

IT Risk Management Policy

# Overview/Purpose

To empower <**person or group responsible for policy**> to perform periodic information security risk assessments (“RAs”) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

# Scope

Risk assessments (RAs) can be conducted by any entity within <**Utility Name**> or any outside entity that has signed a Third Party Agreement with <**Utility Name**>. RAs can be conducted on any information system, including applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

# Policy

The execution, development and implementation of remediation programs is the responsibility of <**person or group responsible for policy**> and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Risk Assessment Team in the development of a remediation plan. The RA process shall use <**Utility Name**> Data Protection and Availability Standards.

# 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.

* Adapted from “Risk Assessment Policy”

(<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)

* Data Classification Policy
* Data Protection and Availability Standards
* Vulnerability Management Policy

# 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 Accountable**> Date

# Revision History

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