# Ameren Email Policy

## 1.0 Purpose

This policy is to ensure the proper use of Ameren's electronic mail (email) systems and to make users aware of what Ameren considers acceptable use of its email systems

## 2.0 Scope

This policy applies to all Ameren companies, employees, contractors, consultants, temporary employees, and other individuals at Ameren, including workers affiliated with third parties who use Ameren email systems, which include Internet, voice mail, and email. Hereafter, referred to as "Privileged User".

## 3.0 Policy Requirements

### 3.1 Ameren Property

All messages generated by Ameren's email systems are the property of Ameren unless third parties have noted copyrights or other rights on the messages.

### 3.2 Authorized Usage

Privileged Users are to use Ameren's email systems for job-related purposes. Personal use is permissible so long as:

a. It does not consume more than a trivial amount of system resources;

b. It does not interfere with Privileged User productivity; and

c. It does not preempt any business activity.

d. It is not used for purposes, such as producing or distributing "chain mail"; operating a business; soliciting for personal, political, or religious causes; or for outside organizations.

e. Messages comply with and are subject to all Ameren policies, including those relating to harassment, discrimination and workplace violence.

f. Individual Business Lines or departments may develop and implement a more stringent policy with regard to personal use.

### 3.3 Privileged User Accountability

Privileged Users must never share or reveal individual passwords to anyone else. Revealing a password exposes the Privileged User to responsibility for the actions of other parties.

### 3.4 Privileged User Identity

Misrepresenting, obscuring, suppressing, or replacing another Privileged User's identity on an email system is forbidden. A Privileged User's name, email address, organizational affiliation, and related information included with electronic messages, must reflect the actual originator of the messages. The Ameren Corporate Email signature should be used on all email messages.

**3.5** Use Only Ameren Email Systems

Unless there is an Information Security approved business reason, Privileged Users must not use their personal email accounts such as Hotmail, Yahoo, or other internet service provided email while on Ameren computing resources, but rather, use authorized Ameren email software (e.g., Microsoft Outlook, Microsoft Outlook Web Access [OWA]).

**3.6** Contractors and Consultants Use of Email Systems

Contractors and consultants may use their own company email systems if approved in advance by Information Security. However, they must adhere to all Ameren policies when doing so.

**3.7** Use of Encryption Programs

Ameren's email systems are not encrypted by default. If sensitive information must be sent by email systems, encryption or similar technologies to protect the information must be employed. Privileged Users should use the current Ameren corporate encryption solution as a relatively simple way to send sensitive information in encrypted form over the Internet. Privileged Users must not use encryption for any production email system unless a backup key or a key escrow system has been established with the cooperation of Information Security. If there are questions, contact Information Security or the IT Service Desk.

**3.8** No Guaranteed Message Privacy

Ameren does not guarantee, nor should Privileged Users have any expectation of the privacy of electronic communications. Privileged Users should exercise care regarding the content of electronic communications. Electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, electronic communications can be accessed by people other than the intended recipients in accordance with the provisions of this policy.

**3.9** Management Review

At any time and without prior notice, Ameren Management may examine email communications, including those previously deleted. Such communication may be monitored, searched, reviewed, disclosed, or intercepted by Ameren for any purpose, including the following: to monitor performance, to ensure compliance with Ameren policies, to prevent misuse of the systems, to troubleshoot hardware and software

problems, to comply with legal and regulatory requests for information, to investigate the disclosure of confidential business or proprietary information, and to investigate conduct that may be illegal or adversely affect Ameren or its employees.

**3.10** Intellectual Property Rights

In accordance with the laws of copyrights, patents, and trademarks, Privileged Users must repost or reproduce material only after obtaining permission from the source, quote material from other sources only if these other sources are properly identified, and reveal internal Ameren information only if the information has been approved for public release.

**3.11** Attachments

Attachments to electronic communications may contain a virus or may cause damage to a Privileged User's computer. Although virus detection software scans attachments received from third parties, Privileged Users should only open attachments from known and trusted senders. Privileged Users should limit the use of attachments to external services and should compress attachments utilizing 7-Zip or similar data compression products before sending. Users cannot send an email attachment larger than 25 Mb.

**3.12** Message Forwarding

Unless the information owner/originator agrees in advance, or the information is clearly public in nature, Privileged Users must not forward email to addresses outside Ameren's network. Blanket forwarding of email messages to any parties outside of Ameren is prohibited unless permission from Information Security is obtained in advance.

**3.13** Unsolicited Email

Ameren prohibits Privileged Users from using Ameren's email systems to transmit unsolicited bulk email advertisements, commercial messages, or spam. When Privileged Users receive unwanted and unsolicited email, they should not respond directly to the sender. Instead, they should click the Junk button in Outlook to report the email. Furthermore, Ameren prohibits Privileged Users from sending large quantities of unsolicited email to internal or external users

**3.14** Handling Security Warnings

Privileged Users must promptly report such things as security alerts, warnings, reported vulnerabilities, and viruses, to the IT Service Desk. Many of these mail messages are hoaxes. Privileged Users must not open any attachments associated with these mail messages and are prohibited from utilizing Ameren's email systems to forward these electronic notices to internal or external users.

**3.15** Purging Electronic Messages

Email systems are not intended for the archival storage of important information. Privileged Users must regularly move important information from email message files to word processing documents, databases, and other files. Emails must not be stored outside of the Ameren email system. See the Ameren Email and Voice Mail Retention Policy for more information regarding the purging of electronic messages.

## 4.0 Enforcement

Management may terminate a Privileged User's email account for violation of this policy. Moreover, violators of this policy may be subject to disciplinary action, up to and including termination. Violations such as accessing child pornography may subject the employee to criminal prosecution. This version supersedes all previous email policies. Ameren Corporation reserves the right to modify or change the policy at any time.

## 5.0 Corporate Responsibility

For further information regarding the content or administration of this policy, contact the Information Security group. The Information Security group must approve any exceptions to this policy in advance.

## 6.0 Definitions

**6.1** **Data compression** -The process of encoding data to take up less storage space.

**6.2** **Chain mail** -A chain letter.

**6.3** **Encryption** -The reversible transformation of data from its original format to a difficult-to-interpret format as a mechanism for protecting its confidentiality, integrity, and authenticity.

**6.4** **Internet service provider** -An organization that provides access to the Internet (ISP).

**6.5** **Password** -Any secret string of characters used in conjunction with a user-ID to identify a computer user (e.g., Mhal4$W).

**6.6** **Spam** -A variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing messages.

**6.7** **Virus** -A program that infects a computer by attaching itself to another program and propagating itself when that program is executed.

**6.8** **7-ZIP** - A utility for compressing and uncompressing files.