[INSERT FIRM LEGAL NAME]
Email Security Policy

[Insert Firm Logo]

Version 1.0
[Insert Date]

This document is proprietary and confidential. The document and information contained herein may not be shared outside of [Insert Firm Legal Name] unless approved by authorized personnel.

Contents

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company-specific document. **Otherwise, it would be a liability exposure to establish a policy and not comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

This document is enhanced using Human Intelligence (Hi) from the Riskigy vCISO team. For additional tuning and generating bespoke policies, procedures and plans the team can be reached at info@riskigy.com

Policy Overview

It is important for users to understand the appropriate use of electronic communications. 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 pose many legal, privacy, and security risks. A company's policies and procedures should address employees' responsibilities with respect to email usage.

The use of email is a privilege. It should be used for legitimate business reasons and its expected use should align with company policy. All employees are expected to conduct themselves according to ethical standards, safe and healthy practices, compliance with applicable laws, and proper business practices.

Email is a vital part of our communication. All email accounts are provided for business use and should be used primarily for business-related purposes. Personal communication is permitted on a limited basis, but non-business-related commercial uses are prohibited.

All data contained within an email message or attachment must be secured according to the Data Protection Standard. In order for information to be secure, it must be encrypted and stored in an encrypted form that is accessible only by authorized individuals.

Email is only a business record if it meets the criteria of being an official and ongoing part of your business. There should be a legitimate reason to preserve the information contained within it.

The email system is provided for business purposes only. The creation or distribution of offensive messages, including emails with lewd or explicit content, emails that are disruptive to the operation of the Business, or offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin will not be tolerated.

Mail forwarding is a violation of Institute policy. Users are prohibited from automatically forwarding emails to a third-party email system. Individual messages which are forwarded by the user must not contain confidential information.

Spamming, bulk emailing, and the use of unapproved email systems (such as Google, Yahoo, and MSN Hotmail) are prohibited. Such communication and transactions should be conducted through proper channels using -approved documentation. All employees should be aware of current IT policies regarding prohibiting the use of unapproved email services while conducting business.

Maintaining a separate folder for personal emails, in addition to work-related emails is highly encouraged. Chain letters and joke emails are not allowed. These are examples of unprofessional behavior that can lead to reprimanding if allowed to continue.

Employees shall have no expectation of privacy in any information they send, receive, or store in the company's email system including, but not limited to, all messages of a personal, political, or religious nature.

Email messages may be monitored by our staff without prior notice. The company is under no obligation to monitor emails sent or received.

Scope and Purpose

Scope
This policy seeks to minimize the risks of email abuse and provide consistent guidelines for all employees, vendors, and agents.

Purpose

The purpose of this email policy is to ensure the proper use of email and make users aware of what deems as acceptable and unacceptable use. This policy outlines the minimum requirements for use of email within Networks.

Compliance

The Information Security team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

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

Exceptions

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

Definitions and Terms

None

Appendix

None

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	2023	Initial Draft	Riskigy
2				