Policy Number: COPO.012.01
Effective Date: 03/28/2005

Information Resources Acceptable Use Policy

1.0 Purpose

The purpose of this policy is to define the appropriate use of Ameren's Information Resources.

2.0 Scope

This policy applies to all Ameren employees, contractors, consultants, and other individuals at Ameren, including those workers affiliated with third parties who have access to Ameren Information Resources. Hereafter, referred to as “Privileged User.”

3.0 Policy Requirements

3.1 Use of Ameren's Information Resources

3.1.1 Ameren authorizes Privileged Users to use Ameren's Information Resources for business purposes only. Limited personal use may be acceptable if it does not interfere with the Privileged User’s productivity and prior management authorization or approval for such personal use is obtained.

3.1.2 Ameren strictly prohibits the use of its Information Resources on behalf of a third party (i.e., client, family member, political, religious, charitable, or school organization, etc.) unless otherwise authorized by Ameren management.

3.1.3 The use of Ameren’s Information Resources for an employee’s own personal interest, gain or enterprise or any enterprise other than that of Ameren on company time is conduct subject to disciplinary action up to and including termination. Use of Ameren’s Information Resources for these purposes outside of working hours requires prior supervisory or management approval.

3.1.4 Use of Ameren’s Information Resources for any unlawful or improper purpose or in violation of any Ameren values or polices at any time is prohibited.

3.1.5 Ameren reserves the right to monitor, audit and inspect the use of its Information Resources.

3.1.6 Privileged Users should have no expectation of privacy or confidentiality when using Ameren’s Information Resources despite the use of individual passwords or other personal security protections.

3.1.7 Information Resources include, but are not limited to:

- Any device capable of electronically storing data (thumb drives, USB devices, MP3 players, PDAs, floppy disks, mobile phones, iPhones, tablets, etc.)

- Hardware – desktops, laptops, terminals, printers, mainframe computer, servers, and network infrastructure equipment
- Software - word processing, spreadsheet, email, business and engineering applications, cad/cam, Internet, Intranet
- Data - information stored in computer files
- Communications Facilities - telephone lines, local area networks (LAN), and wide area networks (WAN)

4.0 Gaining Unauthorized Access

4.1 Privileged Users are prohibited from:

- Installing Ameren Information Resources on any device not owned and maintained by Ameren except for the approved software needed for remote access connectivity.
- Connecting non-Ameren Information Resources to Ameren's devices and/or network except for the provisions covered in the Remote Access Policy.
- Installing any software not approved for use by OPS Enterprise Computing Services or the Information Security Group.
- Gaining unauthorized access to any Information Resources to which they have not been expressly granted access.
- Damaging, disrupting, or interfering in any way with the operations of Information Resources.
- Capturing or otherwise being in possession of passwords, encryption keys, or any other access control mechanisms that have not been expressly assigned to them.
- Possessing or using software tools, which could provide unauthorized access to Information Resources.

5.0 Storing Ameren Information

5.1.1 Ameren data and information is only to be stored on Ameren owned and maintained Information Resources. Privileged Users are prohibited from storing Ameren data on devices not owned by Ameren.

5.1.2 When storing confidential data or data designated as such by legal/regulatory requirements (e.g., HIPAA e-PHI, CEII, FERC – Code of Conduct, or Safeguards Information) on Ameren owned mobile resources (e.g., laptops, PDA, and removable media) Privileged Users must encrypt the data. See the document PGP Software– This data encryption procedure is available on Scholar for instructions on using encryption.

6.0 Due Diligence

6.1.1 Privileged Users are required to notify Information Security immediately of any actual or suspected security violation occurring with Ameren's Information Resources such as:

- Unauthorized access to network, telecommunications, or computer systems
- The apparent presence of a virus on any Information Resources
- The apparent presence of any information resource prohibited by this or any other corporate policy
- The apparent tampering with any data file for which the user has established restrictive discretionary access controls

6.1.2 Privileged Users are responsible for preventing unauthorized access to the Information Resources in their possession whether it be hardware, software, or data.

6.1.3 Extreme care must be taken to protect mobile resources that may contain Ameren data and information. Mobile resources must not be left in places where they can easily be stolen or left behind (e.g., hotel rooms, conference centers, cars, and other forms of transportation).

6.1.4 Mobile resources when left unattended should be physically locked away or locked with special locks and cables. In situations where business reasons require access to be given to others (i.e., a vendor who has come to install a product or make repairs), the Privileged User must oversee and monitor the actions of the individual given temporary access. This includes remote access given to a vendor or unknown person for troubleshooting reasons, such as WebEx, Lync, etc.

6.2 Establishing Network Connections

Privileged Users may not build or connect any private or test networks to the Ameren Corporate network without prior authorization from Network Engineering and the Information Security Group. The Ameren corporate computing infrastructure is the responsibility of the Information Technology department. Ameren infrastructure must be adequately secured and protected from all cyber risks. As such, the installation of hardware is prohibited unless previously approved.

6.3 Software Control

6.3.1 All software installed on Ameren Information Resources, whether managed by Information Technology or some other business line, must be controlled and managed to avoid significant risks such as:

- Security weaknesses in the form of viruses, worms, and Trojans
- Licensing issues
- Data leakage
- Weak access controls into Ameren's network

6.4 Information Technology is responsible for the control, management, and distribution of software to Ameren Information Resources. Any modifications, additions, or deletions to the software running on the Ameren Information Resources must be coordinated with Information Technology before making the change. See the document - "Procedure for Coordination and Acceptable Software List" available on Scholar for coordination information.

6.5 Portable Storage Devices

Portable storage devices should be scanned for viruses before files are transferred from the device. You should use the scanning kiosk, if available, or contact the IT Service Desk at 314-5544357 Option 1 for assistance with scanning the device for viruses.

7.0 Enforcement

Employees who violate this policy may be subject to disciplinary action, up to and including termination. Ameren reserves the right to revoke access to all Ameren Information Resources by any third party for violating the terms of this policy.

8.0 Corporate Responsibility

For further information regarding the Information Resources Acceptable Use Policy, contact the Information Security Group.

9.0 Definitions

Confidential data – Is information whose unauthorized disclosure, compromise, or destruction would directly or indirectly have an adverse impact on Ameren, its customers, or employees. Financial loss, damage to Ameren's reputation, loss of business, and potential legal action could occur. It is intended solely for restricted use within Ameren and is limited to those with a need to know."

HIPAA (Health Insurance Portability and Accessibility Act of 1996) - This law requires policies and procedures to be in place to ensure confidentiality and security for health information. There are nine parts to HIPAA. One part, the HIPAA Security Rule, requires that reasonable and appropriate technical, physical, and administrative safeguards be taken with all electronic protected health information (ePHI) created, received, maintained, or transmitted.

CEII (Critical Energy Infrastructure Information) - CEII is information concerning proposed or existing critical infrastructure (physical or virtual) that:

1. Relates to the production, generation, transmission or distribution of energy;
2. Could be useful to a person planning an attack on critical infrastructure;
3. Is exempt from mandatory disclosure under the Freedom of Information Act; and
4. Gives strategic information beyond the location of the critical infrastructure.

Federal Energy Regulatory Commission's (FERC) Code of Conduct – FERC requires transmission providers to adopt strict codes of conduct to prevent misuse of transmission operations data. The code of conduct requires functional separation of transmission employees from market employees. In addition, any market-sensitive information must be shared with all competitors at the same time through the Open Access Same time Information System ("OASIS").

Safeguards Information - Safeguards information is a special category of sensitive unclassified information authorized by Section 47 of the Atomic Energy Act to be protected. Safeguards information concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material.