



Remote Access Policy Template

1.0 Purpose

To provide our members a template that can be modified for your company's use in developing a Remote Access Policy. This policy compliments the NCSS's VPN Policy, as both documents are necessary for implementing a safe Remote Access policy for your company.

The purpose of this policy is to define the rules and requirements for connecting to our organization's network from any host (cell phones, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

2.0 Policy

It is the responsibility of our company's employees, contractors, vendors and agents with remote access privileges to our corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

General access to the Internet for recreational use through our company network is strictly limited to our employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing our network from a personal computer, Authorized Users are responsible for preventing access to any company computer resources or data by non-Authorized Users.

Performance of illegal activities through our company network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see our Acceptable Use Policy. Authorized Users will not use our networks to access the Internet for outside business interests. For additional information regarding our remote access connection options, including how to obtain a remote access login/VPN, anti-virus software, troubleshooting, etc., see our IT technical lead.

3.0 Connection Procedures

1. Secure remote access will be strictly controlled with encryption through our Virtual Private Networks (VPNs) and strong pass-phrases. For further information see our company's Encryption Policy and the Password Policy.

Still have questions, need help?

Contact us at our "Ask-an-Expert" service, web@thencss.org or visit us at the link below.



Remote Access Policy Template

2. Authorized Users shall protect their login and password, even from family members.
3. While using our corporate owned computer to remotely connect to our corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
4. Use of external resources to conduct our company business must be approved in advance by the appropriate business unit manager.
5. All hosts that are connected to our company's internal networks via remote access technologies must use the most up-to-date anti-virus software this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement with our partner.
6. Personal equipment used to connect to our company's networks must meet the requirements of company owned equipment for remote access - and approved by your business unit leader.

4.0 Compliance

Our company's IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring (if applicable), business tool reports, internal and external audits, and/or inspection. The results of this monitoring will be provided to the appropriate business unit manager.

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

5.0 Exception to Policy

Any exception to the policy must be approved by the business unit manager.

6.0 Other Applicable Policies

- Website Terms of Use
- Password Policy
- Acceptable Use Policy
- Your Organization's Information Security Policy
- VPN Policy
- Encryption Policy

Still have questions, need help?

Contact us at our "Ask-an-Expert" service, web@thencss.org or visit us at the link below.



Remote Access Policy Template

7.0 Applicability

This policy applies to all company employees, contractors, vendors and agents with a company owned or personally-owned computer or workstation used to connect to our network. This policy applies to remote access connections used to do work on behalf of company, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to our company's networks.

8.0 References

Some useful references to learn more:

<https://www.sans.org/security-resources/policies/retired/pdf/virtual-private-network-policy>

<https://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy>

<https://resources.infosecinstitute.com/best-practices-for-securing-remote-access/#gref>

<https://www.smartsheet.com/effective-remote-access-policy>

<https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>

Still have questions, need help?

Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.