REMOTE ACCESS POLICY

PURPOSE

In order to minimize Ameren's exposure to potential damages that may result from unauthorized or inappropriate use of Ameren resources, this policy will define the appropriate security requirements necessary to connect to Ameren's network from any remote information system.

PERSONS AFFECTED

This policy applies to all employees, contractors, consultants, temporary employees, or other individuals, including those workers affiliated with third parties who make remote connections to Ameren. Throughout this policy, the words "Privileged User" refers collectively to all such individuals. The policy also applies to all computer and data communication systems owned by and or administered by Ameren.

POLICY

Ameren information systems, data, and networks are secure systems that contain confidential and proprietary information. Access to Ameren systems without appropriate approval is strictly prohibited.

ACCESS APPROVAL

Employees

When business need dictates, an Ameren employee may access Ameren internal networks from remote locations (e.g., employee's home, hotel room, airport terminals, etc.). The employee's department manager must approve access to Ameren internal networks from remote locations in advance. Ameren reserves the right to revoke access at any time.

Non-Ameren Employees

Occasionally, when business need dictates, Ameren permits third parties access to Ameren internal networks and information. Both the owner of the information accessed and the Ameren project manager must approve the request before access is established. Privileges for third parties are strictly limited to the system facilities and information clearly needed to achieve predefined business objectives. Third parties seeking access to Ameren internal networks must sign the Network Access Agreement, which indicates the involved Privileged User(s) understand(s) and agree(s) to abide by Ameren policies and procedures related to information systems and data.

Ameren may periodically audit third parties access to ensure compliance with Ameren policies. Ameren retains the right to revoke access at any time. The appropriate project manager must review access privileges every six months to ensure the access continues to be appropriate.

Vendors who have sold hardware, software, or other services to Ameren must request approval as described above or get approval from the Information Security Group to gain access to Ameren networks. An Ameren systems administrator may grant temporary remote access privileges to vendors if the requested access does not exceed five days and the appropriate Ameren project manager approves the request.

CONFIDENTIALITY

Shared File Systems

Data stored in Ameren systems is confidential and proprietary. To ensure that confidential information is not inadvertently disclosed to unauthorized persons, connections between non-Ameren computers or networks and Ameren internal computers or networks must not involve the use of shared file systems. Privileged Users are prohibited from storing any Ameren data on any non-Ameren equipment.

Using Wireless Technology for Data Transmission

Ameren prohibits privileged users from using wireless networking technologies such as radio-based local area networks or cellular phones to transmit confidential information unless the link is encrypted. Privileged Users may use wireless technology for electronic mail as long as the transmissions do not contain readable confidential information. Similarly, Privileged Users must not discuss confidential information on wireless telephones, employing a regular voice connection, unless the Information Security Group or Telecommunications Department has encrypted the connections.

Disclosure of Systems Information

Internal addresses, configurations, security measures, and related system design information for Ameren computers and networks is confidential and must not be released without prior approval from the Information Security Group.

EXTERNAL CONNECTIONS STANDARDS

Personal Firewalls

Ameren requires that appropriate firewall protections be in place prior to granting access to Ameren system(s). Personal firewalls must be compliant with Ameren corporate standards before Privileged Users will be granted remote access to Ameren system(s). Ameren will provide a standard personal firewall to privileged users who require remote access via the client Virtual Private Network (VPN). Ameren prohibits privileged users from changing any firewall security parameters while connected to the Ameren network.

Anti-Virus Software

All computers connected to Ameren’s network must use the corporate anti-virus solution. However, connecting to Ameren’s network via a web interface, such as Internet Explorer, is excluded from this requirement.

Two-Factor Authentication

All computer network connections connecting to an Ameren internal network from a location outside Ameren must use an Information Security Group approved two-factor authentication. Computer network connections initiated from inside an official Ameren office, and connecting to an external network or computer, do not require two-factor authentication.

ANALOG/ ISDN LINE STANDARDS

Analog/ISDN Line Connections for Modems

Ameren prohibits connecting modems to office computers or other devices within Ameren except where explicitly authorized by the Information Security Group. Home based, mobile and/or telecommuting computers are an exception to this rule. All new connections require an approval on file with Telecommunications.

Requesting an Analog/ISDN Line

Use of analog or ISDN voice stations (telephones) will be minimized but are permitted in Telecommunications Department designs where other types of telephones are not practical. Once approved by the department manager, the Privileged User requesting an analog/ISDN line must complete the Analog/ISDN Line Request Form. Because of the potential security risk associated with an analog/ISDN line, analog or ISDN lines must be assigned to an Ameren management employee who will be responsible for the line. The line will not be installed without the Information Security Group's approval.

SECURITY

Outbound Connections

Outbound connections must be routed through dial-up modem pools, internet firewalls, and other systems expressly established to provide secure network access.

Installation of Analog and ISDN Communication Lines

Communications lines, particularly analog and Integrated Services Digital Network (ISDN) lines connected to modems in desktop computers and facsimile machines are a main entry point into Ameren's network and therefore pose a high security risk. Privileged Users wishing to make such connections must obtain their Ameren manager's approval to do so.

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 any and all Ameren resources by any third party for violating the terms of this policy.

CORPORATE RESPONSIBILITY

For further information regarding the Remote Access Policy, contact the Information Security Group.

DEFINITIONS

Access control system - A system that manages the permissions for logging on to a computer or network

Firewall - A device that enforces security policies designed to keep a network secure from intruders

Integrated Services Digital Network - A service offered by most telephone carriers for the transmission of voice and data. ISDN is often used for modem connections and videoconferencing

Modem - A device that allows a computer to transmit data over a standard telephone line

Modem pool - A collection of modems and software that let users dial out and remote users dial in on the next available modem

Router - A network device that forwards data from one network to another

Two-factor authentication - A security process that confirms user identity using two distinctive factors such as something a user has (keys, cards, tokens) and something a user knows (passwords or personal identification number PIN)

Virtual private network - A network constructed by using the Internet as the medium for transporting data between nodes.