Internet/Intranet Usage Policy

1.0 Purpose

The wide array of new resources, new services, and interconnectivity available via the Internet introduce new business opportunities as well as new security and privacy risks. This document outlines Ameren's policy regarding appropriate Internet / Intranet usage.

2.0 Scope

This policy applies to all Ameren companies, employees, contractors, consultants, temporary employees, and other individuals at Ameren, including those workers affiliated with third parties with access to Ameren's Internet / Intranet. Throughout this policy, the word "Privileged User" will be used collectively to refer to all such individuals.

3.0 Policy Requirements

3.1. Access Control

3.1.1. Browser User Authentication

Ameren provides Internet access to authorized Privileged Users for purposes of Company business. Privileged Users accessing the Internet must have a unique user-ID and password. Users must not save passwords in web browsers or email clients. Instead, users must provide passwords each time a browser or email client is invoked.

3.1.2. System Standards

Privileged Users must not alter the security configuration or install software that alters the security configuration of the web browser without approval from Information Security.

3.1.3. Management Approval

An employee's department manager must approve any request for an Internet connection. If an individual transfers to another department, their new department manager must review and approve their Internet access.

3.1.4. Internet Service Providers

Privileged Users must not employ Internet Service Provider (ISP) accounts and dial-up lines to access the Internet with Ameren computers. Instead, all Internet activity must use Ameren's corporate Internet provider so that access controls and related security mechanisms can be applied. Likewise, Privileged Users must always employ an Ameren electronic mail address for Internet electronic mail; use of a personal electronic mail address for this purpose is prohibited. Telecommuters and mobile computer users are allowed an exception to this requirement.

3.1.5. Establishing Network Connections

Unless approved in advance by Information Security, Privileged Users may not establish Internet or other external network connections that could allow non-Ameren users to gain access to Ameren systems and information.

3.1.6. Establishing New Business Channels

Privileged Users are prohibited from using new or existing Internet connections to establish new business channels unless approved in advance by Information Security. These channels include such things as electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, and on-line database services.

3.2. Personal Use

3.2.1. Personal Use

Privileged Users are to use Ameren's Internet and Intranet sites 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 the Privileged User's productivity; and

c. It does not preempt any business activity.

d. All usage and access must comply with Ameren's Equal Employment Opportunity and Anti-Harassment Policy and Workplace Violence Policy.

Privileged Users may not use their Internet access to support and further a private business enterprise or to perform work for any outside interest for which the Privileged Users receives any compensation. Individual Business Lines or departments may develop and implement a more stringent personal use policy.

3.2.2. Blocking Sites

Ameren routinely prevents Privileged Users from connecting with certain non-business web sites. Privileged Users who discover they have connected with a web site that contains potentially offensive material must immediately disconnect from that site and notify Information Security. They will take the necessary steps to block the offensive site.

Examples of such material include anything that may be sexually suggestive, demeaning, or pornographic; racially, ethnically or religiously derogatory; or intimidating or offensive on the basis of any other protected factor according to the provision of the Company's Equal Employment Opportunity and Anti-Harassment Policy.

Ameren reserves the right to determine the appropriateness of any material. The ability to connect with a specific web site does not imply that the Privileged User is permitted to visit that site. Ameren will monitor Internet web access to ensure Privileged Users are not visiting sites unrelated to their jobs, and to ensure that users comply with Ameren policies.

3.2.3. Management Review

At any time and without prior notice, Ameren management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, and other information stored on or passing through Ameren computers. Such management access will be used to ensure compliance with internal policies, assist with internal investigations, and assist with the overall management of Ameren information systems. Management reserves the right to terminate a Privileged User's Internet access at any time.

3.2.4. Logging

Ameren routinely logs web sites visited, files downloaded, time spent on the Internet, and related information.

3.2.5. Junk Email

Privileged Users are prohibited from using Ameren computer systems for the transmission of unsolicited bulk email advertisements or commercial messages. Commonly known as "spam," these prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing pitches. When Privileged Users receive such unwanted and unsolicited email, they should not respond directly to the sender. Instead, they should forward the message to the "Spam Mail" Outlook mailbox. Steps will then be taken to prevent further transmissions.

3.2.6. Phishing attempts

Phishing is an attempt to gain privileged information, such as a user ID or password, via an email that appears to come from a known trusted source. If a Privileged User receives an unsolicited email requesting such personal information, this request for information should not be acted on. Instead, report the email by clicking the Junk button in Microsoft Outlook. Please contact the IT Service Desk if there are further questions.

3.3. Information Security

3.3.1. Information Reliability

Privileged Users must exercise caution when relying on information obtained from the Internet. There is no standard quality control process on the Internet, and a considerable amount of information on the Internet is outdated, inaccurate, and in some cases deliberately misleading.

3.3.2. Virus Checking

Privileged Users must obtain permission from Information Security to download software from the Internet. Approved software is available in the Software Center and Application Catalog. Privileged Users should use the application catalog to request new software. Privileged Users are required to run the corporate virus scanning software against every authorized program and/or data file obtained via the Internet and must not execute or use such files and/or programs unless they have been verified to be free from viruses.

Data files downloaded from the Internet will be compressed or encrypted are often compressed. Privileged Users must decompress or decrypt these files before running the virus scanning software. If a virus is detected, the IT Help Desk must immediately be notified, and all activity on the workstation in question must cease until the virus has been eradicated.

3.3.3. Push Technology

Subscription to real-time automatic information distribution services on the Internet (so-called “push services”, “streaming video or media”) is prohibited unless approved by Information Security. While powerful and useful, this technology could be used to spread viruses and cause other operational problems such as system unavailability.

3.3.4. Spoofing Users

Before Privileged Users release any internal Ameren information to, enter into any contracts with, or order any products via public networks from any entity or individual, the identification of such entity or individual must be confirmed. Ideally, identity confirmation performed via digital signatures or digital certificates, but in cases where these are not available, other means such as letters of credit, third party references, and telephone conversations, may be used.

3.3.5. User Anonymity

Privileged Users must not misrepresent, obscure, suppress, or replace their own or another user's identity on the Internet or on any other Ameren information system. In all instances, the Privileged User’s name, electronic mail address, and related contact information must reflect the actual originator of a message or posting. The use of anonymous remailers or other identity hiding mechanisms is forbidden.

3.3.6. Attachments

Because attachments may include viruses or other malicious software, Privileged Users must not open electronic mail attachments unless such attachments were expected from a known and trusted sender.

3.3.7. Web Page Changes

Privileged Users may not establish new Internet web pages, or make modifications to existing web pages dealing with Ameren business, without prior approval from Corporate Communications. Modifications include adding of links to other sites, updating the information displayed, and altering the graphic layout of a page.

3.4. Information Confidentiality

3.4.1. Information Exchange

Ameren software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-Ameren party for any purposes other than business purposes expressly authorized by management.

Exchanges of software and/or data between Ameren and a non-Ameren party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

Regular business practices, such as shipment of a product in response to a customer purchase order, need not involve such a specific agreement since the terms and conditions are implied.

3.4.2. Posting Materials

Internal Ameren information disclosed via the Internet may adversely affect Ameren's stock price, customer relations, or public image. Such information must not be disclosed without prior approval from Corporate Communications. This includes sites such as social networking sites (i.e., Twitter, Facebook, LinkedIn, MySpace, etc.), social media sites including blogging sites (Blogger, WordPress, etc.), bulletin boards, Internet forums, etc.

Similarly, information that might disclose or compromise Ameren network security must not be posted without prior approval from Information Security. This includes photos of generation or transmission equipment or other images related to Ameren infrastructure.

3.4.3. Sending Sensitive Data

Privileged Users must not send any sensitive data such as credit card numbers, telephone calling card numbers, login passwords, or customer account numbers via the Internet unless the data is encrypted with software approved by Ameren's Information Technology Function. Secure Sockets Layer (SSL) is an acceptable Internet encryption standard.

3.5. Public Representation

3.5.1. External Representations

When conducting Ameren business, Privileged Users may indicate their affiliation with Ameren by explicitly adding certain words or by using an electronic mail address. In either case, Privileged Users must clearly indicate the opinions expressed are their own and not necessarily those of Ameren unless they have been expressly designated as a spokesperson for Ameren.

