



Cyber Tree Systems

A Business IT Solution Company

Email & Messaging Use and Retention Policies

Statement of Purpose

This document will outline the appropriate use, security, and retention of email and messaging communications, ensuring confidentiality, integrity, and compliance with regulatory requirements.

1.0 Email Use Policy

1.1 Purpose

To prevent tarnishing the public image of CTS. When email leaves the CTS domain, the public will tend to view that message as an official policy statement from CTS.

1.2 Scope

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

1.3 Policy

1.3.1 Prohibited Use

The CTS 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 CTS employee should report the matter to their supervisor immediately.

1.3.2 Personal Use

Using a reasonable amount of CTS 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 CTS email account is prohibited. Virus or other malware warnings and mass mailings from CTS shall be approved by CTS VP Operations before sending. These restrictions also apply to the forwarding of mail received by a CTS employee.

1.3.3 Monitoring

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

2.0 Email Retention Policy

2.1 Purpose

The Email Retention 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.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to InfoSec.

2.2 Scope

This email retention policy is secondary to CTS policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner.

All CTS 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)

2.3 Policy

2.3.1 Administrative Correspondence

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

2.3.2 Fiscal Correspondence

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

2.3.3 General Correspondence

CTS 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.

2.3.4 Ephemeral Correspondence

CTS 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.

2.3.5 Instant Messenger Correspondence

CTS Instant Messenger General Correspondence may be saved with logging function of Instant Messenger or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address.

2.3.6 Encrypted Communications

CTS encrypted communications should be stored in a manner consistent with CTS Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

2.3.7 Recovering Deleted Email via Backup Media

CTS 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.

3.0 Enforcement

Any employee found to be in violation this of any section of the Use or Retention policy may be subject to disciplinary action, up to and including termination of employment.

4.0 Definitions

Terms	Definitions
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.
Approved Encrypted email and files	Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within CTS is done via a license. Please contact the appropriate support organization if you require a license.
Approved Instant Messenger	The Jabber Secure IM Client is the only IM that is approved for use on CTS computers.
Individual Access Controls	Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use man chmod to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.
Insecure Internet Links	Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of CTS.
Encryption	Secure CTS 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.

Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Chain email or letter	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 directions 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 CTS or its customers' reputation or market standing.
Virus warning	Email containing warnings about viruses 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 CTS, who do not have a need to know that information.

5.0 Revision History

Revision Number	Date	Editor	Reason
2.0	1/16/2025	Aidan Schmeckpeper	Separated into library and prepared for future edits.
2.1	2/19/2025	Aidan Schmeckpeper	Merged “Use” and “Retention” policies into one cohesive policy with two sections.