Company Name> business record shall be retained according to <Company Name> Record Retention Schedule.

4.6 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.

4.7 Users are prohibited from automatically forwarding <Company Name> email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain <Company Name> confidential or above information.

4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct <Company Name> business, to create or memorialize any binding transactions, or to store or retain email on behalf of <Company Name>. Such communications and transactions should be conducted through proper channels using <Company Name>-approved documentation.

4.9 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.

4.10 <Company Name> employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

4.11 <Company Name> may monitor messages without prior notice. <Company Name> is not obliged to monitor email messages.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

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

6 Related Standards, Policies and Processes

- Data Protection Standard

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Updated and converted to new format.