

Information Security Policy

# Purpose

**<Utility Name>**’s Board of Directors recognize the need to protect the utility, our consumers, and both utility and consumer data, and the utility’s information systems, from growing information and cybersecurity threats. This policy establishes an Information Security Program (ISP) within **<Utility Name>** to ensure that adequate measures are taken and controls are in place to mitigate threats and protect company resources.

*[Explanatory Note: This policy draft is intended for the establishment of an overall Information Security Program at the Board level with policies and procedures which the staff can implement. It should be noted that information security is not solely an Information Technology concern, but touches all departments, all employees, and all types of informational transactions. This plan may or may not represent the hierarchy appropriate at a particular Utility, and should be modified as needed.]*

The purpose of this policy is to ensure that technology assets are protected against all internal, external, deliberate, and accidental threats. Information, in all its forms, written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorized modification, or destruction throughout its lifecycle. Policies and procedures are established and shall be administered so as to protect Utility technology systems and data, member financial and protected information, and Utility data acquisition and control systems across the enterprise.

*[Explanatory Note: This policy draft is intended for establishment of an overall Information Security Program and is not just a Cybersecurity program.]*

# Scope

All employees, contractors, consultants, temporary, and other workers at **<Utility Name>** and its subsidiaries must adhere to all policies and procedures authorized and approved under this program. This applies to Utility data sets and technology equipment that is owned, operated, or leased. The ISP policies and procedures describe the technology and information assets that must be protected, and identifies many of the threats to those assets. The equipment, software, and storage medium used to process, store, and transmit information will be protected by appropriate controls.

# Policy

## Policies and procedure objectives

Policies and procedures have been established to ensure that:

* + 1. Sensitive, protected, and/or privileged Information and technology systems will be safeguarded against any unauthorized access;
    2. Confidentiality of sensitive, protected, and/or privileged information will be assured;
    3. Integrity of information will be maintained;
    4. Availability of information for business purposes will be maintained;
    5. Legislative and regulatory requirements will be met; and
    6. Business continuity and disaster recovery plans will be developed, maintained, and tested annually.

*[Explanatory note: the utility should customize this policy statement to include specific requirements within the Utility and testing schedules they deem appropriate.]*

* + 1. All employees, contractors, consultants, temporary and other workers will be provided information security and awareness training on a regular basis
    2. Any actual or suspected information security breaches will be reported to the designated <**person or group responsible for policy**>. All breaches will be investigated thoroughly and logged

The established policies and procedures include appropriate controls and continuity plans. These policies and procedures also address the availability of information systems.

# 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>)

The 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.   
*[Explanatory Note: The RACI model is a common project management tool. See detailed description in ISP Implementation Guidelines.]*

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| CEO/GM | **BOD** | **Legal Department** | **All Employees** |

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

# Approvals

\_

Board of Directors Date

# Revision History

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