E-Mail Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Electronic mail (E-mail) is used as a means of communicating official company information to Staff, is convenient, rapid, environmentally aware, and cost effective. ABC Company issues an e-mail address and disk space (for e-mail storage) to all Staff. ABC Company also distributes e-mail software on computer systems. This practice ensures that all Staff have e-mail communication readily available to them. The purpose of this policy is to set forth the rights and responsibilities of both users and providers of electronic mail for Staff.

# II. Purpose

This policy protects ABC Company’s e-mail related assets and helps ensure our ability to continue business operations including communications with Staff, suppliers, customers, the media, and other business contacts.

# III. Scope

This policy applies to all Staff that have access to ABC Company e-mail.

# IV. Policy

A. Company Uses of E-mail

ABC Company uses electronic mail to communicate official ABC Company information of many kinds to Staff and clients. Staff are responsible for reading their e mail on a frequent and regular basis, since some official communications may be time sensitive. ABC Company suggests that Staff access their e-mail account on a daily basis.

B. Forwarding of E-mail messages

ABC Company issues e-mail accounts and disk storage to all Staff. Staff must not forward e-mail from their ABC Company e-mail address to a different e-mail address, such as one obtained from an external Internet Service Provider (e.g. AOL, gmail, Hotmail). ABC Company has no control over the delivery of e-mail that has been forwarded outside of our domain to external providers.

C. Security and Privacy

ABC Company makes every effort to secure its computer systems, networked resources, and e-mail accounts, but cannot guarantee the infallibility of these systems to unauthorized intrusion, nor the authenticity of the sender of an electronic communication. For this reason e-mail is not appropriate for transmitting confidential or sensitive information of any kind. For example, e-mail should not be used to notify Staff of disciplinary or any other legal action.

Staff are responsible for keeping their e-mail passwords confidential, and should never share this information or access to Company resources with others, including friends and family members.

Without prior notice, ABC Company reserves the right, but not the obligation, to routinely monitor and inspect individual accounts, files, and communications. Staff shall have no expectation of privacy in anything they store, send or receive on ABC Company’s e-mail system. ABC Company may monitor messages without prior notice and is not obliged to monitor e-mail messages.

Spam filters shall be implemented to limit unwanted e-mail as well as reduce the likelihood Staff will perform actions such as clicking on e-mail html links or downloading malware attachments to their local devices.

D. E-mail Retention

This policy is intended to help Staff determine what information sent or received by e-mail should be retained and the appropriate retention period. 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. E-mail is categorized and retained according to the following guidelines.

Administrative correspondence - 3 years. 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 e-mail with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox adminemail@abccompany.com has been created, if you copy (cc) this address when you send e-mail, retention will be administered by the IT Department.

Financial correspondence - 7 years. Financial correspondence includes all information related to revenue and expense for ABC Company. To ensure financial correspondence is retained, a mailbox financeemail@ has been created, if you copy (cc) this address when you send e-mail, retention will be administered by the IT Department.

General correspondence - 1 year. General correspondence addresses information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for e-mail retention of general correspondence.

Refer to the Data Retention Policy for more information on archiving and retention requirements.

E. Encrypted Communications

In general, messages should be stored in a decrypted format. 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 e-mail. Encrypted e-mail should be used when sensitive information is send to non-company e-mail addresses.

International issues regarding encryption are complex. Staff shall follow corporate guidelines on export controls on cryptography, and consult the Legal Department for further guidance.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.03, APO05.03, APO10.05, APO12.02, BAI02.05, BAI04.05, MEA01.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv)

ISO 27001 A13

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 AC-4, AC-20, AC-21, CA-3, PA-4, SC-7, SC-8

NIST Cybersecurity Framework ID.AM-2, ID.GV-4, PR.AC-1, PR.AC-4, PR.AC-7, PR.DS-1-5

PCI 6.1, 6.2, 6.7