Information Classification Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The Information Classification Policy is intended to assist employees of <<Organization Name>> make decisions regarding what information may and may not be released to the public or disclosed to any individual outside of 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.

Policy:

All <<Organization Name>> information will be organized into two main classes. These classes are “Public” and “Confidential.”

Public information is information that can be shared freely with anyone inside or outside of the organization without the possibility of negative consequences. Public information includes, but is not necessarily limited to:

* General information about <<Organization Name>> such as the mission statement
* Most marketing information

Confidential information includes all other information, such as sensitive information, (information that, when shared or disclosed, could possibly have a negative consequence). It is understood that there are varying levels of sensitive information, and the lengths employees should go to protect the information depends on the sensitivity.

<<Organization Name>> will rely on the professional judgment of the individual on a daily basis when using and disclosing confidential information. If an individual is unsure of the relative sensitivity of a piece of information, they could contact their supervisor or the Security Officer.

Confidential information includes, but is not necessarily limited to:

* Business information
* Financial information
* Operational information
* Most personnel information
* Student Data

If the sensitivity of the information is not readily apparent, the creator of the document may mark the document as “<<Organization Name>> Confidential” in a prominent location.

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

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