Network Security Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to secure communication devices and data on the <<Organization Name>> network.

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:

The standard for network protocols in the <<Organization Name>> infrastructure is TCP/IP.

<<Organization Name>> will:

* Use encryption as much as possible to protect data
* Use firewall(s) to secure critical segments
* Deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) on all critical segments
* Disable all services that are not in use or services that have use of which you are not sure
* Use wrappers around all services to log their usage as well as to restrict connectivity

Responsibilities:

The Security Officer will be responsible for ensuring that network protocols are configured securely.

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