Remote Access Policy

Free Use Disclaimer: This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.

Things to Consider: Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.

Last Update Status: Updated June 2014

1. Overview
See Purpose.

2. 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.

3. 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 DSL, VPN, SSH.

4. Policy
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>.

General access to the Internet for recreational use by immediate household members through the <Company Name> Network on personal computers is permitted. 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.

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:

- **Acceptable Encryption Policy**
- **Wireless Communications Policy**
- **Acceptable Use Policy**

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.

4.1 Requirements

4.1.1 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.

4.1.2 At no time should any <Company Name> employee provide their login or email password to anyone, not even family members.

4.1.3 <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.

4.1.4 <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.

4.1.5 Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

4.1.6 Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.

4.1.7 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.

4.1.8 Personal equipment that is used to connect to <Company Name>'s networks must meet the requirements of <Company Name>-owned equipment for remote access.

4.1.9 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 InfoSec.
5. Policy Compliance

5.1 Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes
- Acceptable Encryption Policy
- Acceptable Use Policy
- Password Policy
- Third Party Agreement.
- Wireless Communications Policy

7 Definitions and Terms
The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/
- Dual Homing
- Split Tunneling

8 Revision History

<table>
<thead>
<tr>
<th>Date of Change</th>
<th>Responsible</th>
<th>Summary of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2014</td>
<td>SANS Policy Team</td>
<td>Updated and converted to new format.</td>
</tr>
</tbody>
</table>