Portable Devices Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to secure the use of portable devices used by members of the workforce.

Scope:

This policy applies to all members of the workforce, including volunteers. The policy applies to all types of portable devices, including and not limited to laptops, notebooks, PDAs, smart phones, and any other mobile device that is capable to storing or transmitting sensitive information.

Policy:

Confidential or sensitive data must be accessed only on server systems. Sensitive information may only be stored on portable systems if appropriate encryption software authorized by the IT department is installed on the device. Any information stored on the portable system must be saved only in those folders that keep information encrypted.

Strong password controls must be implemented for all users of portable devices. This includes requirements for minimal password length (such as 8 characters, alphanumeric) and frequency of password changes (such as every 90 days).

When working on portable devices from a remote location, including from home, only secure connections must be used to access sensitive information. If wireless communication is used with portable devices then the device must be configured as defined by the IT department to ensure use of secure protocols.

Backups of information from portable devices must be conducted regularly and stored securely.

Employees must logoff and shut down portable devices with sensitive data before leaving the work space. Protection against malicious software should be in place and be kept up to date.

Devices must be configured to automatically logoff users according to Automatic Logoff Policy, XXXX.

Portable devices must not be left unattended. When not in use, portable devices should be locked away or special locks should be used to secure the equipment.

Responsibilities:

Employees are responsible for the security of portable devices they use for work. Special care should be taken to ensure that sensitive information is not compromised.

The Security Officer will ensure that key elements of this policy are included in annual training provided to all members of the workforce. The Security Officer will also include elements of this policy as security reminders sent to members of the workforce. If encryption software is installed on portable devices or if strong password controls are implemented then members of the workforce must be trained in this area.

The Security Officer is responsible for conducting random audits of portable systems to check for unauthorized or unsecured files.

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