Remote Access Policy

1. Overview

Remote access to our corporate network is essential to maintain our team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. We must mitigate these external risks the best of our ability.

2. Purpose

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

3. Scope

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

4. Policy

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

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

Authorized Users will not use noesya networks to access the Internet for outside business interests. For additional information regarding noesya remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., ask to the Security Team.

5. Requirements

A. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Password Policy.

B. Authorized Users shall protect their login and password, even from family members.

C. While using a noesya-owned computer to remotely connect to noesya 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.

D. Use of external resources to conduct noesya business must be approved in advance by the Security Team and the appropriate business unit manager.

E. All hosts that are connected to noesya 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.

F. Personal equipment used to connect to noesya networks must meet the requirements of noesya-owned.

6. Policy Compliance

A. Compliance Measurement

The security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, internal audits, and feedback to the policy owner..

B. Non-Compliance

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

7. Related Policies

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of noesya network:

- Acceptable Use Policy
- Password Protection Policy

8. Revision History

1.0 Date of change: 01/09/2021 - Responsible: Technical team - Summary of Change: Initial release