Employer Security Policy

All new employees will receive training related to computer and organization security during the required new hire training. The employee must agree to the security requirements to receive the user ID and temporary password. All employees are expected to maintain secrecy of their password and abide by company security procedures.

Computer and Workstation Security

All computers accessing the A Energy Company network are required to have an IT administrative account to access the computer and the password-protected log in. All computer activity may be audited and all activity is tracked by user ID. All laptop computers and workstations are equipped to automatically lock at a set number of minutes of inactivity for protection from intentional or unintentional misuse of an employee's account. A single user ID and password is used to access the computer and e-mail system.

All hardware, including computers, projectors, external hard disk drives, and printers, contain tracking mechanisms in case of loss or theft. Laptop computers are assigned to a single user. Workstations may be shared and require authentication by each user with the individual's user ID and password. All printing requires a pass code to be entered for proper billing and cost allocation.

Internet browsing is managed to safeguard bandwidth. Select Internet sites are blocked using web filtering software. Appeals may be filed for access to sites that have been blocked and have a business necessity.

Staff Security

A Energy Company safeguards its employees with monitoring technology. High-definition digital security cameras monitor internal and external environments. All employees are offered personal safety training by an approved instructor. Entrance into the building and movement from one area to another requires each employee to swipe an electronic identification card. At no time are employees permitted to allow another employee or a guest access without the individual swiping an electronic identification card.

Guest Security

All guests are required to receive a visitor's electronic identification card. The card will be coded to allow access to the approved areas of the facility. Guests may be asked to sign a nondisclosure form to protect proprietary information and technology.

Monitoring

The physical location and network use are monitored to identify and respond to any unauthorized access to the facility or network.

Physical Location Monitoring

High-definition digital cameras record movement at internal and external locations at each site. Security personnel monitor the video output. All images are saved for future analysis. Motion sensors are in place for additional security.

Network and Resource Usage Monitoring

The A Energy Company network and servers are accessible only through authentication by an approved user ID and password. Some levels of the network require a SecurID token in addition to an approved user ID and password. Use of network resources is monitored and linked to the user ID and password that authenticated the computer accessing the network. Locking or logging off laptop computers or workstations when not in use is advised to avoid intentional or unintentional misuse of the network.

Internet access to some sites is limited. If these blocked sites are necessary for business related activities, an appeal can be made. Reviews of appeals will be within one business day. E-mail accounts can be reviewed at any time. If a personal e-mail is sent from the work account, employees can mark the subject line as "personal" to avoid that e-mail being opened during the monitoring process.

Confidentiality of trade secrets is essential for a competitive edge; each person must help protect the company. E-mail etiquette is suggested to portray the professional image of the company.

Computer Security

Each computer and workstation has virus protection software. This software automatically updates once per week and also whenever critical updates are identified. Each computer will be scanned for viruses and malware once a month. Updates and scans are scheduled to be performed to minimize impact on productivity.

Passwords must be changed every 90 days, must be a minimum or 8 characters in length, and must contain at least three of the four following criteria: a capital letter, a lowercase letter, a symbol, or a number. All computers have VPN access that requires authentication with an approved user ID and password to tunnel through firewalls when using the internal network or any external network.

Each laptop computer has an encrypted hard drive to protect sensitive information in the event of loss or theft. Each employee is issued a security cable to use when traveling to help deter theft.

Violations

Violations of the security policies will be reviewed to determine the cause of the security breech. Intentional misuse will be prosecuted to the full extent of the law.