Remote Access Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to <<Organization Name>>’s enterprise infrastructure to a ***reasonable and appropriate level***.

Scope:

This policy applies to <<Organization Name>> in its entirety, including all facilities and systems that process sensitive information. Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.

Policy:

The <<Organization Name>> remote access infrastructure must follow these guidelines:

* It is the responsibility of <<Organization Name>> employees, contractors, vendors and agents with remote access privileges to <<Organization Name>>'s corporate network to ensure that their remote access connection is given the same consideration as the user’s on-site connection to <<Organization Name>>.
* Secure remote access must be strictly controlled. Control will be enforced by using strong passwords.
* At no time should any <<Organization Name>> employee provide their login or e-mail password to anyone, not even family members.
* <<Organization Name>> employees and contractors with remote access privileges must ensure that their <<Organization Name>>-owned or personal computer or workstation, which is remotely connected to <<Organization Name>>'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
* <<Organization Name>> employees and contractors with remote access privileges to <<Organization Name>>'s corporate network must not use non-<<Organization Name>> e-mail accounts (for example, Hotmail, Yahoo, AOL), or other external resources to conduct <<Organization Name>> business, thereby ensuring that official business is never confused with personal business.
* Routers for dedicated ISDN lines configured for access to the <<Organization Name>> network must meet minimum authentication requirements of CHAP.
* Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
* Frame Relay must meet minimum authentication requirements of DLCI standards.
* Non-standard hardware configurations must be approved by the Security Officer.
* All hosts that are connected to <<Organization Name>> internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers.
* Organizations or individuals who wish to implement non-standard Remote Access solutions to the <<Organization Name>> production network must obtain prior approval from the Security Officer.

Responsibilities:

The Security Officer has the responsibility to ensure that all remote access connections are used based on policy requirements. The Security Officer must review related log files from key systems on a regular basis. The Security Officer must send reminders to all employees about remote access security.

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