E-mail Security Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose of this policy is to protect the confidentiality and integrity of sensitive information that may be sent or received via email.

Scope:

This policy applies to all <organization name>> workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by <<Organization Name>>. Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

<<Organization Name>> recognizes that using email without the use of an encryption mechanism is an insecure means of sending and receiving messages. <<Organization Name>> will evaluate emerging encryption solutions for email and implement them when one is found that is:

* Technically sound
* Reasonable to implement and use by workforce members
* Financially reasonable

Until a workable encryption mechanism is implemented, <<Organization Name>> will utilize the following guidelines regarding sending sensitive information via email:

* Emails containing sensitive information are permitted only when both the sender and receiver are members of <<Organization Name>>’s workforce and the e-mail stays within the confines of <<Organization Name>>’s local network. That is, both email addresses must end with “<<Organization Name>>.com. When sending sensitive information via email, care should be taken to send only the minimum necessary.
* Emails containing sensitive information may not be sent to any other person outside of <<Organization Name>>’s network.

<<Organization Name>> provided e-mail systems are intended for official and authorized purposes only. E-mail messages are considered by <<Organization Name>> to be company property. Therefore, e-mail equipment operated by or for <<Organization Name>> staff are subject to the same restrictions on their use as any other company furnished resource provided for use by members of the workforce.

Electronic information about an individual, such as a client or a patient, in an organized set of records, should be protected to the extent that a hard copy record is protected, and disclosed only when required for authorized purposes.

E-mail system administrators and others with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by appropriate <<Organization Name>> management officials. However, <<Organization Name>> officials will have access to e-mail messages whenever there is a legitimate purpose for such access, e.g., technical or administrative problems.

When e-mail is not in use, users are to exit the software to prevent unauthorized access.

Responsibilities:

All individuals identified in the scope of this policy are responsible for:

* Abide by the terms and guidelines set forth by this policy

The Security Officer is responsible for:

* Evaluating, on a periodic basis, emerging encryption solutions for email and implementing them when one is found the meets the criteria described in the policy section of this document
* Maintaining procedures and forms in support of this policy
* Monitoring and enforcing workforce compliance with this policy

Compliance:

Failure to comply with this or any other security policy will result in disciplinary actions as per the HR XXXXX Policy. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

Procedure(s): None

Form(s): None

References:

* The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
* International Standards Organization (ISO 27002).

Contact:

John Doe, Security Officer

1234 Anystreet

Anywhere, WY XXXXX

E: John.doe@anywhere.com

P: 307.XXX.XXXX

F: 307.XXX.XXXX

Policy History: Initial effective date: July 1, 2015