

Email 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. This email Policy defines the proper use of the electronic mail system (Email), and the uses of it that **<Utility Name>** deems as acceptable and unacceptable. Users shall make every effort to prevent tarnishing the utility’s public image and themselves. When email is sent out from **<Utility Name>**, the general public will tend to view that message as an official policy statement from the company. **<Utility Name>**’s intentions in publishing an Email Use Policy are not to impose restrictions that are contrary to **<Utility Name>**’s established culture of openness, trust and integrity.

# Scope

This policy is intended to detail the rules of conduct for Email sent from a **<Utility Name>** Email address or through the company’s Email server, and applies to all employees, contractors, consultants, temporaries and other workers, including all personnel affiliated with third parties.

# Policy

## Prohibited Use

The Email system referenced in this policy is the property of **<Utility Name>** and shall not be used for the creation or distribution of any of the following:

* Sending or forwarding Emails consisting of any of the following: disruptive or offensive messages, including but not limited to offensive comments about race, gender, color, disabilities, age, sexual orientation, pornography, obscenity, religious beliefs and practice, political beliefs, or national origin. If you receive an Email of this nature, notify your immediate supervisor.
* Forging or attempting to forge Email messages.
* Disguising or attempting to disguise your identity when sending Email.
* Sending Email using another person’s account.
* Sending chain letters or offensive joke emails from a company Email account.
* Forwarding of company confidential messages to external Email addresses.
* Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.
* Accessing copyrighted information in a way that violates copyright laws.
* Breaking into the company's or another organization’s systems, or unauthorized use of a password/mailbox.
* Transmitting unsolicited commercial or advertising material unless part of a company-approved targeted marketing campaign.
* Undertaking deliberate activities that waste staff effort or networked resources.
* Introducing any form of computer virus or malware into the corporate network.

Email generated and sent from a **<Utility Name>** Email account should be limited to business content only. Emails shall not contain content, signature lines, or images promoting unsolicited personal views on social, political, religious or other non-business related matters.

## Best Practices

**<Utility Name>** considers Email as an important means of communications and recognizes the importance of proper Email content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an Email as they would for any other communication. Therefore, the company requires users to adhere to the following guidelines.

### Writing Emails:

* Write well-structured Emails, and use short, descriptive subjects.
* **<Utility Name>**’s Email style is informal. Use of common salutations is acceptable such as “Hi” or “Dear” and the name of the person, and ending with “Best Regards”.
* Signatures should include pertinent information relative to your job classification such as your name, job title, company name, and company logo’s only. A disclaimer will be added underneath your signature, as described below. Signature lines shall not contain statements conveying religious, political, or other such references.
* Users should spell check all emails prior to sending. This can be set to be performed automatically by most Email programs.
* Do not send unnecessary attachments. Compress attachments larger than 200K before sending.
* Do not write in ALL CAPITAL LETTERS.
* Do not use Blind Carbon Copy (bcc ) fields unless the bcc recipient is aware you will be copying the message to him/her and knows what action, if any, to take. The bcc recipient should be aware that they were copied without other recipient’s knowledge.
* If you forward Emails, state clearly what actions you expect the recipient to take.
* Only send Emails for which the content could be displayed publicly. If they cannot be displayed publicly in their current state, consider rephrasing the Email or using another means of communication.
* Only mark Emails as important if they really are important.
* Don’t set every Email to require a read receipt, only those that really require it.  
  <IT Manager can add guidelines as to what kind of Emails requires a read receipt>

### Replying to Emails:

* Emails should be answered in a timely manner.
* Users should endeavor to answer priority Emails as soon as possible.
* Priority Emails are Emails from customers and business partners.

## Personal Use

**<Utility Name>** Email services may be used for incidental personal purposes, provided that:

* Usage is reasonable and does not interfere with work productivity.
* Non-work related Email is saved in a separate folder from work-related Email.
* Such use does not directly or indirectly interfere with business operations, IT facilities or Email services.

It is recommended that anyone using Email for personal reasons have a separate Internet Email account such as Google Gmail, Yahoo Mail, or Hotmail. This will put fewer burdens on the **<Utility Name>** Email servers allowing the system to work more efficiently.

## Conducting <Utility Name> business using personal Email accounts

No business activities related to **<Utility Name>** will be conducted using a personal email account. All company business involving the sending or receipt of Email will take place using as assigned company Email account.

## Email Retention

Email retention is subject to the Data Retention Policy.

## Expectation of Privacy

The Email accounts and systems provided for company users are intended to assist them in the performance of their jobs. Users should not have any expectation of privacy while using **<Utility Name>**’s Email system.

## Encryption

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>**.

## Disclaimer

The following disclaimer will be added to each outgoing Email:

***Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, copy, use, disclosure, or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply Email and destroy all copies of the original message.***

# 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>

# 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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |