**Remote Access Policy**

**1.0 Purpose**

The purpose of this policy is to define standards for connecting to ***<Company Name>'s*** network from any host. These standards are designed to minimize the potential exposure to ***<Company Name>*** from damages which may result from unauthorized use of ***<Company Name>*** resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical ***<Company Name>*** internal systems, etc.

**2.0 Scope**

This policy applies to all ***<Company Name>*** employees, contractors, vendors and agents with a ***<Company Name>***-owned or personally-owned computer or workstation used to connect to the ***<Company Name>*** network. This policy applies to remote access connections used to do work on behalf of ***<Company Name>***, including reading or sending email and viewing intranet web resources.

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, etc.

**3.0 Policy**

**3.1 General**

1. It is the responsibility of ***<Company Name>*** employees, contractors, vendors and agents with remote access privileges to ***<Company Name>'s*** corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to ***<Company Name>.***
2. General access to the Internet for recreational use by immediate household members through the ***<Company Name>*** Network on personal computers is permitted for employees that have flat-rate services. The ***<Company Name>*** employee is responsible to ensure the family member does not violate any ***<Company Name>*** policies, does not perform illegal activities, and does not use the access for outside business interests. The ***<Company Name>*** employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of ***<Company Name>'s*** network:
   1. *Acceptable Encryption Policy*
   2. *Virtual Private Network (VPN) Policy*
   3. *Wireless Communications Policy*
   4. *Acceptable Use Policy*
4. For additional information regarding ***<Company Name>'s*** remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

**3.2 Requirements**

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any ***<Company Name***> employee provide their login or email password to anyone, not even family members.
3. ***<Company Name>*** employees and contractors with remote access privileges must ensure that their ***<Company Name>***-owned or personal computer or workstation, which is remotely connected to ***<Company 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.
4. ***<Company Name>*** employees and contractors with remote access privileges to ***<Company Name>'s*** corporate network must not use non***-<Company Name>*** email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct ***<Company Name>*** business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the ***<Company Name>*** network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Remote Access Services must approve non-standard hardware configurations, and organization must approve security configurations for access to hardware.
9. All hosts that are connected to ***<Company 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. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to ***<Company Name>'s*** networks must meet the requirements of ***<Company Name>***-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the ***<Company Name>*** production network must obtain prior approval from Remote Access Services and IT department.

**4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Source:** <http://csirt.org/sample_policies/index.html>