SecOps® Solution

Remote Access Policy

Free Use Disclaimer: *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new or updated version of this one.*

1. Overview

A remote access policy is defined as a document containing the guidelines for connecting to a company's network from a location other than the office. As remote work continues to gain popularity, it is one technique to help secure corporate data and networks. It is especially helpful for large firms with geographically distributed people logging in from unsafe sites like their home networks. This policy helps to mitigate external risks to the best of our ability.

2. Purpose

This policy's objective is to specify standards for connecting to **<Company Name>** network from any host. These standards are designed to minimize the potential security exposure to **<Company Name>** from damages that may result from the unauthorized use of **<Company Name>** resources. Damages can include the loss of private or business information, intellectual property, harm to one's reputation, harm to vital internal systems, fines, or other financial obligations resulting from those losses. It aims to ensure that a security posture is maintained that will reduce the chances of unauthorized access to the information.

3. Scope

All employees, including permanent, temporary, consultants, and contractors of **<Company Name>** must follow this policy. This policy covers any and all technical implementations of remote access used to connect to **<Company Name>** networks.

4. Policy

Employees, contractors, suppliers, and agents of **<Company Name>** with remote access rights to the corporate network of **<Company Name>** shall guarantee that their remote access connection is treated with the same care as the user's on-site connection to **<Company Name>**.

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

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

4.1 Requirements:

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Acceptable Encryption Policy and the Password Policy.
- Authorized Users shall protect their login and password, even from family members.
- While using a **<Company Name>**-owned computer to remotely connect to **<Company Name>**'s 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.
- Use of external resources to conduct **<Company Name>** business must be approved in advance by InfoSec and the appropriate business unit manager.
- 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.

- Personal equipment used to connect to **<Company Name>**'s networks must meet the requirements of **<Company Name>**-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to **<Company Name>** Networks.

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 inspection, and will provide feedback to the policy owner and appropriate business unit manager.

5.2 Exceptions

Any exception to the policy must be approved by Remote Access Services and 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

For information on how to protect your information when using remote access to the corporate network and what constitutes appropriate usage of the network, please study the following policies:

- Acceptable Encryption Policy
- Password Policy
- Third Party Agreement
- Hardware and Software Configuration Standards for Remote Access to **<Company Name>** Networks.

7. Revision History

Version	Date	Description
1.0	26-10-2022	Initial Policy