

Physical and Environmental Security Policy

# Overview/Purpose

**<Utility Name>** is committed to protecting its employees, members and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This Physical Security Policy details the requirements and guidelines for the physical protection of **<Utility Name>** information, assets, and personnel.

# Scope

This Policy applies to all **<Utility Name>** facilities, information, assets, and all personnel who are conducting work while on **<Utility Name>** premises up to and including: employees, contractors, workforce members, vendors and agents with a computer/device connected to the **<Utility Name>** network.

# Policy

## Facility Security

* Sensitive exterior areas will be illuminated by security lighting from dusk to dawn. Lighting faults or failures should be reported to the **<person or group responsible for policy>** in a timely manner.
* Sensitive facilities will be protected by an intrusion alarm system, which is externally monitored. **<Person or Group responsible for policy>** will be responsible for designating which employees will be designated to arm/disarm the alarm system. The alarm system will be tested on a recurring basis.
* Public areas will be accessible during normal business hours. Non-public areas of all buildings will be designated as sensitive areas. Only authorized personnel are allowed in sensitive areas.
* Access to sensitive areas will be controlled by an access control system, and will be recorded by using a video surveillance system.
* Lost access tokens/keys must be reported to the **<person or group responsible for policy>** immediately.
* Visitors will be escorted at all times in sensitive areas. Visitors will be required to sign in using a visitor log maintained at the main entrance, and will be issued a visitor badge. Visitor logs will be retained for at least three months,

*[Explanatory note: Modify the visitor sign-in requirements to meet the particular policies, or reference an existing visitor sign-in policy.]*

* Wiring closets and areas that contain vital IT infrastructure, systems, or confidential data will follow the principal of Least Privileged Access. Employees, contractors, and vendor staff will be granted access only to facilities and equipment necessary to fulfill their job function.
* **<Person or Group responsible for policy>** will be responsible for assigning access to secure areas as is appropriate. Access reviews will be conducted and removal of individuals that no longer require access will be completed.
* All employees are responsible for checking to ensure that doors, windows, and other access means in their area of responsibility are locked and secure at close of business. Employees should report open or unlocked access means to the **<person or group responsible for policy>** immediately.

## Device and Server Security

* All servers that host sensitive data and all critical IT resources will be placed in access controlled areas.
* Laptops, tablets, cell phones, and other portable equipment will be kept in a secured area such as a locked drawer, locked office, or secured to a permanent object when not in use via rugged locking equipment.
* Backups, portable hard drives, and other removable media will be kept in a secure area such as a locked drawer or locked office when not in use.
* Employees shall consider the sensitivity of the information to which they have access, such as Personally Identifiable Information (PII) and Protected Health Information (PHI), and shall take appropriate steps to prevent unauthorized access.
* **<Utility Name>** will implement physical and technical safeguards for all devices that access sensitive information to restrict access to authorized users. Appropriate measures include:
  + Restricting physical access to devices to only authorized personnel.
  + Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
  + Where supported, enabling automatic screen locking after 15 minutes of inactivity.
  + Complying with all applicable password policies and procedures. See the *Password* Policy.
  + Ensuring devices are used for authorized purposes only.
  + Never installing unauthorized software on devices.
  + Storing all sensitive information, including PII and PHI on appropriately secured systems.
  + Keeping food and drink away from servers, network equipment, and workstations in order to avoid accidental spills.
  + Arranging screens to limit visibility of sensitive data, or using polarized screen filters to block screen viewing from the sides.
  + Ensuring devices are left on but logged off in order to facilitate after-hours updates.
  + Exiting running applications and closing open documents when leaving for the day.
  + If wireless network access is used, ensuring access is secure by following the *Network Configuration Standard.*
  + Implementing file integrity monitoring systems to monitor for unauthorized changes to system files*.*

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adapted from “Cyber Security Policy Framework” ( <https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
  Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **CFO**  **COO**  **Legal Department** | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |