|  |  |  |
| --- | --- | --- |
| Document ID  **ITAD108** | Title  **EMAIL POLICY** | Print Date  **mm/dd/yyyy** |
| Revision  **0.0** | Prepared By  **Preparer’s Name / Title** | Date Prepared  **mm/dd/yyyy** |
| Effective Date  **mm/dd/yyyy** | Reviewed By  **Reviewer’s Name / Title** | Date Reviewed  **mm/dd/yyyy** |
|  | Approved By  **Final Approver’s Name / Title** | Date Approved  **mm/dd/yyyy** |

**Policy:** The use of electronic mail (or email) shall be limited to support of the Company’s business needs.

**Purpose:** To delineate specific standards regarding the use of email within the Company Information Technology network.

**Scope:** This policy applies to all Company personnel and computer systems.

**Responsibilities:**

All Employees are responsible for knowing, understanding, and adhering to the Company’s email policy.

The Human Resources Manager is responsible for communicating the email policy to all new Employees and retaining employee policy acknowledgements.

Department Managers are responsible for communicating revisions to the email policy to employees in their respective departments.

Information Technology Managers are responsible for developing email policy and reviewing the policy (and any changes) with the Policy Committee.

The Information Technology Security Manager is responsible for monitoring email use and enforcing the Company email policy.

The Email Policy Committee is responsible for review and final approval of the Company email policy and any revisions.

**Definitions:** Email Policy Committee – A group comprised of Top Management, the Information Technology Security Manager, and Information Technology Managers and led by Information Technology Managers. The purpose of the Email Policy Committee is to develop, revise (as needed), and approve the Company’s email policy.

Top Management – A group comprised of the Company’s chief executive and chief financial officers, at a minimum.

**Procedure:**

### 1.0 EMAIL POLICY DEVELOPMENT

1.1 Information Technology Managers shall develop the Company email policy, which may be based on common business standards and practices and on legal/regulatory requirements (see Reference B).

1.2 Information Technology Managers shall present the policy to the Email Policy Committee for review.

1.3 The Email Policy Committee shall review the email policy, revise as needed, and signify its approval.

### 2.0 email POLICY IMPLEMENTATION

2.1 Upon approval of the email policy by the policy committee, Information Technology Managers shall communicate the policy to all department managers. Department managers shall, in turn, communicate the policy to all employees in their departments.

* The Human Resources Manager shall be responsible for communicating the Company email policy to all new employees.
* All employees shall receive a copy of ITAD108-1 COMPANY EMAIL POLICY ACKNOWLEDGEMENT. Upon reviewing the document, each employee shall sign and date their copy of the acknowledgement and return it to Human Resources. Employees should keep a copy of this document for themselves.

2.2 Email records shall be managed in accordance with ITAD102 IT RECORDS MANAGEMENT.

2.3 The Information Technology Security Manager shall be responsible for monitoring Company email and enforcing the email policy.

### 3.0 EMAIL POLICY review

3.1 At regular intervals (annually, at a minimum), Information Technology Managers shall review the Company’s email policy, to see if it continues to meet Company requirements.

3.2 If the email policy does not conform to Company requirements, Information Technology Managers shall convene the policy committee for the purpose of implementing improvements to the policy.

### 4.0 EMAIL POLICY CHANGES

4.1 The Email Policy Committee shall periodically review the Company email policy, to verify that it continues to meet Company requirements.

4.2 Where the policy does not meet requirements, the Policy Committee shall revise the policy as needed and communicate the revised policy to all employees.

4.3 Within one month of such changes to the email policy, the Information Technology Security Manager shall verify that they are being implemented and that they are having the intended effect.

**Forms:**

* ITAD108-1 COMPANY EMAIL POLICY ACKNOWLEDGEMENT

**References:**

1. **ISO 9001 QUALITY MANAGEMENT SYSTEMS-REQUIREMENTS, CLAUSE 4.2.4 (CONTROL OF RECORDS)**

Clause 4.2.4 of this Standard states that “(r)ecords shall be established and maintained to provide evidence of conformity to requirements and of the effective operation of the quality management system. Records shall remain legible, readily identifiable, and retrievable. A documented procedure shall be established to define the controls needed for the identification, storage, protection, retrieval, retention time, and disposition of records.”

1. **SARBANES-OXLEY ACT OF 2002**

The Sarbanes-Oxley Act (“SOX”) passed by the U.S. Congress in 2002 is designed to prevent manipulation, loss, and/or destruction of publicly-held companies’ records. According to a number of high-profile SOX-related cases, email is a company record and is subject to inspection and retention guidelines like any other Company document. Therefore, an organization has to have – and follow – an email policy to be in compliance with SOX.

**Additional Resources:**

1. ITAD103 IT DOCUMENT MANAGEMENT

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of Changes** | **Requested By** |
| 0 | mm/dd/yyyy | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[This page intentionally left blank]

**ITAD108-1 COMPANY EMAIL POLICY ACKNOWLEDGEMENT**

Revision

Date

### 1.0 EMAIL AND THE COMPANY

All portions of the Company information infrastructure, including the information being transported by this infrastructure, are the property of the Company. This includes all email transmitted or received through the Company information infrastructure.

Since email is the property of the Company, all email accounts and the email stored by these accounts are subject to inspection at any time. Email is a powerful tool that can greatly enhance communication. The use of email within the following guidelines by Employees is encouraged.

### 2.0 GENERAL GUIDELINES

Employees shall follow the following general guidelines concerning the use of this company resource:

* Email is not private. Messages transmitted through the Company email system or network infrastructure are the property of the Company and are, therefore, subject to inspection at any time. Use of the Company email system automatically imply consent to search.
* Employees shall be required to retain emails related to essential, or mission-critical, projects. Emails that do not pertain to mission-critical projects or issues should be deleted when they are no longer needed.
* Because attachments to emails are a common method of attacking computers and systems and because attachments occasionally use a lot of bandwidth, sending a file as an email attachment or opening an email attachment is strongly discouraged.
* Use of Company email or messaging services shall be used for the conduct of Company business only. Company email shall not be used for private, recreational, or any other non-Company-related activity.
* Company email shall not be used for commercial or partisan political purposes.
* Employees shall ensure all communication through Company email or messaging services is conducted in a professional manner. The use of vulgar, obscene, lewd, or suggestive language is prohibited.
* Company users shall not reveal private or personal information by email without specific approval from management.
* Users should ensure that email messages are sent to only those users with a specific need to know. The transmission of email to large groups should be avoided.
* Company email shall not be used for any illegal or unlawful purposes. Examples of this are transmission of violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful material.
* Company email services shall not be used to harass, intimidate, or otherwise annoy another person.
* The Company shall not be held liable for damages related to inappropriate use of email by Employees or their families.
* FAILURE TO FOLLOW ANY PART OF THIS POLICY WILL RESULT IN DISCIPLINARY ACTION, UP TO AND INCLUDING TERMINATION.

### 3.0 EMPLOYEE ACKNOWLEDGEMENT

I have reviewed the Company’s email policy. By signing and dating this form, I attest to my understanding and acceptance of this policy. I understand that if I am found in violation of this policy, I may be subject to Company disciplinary action, up to and including termination, as well as civil and/or criminal prosecution.

Signature: Date:

Print name: