

Third Party Access Policy

# Overview/Purpose

This policy covers outside entities or individuals, such as software providers, hardware technical support personnel, or any other outside personnel, known as Third Parties, who have a need to access **<Utility Name>**-owned IT systems or applications in order to provide a service to the utility.

The purpose of this policy is to define standards for connecting to networks from any host. These standards are designed to minimize the potential exposure to the company from damages which may result from unauthorized use of resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

# Scope

This policy applies to all Third Parties with a **<Utility Name>** owned or personally owned computer or workstation used to connect to the 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, or any other activity involving the utility's systems or applications. Remote access implementations that are covered by this policy include, but are not limited to VPN, VPN over SSH, or other means.

# Policy

## General Requirements

It is the responsibility of Third Parties with remote access privileges to the network to ensure that their remote access connection meets all security policies and requirements. General access to the Internet via thenetwork for recreational use, or unrelated outside business interests, is not permitted. The Third Parties, and the individuals which they employ, are responsible for the consequences should the access be misused. Please review the following policies for details of protecting information when accessing the network via remote access methods, and acceptable use of the network:

* *Encryption* Policy
* *Remote Access* Policy
* *Acceptable Use* Policy

## Requirements

* + 1. Third party connections must comply with requirements as stated in the Third Party Agreement, to be signed by any Third Party accessing **<Utility Name>** Systems or Applications.   
        [***NOTE:*** *Not included as part of this package.]*
    2. The IT manager should use the Third Party Access Procedure for granting Third Party access to the network.
    3. Connectivity details, restriction and access termination is documented in the Third Party Access Form.
    4. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with a strong passphrases.
    5. At no time should any employee provide their User Account or email password to anyone, including family members.
    6. Third Parties with remote access privileges to the network must not use non-**<Utility Name>** email accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct company business, thereby ensuring that official business is never confused with personal business.
    7. Reconfiguration of equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
    8. Personal equipment that is used to connect to networks must meet the same requirements as utility-owned equipment for remote access.
    9. 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**>.

# 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 SANS “Remote Access Policy” template( <https://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **CFO**  **COO**  **Legal Department** | **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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |