
Introduction

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of email.
- To educate individuals using email with respect to their responsibilities associated with such use.

Purpose

The purpose of the [AGENCY] Email Policy is to establish the rules for the use of [AGENCY] email for the sending, receiving, or storing of electronic mail.

Audience

The [AGENCY] Email Policy applies equally to all individuals granted access privileges to any [AGENCY] information resource with the capacity to send, receive, or store electronic mail.

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email Policy

- The following activities are prohibited by policy:
 - ❖ Sending email that is intimidating or harassing.
 - ❖ Using email for conducting personal business.
 - ❖ Using email for purposes of political lobbying or campaigning.
 - ❖ Violating copyright laws by inappropriately distributing protected works.
 - ❖ Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
 - ❖ The use of unauthorized e-mail software.

- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
 - ❖ Sending or forwarding chain letters.
 - ❖ Sending unsolicited messages to large groups except as required to conduct agency business.
 - ❖ Sending excessively large messages
 - ❖ Sending or forwarding email that is likely to contain computer viruses.

- All sensitive [AGENCY] material transmitted over external network must be encrypted.

- All user activity on [AGENCY] Information Resources assets is subject to logging and review.

- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of [AGENCY] or any unit of the [AGENCY] unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the [AGENCY]. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."

- Individuals must not send, forward or receive confidential or sensitive [AGENCY] information through non-[AGENCY] email accounts. Examples of non-[AGENCY] email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

- Individuals must not send, forward, receive or store confidential or sensitive [AGENCY] information utilizing non-[AGENCY] accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers and cellular telephones.

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of [AGENCY] Information Resources access privileges, civil, and criminal prosecution.

Supporting Information

This Security Policy is supported by the following Security Policy Standards.

Reference # Policy Standard detail

-
- 3 All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

 - 6 The use of IR must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management.

 - 7 Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

 - 8 All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as if it were state property.

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications