Unique User Identification Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to assign a unique name and/or number for identifying and tracking user identity.

Scope:

This policy applies to <<Organization Name>> in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications, as well as all facilities, which process, store or transmit sensitive information.

Policy:

Each individual that accesses sensitive information, such as sensitive information, via computer at <<Organization Name>> will be granted some form of unique user identification, such as a login ID. At no time will any workforce member allow anyone else to use their unique ID. Likewise, at no time will any workforce member use anyone else’s ID.

<<Organization Name>> will develop a standard convention for assigning unique user identifiers.

<<Organization Name>> will maintain a secure record of unique user identifiers assigned.

<<Organization Name>> will track individual activities and record events as required by policies such as Audit and Information System Activity Review.

Responsibilities:

The Security Officer will be responsible for ensuring the implementation of the requirements of Unique User Identification 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