3.5.2. Appropriate Behavior

Whenever any affiliation with Ameren is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, Privileged Users must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

3.5.3. Removal of Postings

Messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, which include an implied or explicit affiliation with Ameren, may be removed if management deems them inconsistent with Ameren's business interests or existing Ameren policy.

3.6. Intellectual Property Rights

3.6.1. Copyrights

Ameren strongly supports strict adherence to software vendor license agreements. When Ameren resources are employed, copying of software in a manner that is not consistent with the vendor license is strictly prohibited (e.g., participating in pirate software bulletin boards). Reproducing, forwarding, or in any other way republishing or redistributing words, music, graphics, or other copyrighted materials is prohibited unless permission is obtained from the author/owner. Privileged Users should assume that all materials on the Internet are copyrighted unless specific notice states otherwise.

3.7. Internet Services

3.7.1. Internet Services

In general, native Internet services (e.g., File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), and Telnet), are only to be used for specific business needs.

3.7.2. Instant Messaging and Collaboration Software

Instant messaging (IM) and collaboration software such as Lync is only to be used to support business needs. Personal use is strictly prohibited.

3.8. Intranet Usage

3.8.1. Intranet Access

Ameren's Intranet ("Scholar") gives Privileged Users easy access to non-confidential corporate information. Any Privileged User granted network access would be granted access to "Scholar".

3.8.2. Intranet Changes

Privileged Users may develop Intranet applications. Information Technology will provide technical support for the applications and the network infrastructure. The support includes, but is not limited to:

a. Selection and support of the development tool set and appropriate standards

b. Administration and protection of the Intranet server

c. Control and capacity planning of the Intranet network

d. Staging of the application from test to production

e. Standards for ease of use and common look and feel

4.0 ENFORCEMENT

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 Internet/Intranet policies. Ameren Corporation reserves the right to modify or change its policy at any time.

5.0 CORPORATE RESPONSIBILITY

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

6.0 DEFINITIONS

Anonymous remailer – Organization that forwards received email anonymously by stripping out the sender's name and email address. Remailers are used by people who wish to express an opinion to newsgroups or to individuals without fear of excessive responses or retaliation

Decrypt - To convert encrypted data back into its original form

Digital certificate - The digital equivalent of an ID card used in conjunction with encryption systems

Digital signatures - Digital guarantee that a file has not been altered

Electronic bulletin boards - (Bulletin Board System / BBS) A computerized version of a bulletin board

Electronic Data Interchange (EDI) - The electronic communication of a business transaction between organizations

Encrypt -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

File Transfer Protocol (FTP) **–** Internet protocol used to transfer files over a network

Flaming - To communicate emotionally via email

Instant messaging - Real-time conferencing capability between two or more users on a computer network such as the Internet

Internet - An electronic communications network that connects computer networks and organizational computer facilities around the world

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

Intranet - An internal web site accessible to employees

Newsgroup - An Internet-based discussion group

Object-oriented programming - A form of modular programming that allows pieces of software to be reused and interchanged between other programs

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

Phishing – Act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Protocol - Hardware and software standards that govern how data is transmitted and received between computers

Secure Sockets Layer (SSL) - A protocol designed to provide secure communications on the Internet

Simple Mail Transfer Protocol (SMTP) - Standard email protocol on the Internet

Spam - To send copies of the same message to large numbers of newsgroups or users on the Internet

Spoof - To fake the identity of a user or the address of a data transmission in order to gain illegal entry into a secure system

Streaming media or video - Playing audio or video files immediately as they are downloaded from the Internet

Telnet - A terminal emulation protocol commonly used on the Internet that allows a user at a computer to logon to a remote device and run a program

Trivial File Transfer Protocol - A simpler version of file transfer protocol, FTP (TFTP)

User-ID - A string of characters that uniquely identify computer users to information systems (e.g., C12345 or E56789)

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

Web browser - Computer software that accesses web pages stored on the Internet (e.g., Internet Explorer)