

Internet Access 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. This Internet Access Policy defines the acceptable use of the Internet by employees, contractors, consultants, temporaries and other workers, including all personnel affiliated with third parties, while using utility-owned or leased equipment, facilities, Internet addresses, or domain names registered to **<Utility Name>**. The intent for publishing an Internet Access Policy is not to impose restrictions that are contrary to established culture of openness, trust and integrity.

# Scope

This policy is intended to detail the rules of conduct for Internet use from a **<Utility Name>** computer or through corporate network and applies to all employees, contractors, consultants, temporaries and other workers, including all personnel affiliated with third parties.

# Policy

Access to the Internet is available to employees, contractors, subcontractors, and business partners, whose duties require it for the conduct of company business. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy. Internet access may also be limited by user, to specific domains and websites or during predetermined hours, at management's discretion.

## Acceptable Use

**<Utility Name>** provides Internet access to facilitate the conduct of company business. Occasional and incidental personal Internet use is permitted for individuals whose duties otherwise require Internet access, if such use does not interfere with their work, the company’s ability to perform its mission, does not directly or indirectly interfere with business operations, IT facilities or electronic mail services, and meets the conditions outlined in official company policies.

## Prohibited Use

Prohibited Internet activities, whether during normal working hours or on personal time, using company equipment include, but are not limited to, the following:

* Browsing explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that the company has determined to be inappropriate.
* Accessing, retrieving, or printing text and graphical information which exceeds the bounds of generally accepted standards of good taste and ethics.
* Posting, sending or acquiring sexually explicit or sexually oriented material, hate based material, hacker-related material, or other material determined by **<Utility Name>** to be inappropriate.
* Posting or sending sensitive information outside of the company without management authorization.
* Using other services available on the Internet such as File Transfer Protocol (FTP) or Telnet, on systems for which the user does not have a named account.
* Posting commercial announcements of advertising material without management authorization.
* Promoting or maintaining a personal or private business, including offering services or merchandise for sale.
* Receiving news feeds and push data updates, unless the material is required for company business.
* Accessing or transferring information that is a violation of local, state, federal, or international copyright laws, or that contradicts the intent and spirit of these policies or procedures.
* Downloading any applications or software that are not specifically authorized by **<IT Manager>**.
* Engaging in any activity, which would compromise the security and integrity of any company computer or system.
* Engaging in any fund raising activity, endorsing any product or services, participating in any lobbying activity, or engaging in any political activity without management authorization.
* Downloading any file from the Internet without prior approval, unless the download is from an authorized business partner. All requests will be sent through <**person or group responsible for policy**> to verify the source and security of the download. The access may be approved for only a single download or the user may be granted permanent download rights, depending on the business requirements. Once download access is granted, all aspects of this policy apply. Users are not to download screen savers, animated cursors, weather alert programs or other software programs from the Internet that can introduce spyware, ad-ware, and viruses or impact computer performance.

## User Responsibilities

Use of computer equipment and Internet access to accomplish job responsibilities will always have priority over incidental personal use. To avoid capacity problems and to reduce the susceptibility of information technology resources to malware, Internet users shall comply with the following guidelines:

* Files obtained via the Internet may only be stored on individual PC hard drives, or on file server shares, after they have been scanned for viruses.
* Video and voice files may not be downloaded from the Internet except when they will be used to serve an approved business function.
* Streaming Video and Music greatly impact corporate network bandwidth and access speeds and may not be initiated except when they will be used to serve an approved business function.
* Users shall follow existing security policies, and procedures in the use of Internet services, and shall refrain from any practices, which might jeopardize computer systems and data files, including but not limited to malware attacks, when downloading files from the Internet.
* It is suggested that users learn about, and adhere to Internet etiquette, customs, and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
* Users shall conduct themselves in a way that reflects positively on **<Utility Name>**, since they are identified as company employees on the Internet.

## Expectation of Privacy

The computers,computer accounts, and network and Internet resources that are provided for users are intended to assist them in the performance of their jobs. Users should not have expectation of privacy while using any such resources. Users of the Internet should be aware that most sessions on the Internet are not private.

## System Monitoring

**<Utility Name>** has the right to monitor any and all aspects of its computer systems and networks, including but not limited to, adherence to the Internet Access policy. Circumvention of any monitoring software or tools is prohibited and is subject to the same penalties as any other violation of the Internet access policy.

## <Utility Name> Liability

**<Utility Name>** has no liability for any issues employee may experience with personal accounts (banking for example) while accessing Internet from company network or using company mobile devices.

# 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 “Internet Usage Policy”  
  (http://www.sans.org/security-resources/policies/retired/doc/internet-usage-policy)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |