Version 1.0

Date: 10/5/2019

Virtual Private Network Policy Template

1. 0 Purpose

To provide our members a template that can be modified for your company’s use in developing a Virtual Private Network (VPN) Policy. This policy compliments the NCSS’s Remote Access Policy, as both documents are necessary for implementing a safe remote access policy for your company.

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the <Organization Name> corporate network.

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 use a VPN enabled connection. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Approved employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of our VPN, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees if applicable. Further details may be found in the Remote Access Policy.

3.0 Connection Procedures

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to our company’s internal networks.

2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase (See Password Policy for details).

3. When actively connected to our corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel all other traffic will be dropped.

4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

5. VPN gateways will be set up and managed by our company’s operational groups.

6. All computers connected to our internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.

7. VPN users will be automatically disconnected from our company's network after <10 minutes or select another time> of inactivity. The user must then must logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.

9. Users of non-corporate owned equipment must configure the equipment to comply with our company's VPN and Network policies.

10. Only company approved VPN clients may be used.

11. By using VPN technology with personal equipment, users agree and understand that their machines are a de facto extension of company's network, and as such are subject to the same rules and regulations that apply to company owned equipment, i.e., their machines must be configured to comply with company's Information Security Policies.

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
- Remote Access Policy
- Encryption Policy

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.