

Compliance Requirements Policy

# Overview/ Purpose

There are many external compliance requirements which <**Utility Name**> must adhere to from a regulatory standpoint, as well as all internal policies that the company has developed and implemented. These policies must be periodically reviewed and internal practices modified as necessary to ensure compliance with all applicable policies and regulatory requirements.

The purpose of this policy is to delineate those policies and requirements that have been determined to be critical for maintaining a strong overall information security program.

# Scope

This policy applies to the senior management staff at <**Utility Name**> who are responsible for determining the overall information security program and to the <**person or group responsible for policy**> who provide information security guidance to the management staff, implement those policies that are approved by the appropriate authority, and ensure that all policies are kept up-to-date with current guidelines/best practices.

# Policy

<**Utility Name**> will comply with all external policies, including:

* Health Insurance Portability and Accountability Act (HIPAA)
* The Payment Card Industry Data Security Standard (PCI DSS)
* Fair and Accurate Credit Transactions Act of 2003 (FACT Act Red Flags Rules)
* State requirements such as reporting any data breaches which involves PII (Personal Identification Information) <**remove if not applicable**>
* Federal Energy Regulatory Commission/ North American Electric Reliability Corporation (FERC/NERC) <**remove if not applicable**>
* The Sarbanes–Oxley Act (SOX) <**remove if not applicable**>
* The Gramm–Leach–Bliley Act (GLBA) <**remove if not applicable**>
* The United States Rural Utilities Service (RUS) requirements.

<**Utility Name**> senior management and legal counsel will determine those compliance requirements to be appropriate as well as any internal policies developed by <**person or group responsible for policy**>, the combination of which comprise the overall information security plan.

# 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

(Cross references to industry standards)

* 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.

# Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| Legal | **CEO/GM** | **COO**  **CFO HR**  **MS** | **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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |