Data Backup and Storage Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to create a retrievable, exact copy of sensitive information, when needed, before the movement of equipment.

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:

<<Organization Name>> will determine when backups are needed and this will be done prior to the movement of any required systems.

<<Organization Name>> will make an exact, retrievable copy of the data.

<<Organization Name>> will test the copy of the data to make sure the copy of the data is exact and retrievable.

<<Organization Name>> will store the backed up data in a secure location and ensure that the appropriate access controls are implemented to only allow authorized access to all such data.

Responsibilities:

The Security Officer will be responsible for ensuring the implementation of the Data Backup and Storage 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