Applications and Data Criticality Analysis

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to assess the relative criticality of specific applications and data in support of other contingency plan components.

Scope:

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

Policy:

<<Organization Name>> should assess the “critical” areas of the business, which would include:

* Critical business functions
* Critical infrastructure
* Critical sensitive information or records

The specific components of applications and data criticality analysis must include:

* Network architecture diagrams and system flowcharts that show current structure, equipment addresses, communication providers and system interdependencies.
* Identification and analysis of critical business processes surrounding sensitive information.
* Identification and analysis of key applications and systems used to support critical business processes.
* A prioritized list of key applications and systems and their recovery time objectives.
* Documented results of an analysis of the internal and external interfaces with key applications and systems.
* Adequate redundancies within the network infrastructure to reduce or eliminate single points of failure.
* Mitigating controls or work-around procedures in place and tested for single points of failure that are unable to be eliminated.

Responsibilities:

The Security Officer will be responsible for ensuring the implementation of the requirements of Applications and Data Criticality Analysis.

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