Security Awareness and Training Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to implement a security awareness and training program for all members of <<Organization Name>>’s workforce, including management.

<<Organization Name>> understands that “people”, not necessarily technology, are often the largest threat to the security of sensitive information in the organization.

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>>.

Policy:

<<Organization Name>> will ensure that all workforce members have been trained in and understand the security policies and procedures. In addition, all workforce members will be trained how to identify, report, and prevent potential security incidents.

Security training will be an ongoing activity at <<Organization Name>>. Periodic security reminders will keep workforce members up to date with new threats, such as computer viruses or “scams” to watch out for. The frequency and form these reminders take will be determined by the Security Officer but should include things like security-related flyers or posters in break rooms, reminders in paycheck stubs or emails, and verbal updates at staff meetings.

<<Organization Name>> will run anti-virus software on all computers that connect to the Internet and/or are networked together. Members of the workforce must be trained how to use the software and how to spot unusual activity that might indicate the presence of a virus. The anti-virus software must be kept up to date, as new viruses (and other types of malicious code) are discovered daily.

<<Organization Name>> will develop security policies to identify core activities in the areas of security reminders, protection from malicious software, log-in monitoring, and password management.

Responsibilities:

All workforce members are responsible for:

* Understanding and following all security related policies and procedures

The Security Officer is responsible for:

* Ensuring all workforce members understand and follow security related policies and procedures
* Maintaining an ongoing security awareness program at <<Organization Name>>
* Ensuring all workforce members understand and use the installed anti-virus software
* Keeping all anti-virus software up to date
* Leading compliance activities that bring <<Organization Name>> into compliance with regulatory requirements.

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