

Remote Access Policy

# Overview/Purpose

The purpose of this policy is to define standards for connecting to <**Utility Name**>'s network from external networks.

# Scope

This policy applies to all employees, contractors, vendors and agents with a <**Utility Name**>-owned or personally-owned computers or mobile devices used to connect to the <**Utility Name**> network. This policy applies to remote access connections used to do work on behalf of <**Utility 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 VPN, and VPN over SSH.

# Policy

It is the responsibility of employees, contractors, vendors and agents with remote access privileges to the company's network to ensure that their remote access connection meets all requirements outlined in this policy.

Remote access by individuals without specific company authorization is prohibited. The employee associated with a remote access account bears responsibility for any misuse.

Please review the following policies for details of protecting information when accessing the network via remote access methods, and acceptable use of <**Utility Name**>'s network:

* Encryption Policy
* Network Configuration Standard
* Acceptable Use Policy

## Requirements

* + 1. Secure remote access must be strictly controlled with use of Multi Factor Authentication or certificates deployed by a MDM (Mobile Devices Management) system.
    2. At no time should any employee provide their remote access credentials to anyone, including family members.
    3. All systems that are connected to internal networks via remote access technologies must use the most up-to-date version available of an anti-virus software package approved by the IT Manager.
    4. Authorized employees may also access the internal network from mobile devices. In this case, Multi Factor Authentication is required, and the mobile device must have the MDM application deployed.
    5. Third party connections must comply with requirements as stated in the *Third Party Access* Policy.
    6. Organizations or individuals who wish to implement non-standard Remote Access solutions to the production network must obtain prior approval from <**person or group responsible for policy**>.
    7. Wireless access within the <**Utility Name**> facilities shall be treated as remote access.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adapted from “Cyber Security Policy Framework” (<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
  Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.
* Adapted from “Remote Access Policy” (<http://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy>)
* PCI DSS Requirements (<https://www.pcisecuritystandards.org/document_library>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| CIO | **CEO/GM** |  | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |