

Acceptable Use Policy

# Overview/ Purpose

**<Utility Name>** is committed to protecting its employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. All systems and accounts, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet Web browsing, and FTP, are the property of the utility. These systems and accounts are to be used for business purposes in serving the interests of the company, and our customers in the course of normal operations, except where incidental personal use is explicitly permitted. **<Utility Name>**’s intentions in publishing an Acceptable Use Policy are not to impose restrictions that are contrary to **<Utility Name>**’s established culture of openness, trust and integrity.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every system user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment and the Information Technology (IT) infrastructure at. These rules are in place to protect the employees and **<Utility Name>.** Inappropriate use exposes the utility to risks including computer malware attacks, compromise of network systems and services, and legal/compliance issues. The policy balances the employee’s ability to benefit fully from information technology with the company’s need for secure and effectively allocated IT resources.

# Scope

This policy applies to employees, contractors, consultants, temporaries and other workers, including all personnel affiliated with third parties. This policy applies to all equipment, software and/or applications that is owned, leased, or used by **<Utility Name>**.

# Policy

## General Use and Ownership

* + 1. While the network administration team seeks to provide a reasonable level of privacy, users should be aware that data they create on corporate systems remains the property of the company.Because of the need to continually monitor the internal network in order to protect **<Utility Name>**’s IT resources and information, management cannot guarantee the confidentiality of personal information stored on any device belonging to the utility or in files on the network.
    2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of company systems and networks, unless such personal use is otherwise defined in overall company policies. In the absence of such policies, Company owned IT equipment, computers, networks, and related services may be used for incidental personal use purposes provided that:
* Usage is reasonable and does not interfere with work productivity.
* Usage does not directly or indirectly interfere with business operations, IT facilities or electronic mail services.
* Usage does not burden the utility with noticeable incremental cost.

If there is any uncertainty as to what constitutes acceptable personal use, employees should consult their supervisor or manager, who will make the final determination.

* + 1. Since all Internet, network, and system activities may be monitored, all personnel accessing such systems shall have no expectation of privacy.

## General Use and Ownership

* + 1. Users may not encrypt any emails without obtaining written permission from their supervisor and **<person or group responsible for policy**>. If approved, the encryption key(s) must be made known to **<person or group responsible for policy>.**
    2. Data residing on corporate IT systems may be classified as either confidential or not confidential, as defined by the company's *Data Classification* Policy. Examples of confidential information include but are not limited to: company private, corporate strategies, sensitive competitive information, trade secrets, specifications, and customer details and lists. Employees should take all necessary steps to prevent unauthorized access to this information.
    3. For security, network maintenance, and policy compliance purposes, authorized individuals may monitor equipment, systems and network traffic at any time, per the *System Logging and Monitoring* Policy.
    4. Employees must use extreme caution when opening email attachments received from unknown senders which may contain various forms of malware. Although **<Utility Name>** utilizes Anti-Virus software on each workstation and server {as well as filtering all inbound email through an outside security service,} some unsafe attachments may still find their way through the defenses. If attachments are received that were not expected, their validity should be confirmed with the sender via phone, prior to opening them. If any questions or uncertainty exist, please contact **<person or group responsible for policy>** prior to opening the attachment.
    5. Because information contained on portable and laptop computers is especially vulnerable, special care should be exercised to protect both the computer and its information.
    6. Employees shall not use company email, or other facilities to post to news groups, message boards, or websites unless the posting is in the course of assigned business duties.

## Passwords

Please refer to thePassword Policy.

## Anti-Virus Protection and Prevention

All workstations will be equipped with anti-virus software that cannot be disabled by non-IT staff members. Employees will be educated about safe anti-malware practices such as, but not limited to;

* Opening unexpected attachments or following links included in emails
* Downloading files from unknown sources
* Deleting spam, chain mails, junk emails
* NOT trusting any source for virus protection patches than those provided by the IT Department.

## Unacceptable Use

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

### System and Network Activities

* Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal, or international law, while utilizing company-owned resources.
* Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by **<Utility Name>**.
* Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, or the installation of any copyrighted software for which the utility or the end user does not have an active license.
* Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question.
* Introduction of malicious programs into the network or server (e.g., viruses, worms,, or other forms of malware)
* Using company computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
* Making fraudulent offers of products, items, or services originating from any company account.
* Making statements about warranty, expressly or implied, unless it is a part of assigned job duties.
* Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an authorized user, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of assigned duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service (DOS), and forged routing information for malicious purposes.
* Port scanning or security scanning is expressly prohibited unless prior notification to **<person or group responsible for policy>** is made.
* Executing any form of network monitoring which will intercept data not intended for the intercepting employee, unless the activity is a part of the employee’s assigned duties.
* Circumventing user authentication or the security of any computer, network, or account.
* Interfering with or denying service to any user (for example, denial of service attack).
* Using any program/script/command, or sending messages of any kind with the intent to interfere with, or disable, a user’s usage of any system, network, or application, via any means.
* Providing information about, or lists of, employees to parties outside **<Utility Name>** without Human Resources Department approval.

### Email and Communications Activities

The Email system is the property of the utility, and as such shall not be misused in any way, including but not limited to the following:

* Sending unsolicited Email messages, including the sending of “junk email” or other advertising material to individuals who did not specifically request such material (spam), unless part of a company-approved targeted marketing campaign.
* Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
* Sending or forwarding inappropriate emails, including any of the following: disruptive or offensive messages, still images, audio, or video images, including but not limited to offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. If you receive an email of this nature, promptly notify your immediate supervisor or manager.
* Forging or attempting to forge email messages.
* Disguising or attempting to disguise your identity when sending email.
* Sending email messages using another person’s e-mail account unless authorized to do so.
* Copying a message or attachment belonging to another user without permission of the originator.
* Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
* Posting the same or similar non-business-related messages to large numbers of Usenet Newsgroups or message boards.

*For additional information please refer to the* the *E-Mail Use Policy*

### Internet Access Activities

The following uses of the Internet, either during working hours or personal time, using company equipment or facilities, are strictly prohibited:

* Accessing, retrieving, or printing text and graphical information which exceeds the bounds of generally accepted standards of good taste and ethics.
* Using the Internet to access other systems for which the user has no authorization.
* Using Internet or Internet connections to access or transfer information that is in violation of local, state, federal, international, or copyright laws, or in a way that contradicts the intent or spirit of these policies and procedures.
* Engaging in personal commercial activities on the Internet, including offering services or merchandise for sale.
* Engaging in any activity which would compromise the security of any company computer or system.
* Endorsing any product or services, participating in any lobbying activity, or engaging in any political activity. The prohibition against engaging in any political activity or fundraising activity does not apply to employees that have authorization.
* Initiating non-work-related Internet sessions using company information resources from remote locations. That is, employees shall not connect into company resources from home or other noncompany locations for the purpose of participating in non-job-related Internet activities.
* Engaging in the transmittal of **<Utility Name>** information or data for non-business purposes and/or personal gain or benefit.

*For additional information please refer to the Internet Access 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 “Acceptable Use Policy”  
  (<http://www.sans.org/security-resources/policies/general/doc/acceptable-use-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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |