Cyber Resilience Initiative

Information Security Program Library

Version 1.0

SEDC

For more information
t | 770-414-8400
e | cri@sedata.com
i | sedata.com

Table of Contents

Introduction

In 2016, SEDC created its Cyber Resilience Initiative (CRI) to help customers improve their cybersecurity posture. One of the fundamentals of CRI is the Information Security Program Library (ISPL). This collection of policies, procedures, standards, and forms can be used by utilities as a template to create customized documents.

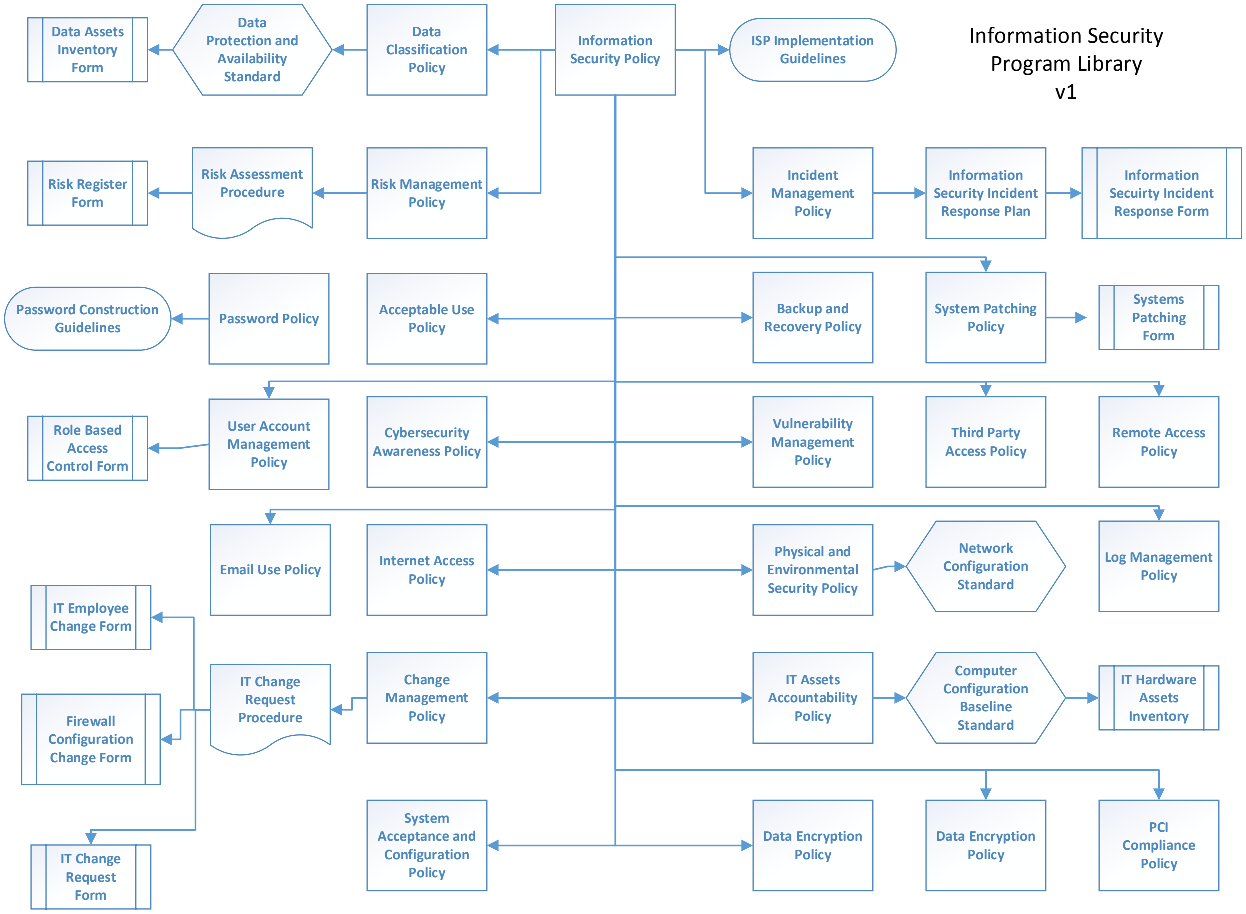
ISPL is a compilation of best practices developed by other entities. We acknowledge our resources: the Kentucky Association of Electric Cooperatives (KAEC), NRECA, SANS Institute, NIST 800 publications, FIRST (Forum of Incident Response and Security Teams) and the PCI Security Standards Council.

The first version of ISPL is available to all SEDC customers and can be obtained at the SEDC Users Conference 2016 and on The Bridge under the CRI section. As new cybersecurity-related standards and technologies are identified, applicable updates to ISPL will be made and distributed.

ISPL, in its current entirety, is presented here in hardcopy for ready access and also in electronic form on The Bridge as individual documents for easy customization.

These documents, collectively and individually, are provided for illustrative purposes only and may not be suitable in their entirety for all the individual needs of your company.

The end user agrees to hold harmless Southeastern Data Cooperative (SEDC) from any claims arising out of misuse or the inappropriate use of these documents and the actions described therein.


Information Security Program Library v1
Data Assets Inventory Form
Data Protection and Availability Standard
Data Classification Policy
Information Security Policy
ISP Implementation Guidelines
Risk Register Form
Risk Assessment Procedure
Risk Management Policy
Incident Management Policy
Information Security Incident Response Plan
Information Security Incident Response Form
Password Construction Guidelines
Password Policy
Acceptable Use Policy
Backup and Recovery Policy
System Patching Policy
Systems Patching Form
Role Based Access Control Form
User Account Management Policy
Cybersecurity Awareness Policy
Vulnerability Management Policy
Third Party Access Policy
Remote Access Policy
Email Use Policy
Internet Access Policy
Physical and Environmental Security Policy
Network Configuration Standard
Log Management Policy
IT Employee Change Form
Firewall Configuration Change Form
IT Change Request Procedure
Change Management Policy
IT Assets Accountability Policy
Computer Configuration Baseline Standard
IT Hardware Assets Inventory
IT Change Request Form
System Acceptance and Configuration Policy
Data Encryption Policy
Data Encryption Policy
PCI Compliance Policy

References

- KAEC
  Cyber Security Policy Framework
  https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx

- NRECA
  Cyber Security Resource Guide
  http://www.nreca.coop/what-we-do/bts/cyber-security/cyber-security-resource-guide/

- SANS – Information Security Policies Templates
  https://www.sans.org/security-resources/policies/

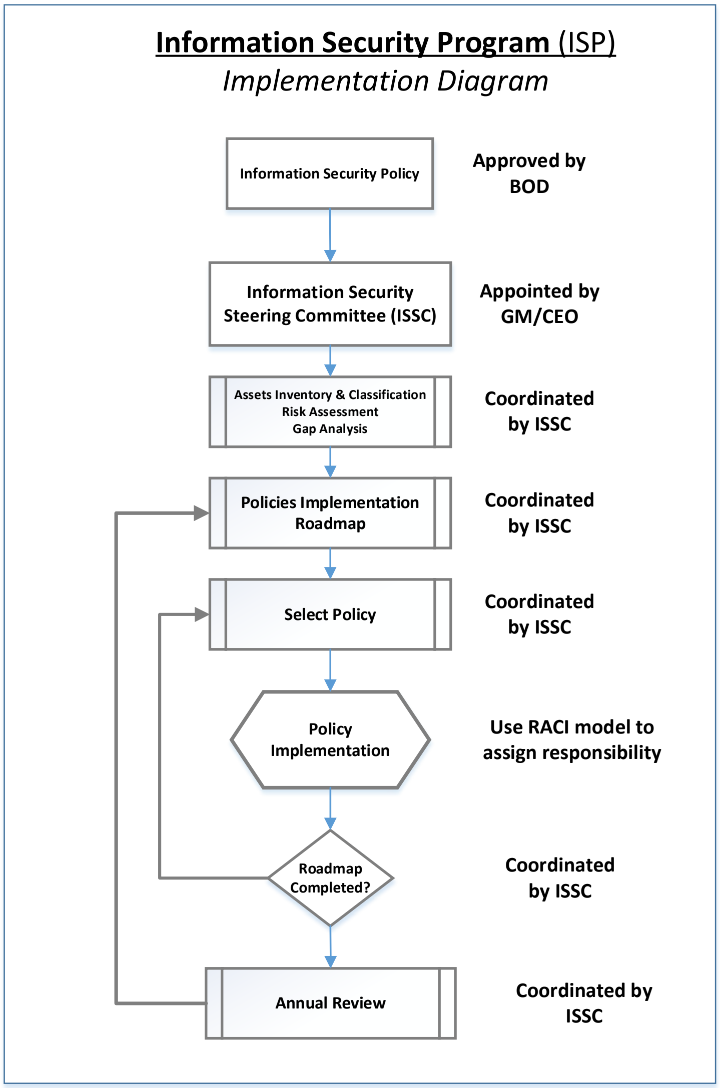
- NIST Special Publications (800)
  http://csrc.nist.gov/publications/PubsSPs.html

- PCI Security Standard Council
  https://www.pcisecuritystandards.org/document_library

- FIRST - Forum of Incident Response and Security Teams
  https://www.first.org

Implementation Plan

Information security is no longer viewed as just an "IT" issue and successful implementation of information security policies requires all employee involvement and coordination among all departments.



Information Security Program Implementation Guidelines document describes suggested phases of implementation:

1) The Board of Directors (BOD) approves an Information Security Policy and Information Security Program (ISP) Implementation Guidelines.

2) The CEO/General Manager establishes an Information Security Steering Committee (ISSC) that shall include staff from Administration, IT, E&O, Accounting, HR, Legal, etc.

3) ISSC will coordinate:

   - Initial assets inventory and data classification
     (ISPL includes *Data Classification Policy* and *Data Assets Inventory Form*);

   - Risk assessment
     (ISPL *Risk Assessment Procedure* and *Risk Register Form* can be used to support risk assessment);

   - Gap analysis
     {PCI DSS (Payment Card Industry Data Security Standard), DOE ES-C2M2 (Electricity Subsector - Cybersecurity Capability Maturity Model) or NIST Cybersecurity Framework can be used for gap analysis which can be conducted internally or by external consultant}.

4) ISSC creates Policies Implementation Roadmap (Roadmap) by assigning priorities for implementing policies and controls.

5) On regular basis (i.e., monthly), ISSC reviews implementation progress and selects the next policies for implementation.

6) On annual basis, ISSC reviews status of ISP and recommends changes to the Roadmap.

Insert
Utility
logo
here

Information Security Policy

1 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.]*

2 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.

3 Policy

3.1 Policies and procedure objectives

Policies and procedures have been established to ensure that:

3.1.1. Sensitive, protected, and/or privileged Information and technology systems will be safeguarded against any unauthorized access;
3.1.2. Confidentiality of sensitive, protected, and/or privileged information will be assured;
3.1.3. Integrity of information will be maintained;
3.1.4. Availability of information for business purposes will be maintained;
3.1.5. Legislative and regulatory requirements will be met; and
3.1.6. 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.]

3.1.7. All employees, contractors, consultants, temporary and other workers will be provided information security and awareness training on a regular basis
3.1.8. 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.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

6 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.]

7 Approvals

______________________________ ______________________________
Board of Directors Date

8 Revision History

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

Insert
Utility
logo
here

Information Security Program (ISP) Implementation Guidelines

1 Purpose

<Utility Name> recognizes the need to involve all employees to effectively implement the Information Security Program (ISP).

> *[Explanatory Note: This policy draft is intended for establishing a process for implementing an ISP at the Board of Directors (BOD) level with policies and procedures which the staff will implement and follow. Examples of organizational hierarchy most likely will require modification to reflect organizational structure of a particular Utility.]*

2 Scope

This document provides guidelines for the effective implementation of an Information Security Program (ISP), and will emphasize the importance of defining document types and a model for assigning responsibility. The scope of the ISP is broader than the IT discipline. These guidelines suggest establishing a Steering Committee to develop a security-conscious culture throughout the organization.

3 Guidelines

3.1 Documents structure

The ISP will use the following documentation structure:

3.1.1 Policy

A Policy is a formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policies always state required actions, and may include pointers to standards. Policy attributes include the following:

- Require compliance (mandatory)
- Failure to comply results in disciplinary action
- Focus on desired results, not on means of implementation
- Further defined by standards and guidelines

3.1.2 Standard

A Standard is a mandatory action or rule designed to support and conform to a policy.

- A standard should make a policy more meaningful and effective
- A standard must include one or more accepted specifications for documentation, hardware, software, and behavior

3.1.3 Procedure

A Procedure describes the process of implementing a Policy and enforces that Policy. A Procedure is a series of steps taken to accomplish an end goal:

- Defines "how" to protect resources and are the mechanisms to enforce policy
- Provides a quick reference in times of crisis
- Eliminates the problem of a single point of failure; and
- Also is known as a Standard Operating Procedure (SOP)

3.1.4 Guidelines

General statements, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement procedures.

- A guideline can change frequently based on the environment, and should be reviewed more frequently than standards and policies
- A guideline is not mandatory, rather a suggestion of a best practice. Hence "guidelines" and "best practices" are interchangeable

3.1.5 Forms and other documents

Forms are used to create records, checklists, surveys, or other documentation used in the creation of a product or service. Records are a critical output of any procedure or work instruction and form the basis of process communication, audit material, and process improvement initiatives.

3.2 Responsibility model

The Information Security Program uses the RACI model for assigning responsibility during its implementation. The RACI model is a common project management tool. The acronym RACI stands for:

R – **Responsible** – (also ***Recommender***)
Those who do the work to achieve the task. There is at least one role with a participation type of *Responsible*, although others can be delegated to assist in the work required.

A – **Accountable** – (also ***Approver*** or *final approving authority*)
The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those *Responsible*. In other words, an *Accountable* must sign off (approve) work that *Responsible* provides. There **must** be only one *Accountable* specified for each task or deliverable.

C – **Consulted** (sometimes ***Consultant*** or *counsel*)
Those whose opinions are sought, typically subject matter experts and with whom there is two-way communication (in other words, the *Consulted* contributes to the task or deliverable, providing input and suggested output).

I – **Informed** (also *Informee*)
Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication (as receivers to information).

3.3. Implementation Process

- BOD approves Information Security Policy and ISP Implementation Guidelines
- CEO establishes Information Security Policy Steering Committee (ISSC)
- ISSC shall include staff from Administration, IT, E&O, Accounting, HR, Legal, etc.
- ISSC responsibilities include:
  - Coordinate initial assets inventory and data classification
    ISPL includes *Data Classification Policy* and *Data Assets Inventory Form*

  - Coordinate risk assessment
    ISPL *Risk Assessment Procedure* and *Risk Register Form* can be used to support risk assessment.

  - Coordinate gap analysis
    PCI DSS (Payment Card Industry Data Security Standard) or DOE C2M2 (Cyber can be used for gap analysis which can be conducted internally or by external consultant.

  - Meeting on regular basis and use project management tools to plan, monitor and control implementation process

  - Selecting policies and standards for implementation

  - Using RACI model for assigning responsibilities for implementing each policy and standard

  - Review and recommend changes to existing policies, procedures, standards and forms

4 Related Standards, Policies, and Processes

- Inspired by "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.

5 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed

CEO/GM	BOD	Legal Department	All Employees

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

6 Approval

____ ____________________

<Insert title of approver> Date

7 Revision History

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

Insert Utility logo here

Physical and Environmental Security Policy

1 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.

2 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.

3 Policy

3.1. 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.

3.2 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*.*

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

6 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.]

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

IT Assets Accountability Policy

1 Overview/Purpose

The purpose of this policy is to ensure that all <**Utility Name**> information technology (IT) assets are accounted for, classified, inventoried, tracked, and managed throughout each IT asset's lifecycle.

Through this policy, <**Utility Name**> is establishing the baseline standards by which the Utility will manage, collect, and report information about the IT assets under its control. <**Utility Name**> may establish additional written policies, standards, processes and procedures as necessary to accomplish its business objectives.

2 Scope

All employees, contractors, consultants, temporary and other workers at <**Utility Name**> and its subsidiaries must adhere to this policy. This policy applies to IT equipment that is owned, operated, or leased by **<Utility Name>**.

3 Policy

3.1 Assets to be inventoried

All technology hardware costing over $**< X >** will be included in the inventory. Additionally, all removable storage devices will be included. All purchased software will be inventoried.

3.2 Inventory Requirements

3.2.1. As possible, all hardware assets will be tagged with a Utility inventory label with a unique number, designed to be difficult to remove.

3.2.2. Newly purchased technology, as defined above, will be tagged and recorded in the appropriate Technology Inventory.

3.2.3. Existing technology in the appropriate Technology Inventory will be physically inventoried on a periodic basis.

3.2.4. The **<person or group responsible for policy at Utility>** is responsible for establishing procedures to issue and inventory technology assigned to employees and contractors.

3.2.5. The Technology Inventory shall be available for audit.

3.2.6. The **<person or group responsible for policy at Utility>** will ensure that appropriate software licensing agreements for software used by Utility employees are in place and that the Utility is in compliance with those agreements.

3.3 Configuration Requirements

3.3.1. Newly purchased computers are configured according to the **Computer Configuration Baseline Standard**

3.3.2. Newly purchased mobile devices are configured according the **Mobile Devices Configuration Baseline Standard** {not included}

3.3.3. Newly purchased network equipment is configured according to the **Network Equipment Configuration Baseline Standard** {not included}

4 Compliance

4.1 Compliance Measurement

The <**person or group responsible for policy at Utility**> 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from SANS , "Inventory of Authorized and Unauthorized Devices" (http://www.sans.org/critical-security-controls/control/1) and "Inventory of Authorized and Unauthorized Software" (http://www.sans.org/critical-security-controls/control/2)

- IT Hardware Inventory Form

6 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.]

7 Approval

____ ____________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Data Classification Policy

1 Overview/Purpose

<Utility Name> transmits, produces, collects and uses many different type of data in fulfilling its mission. Federal and state regulations mandate the privacy and protection of certain types of data. Availability of data processed is critical to **<Utility Name>**'s mission, integrity and core functions. This Data Classification Policy shall determine how data needs to be protected, and its required availability.

2 Scope

This policy is intended to define data classes for information protection and availability. The defined classes are used by other procedures and standards.

3 Policy

3.1 Data Protection Classification

3.1.1 Public Data

Public Data is information that may be freely shared with anyone. Examples include:

- Information posted on the **<Utility Name>** website
- Publicly posted job announcements
- Newsletters

3.1.2 Internal Data

All employees have access to Internal Data.
Examples of internal data:

- General policies, procedures, guidelines, instructions
- Phone lists, organizational charts, internal job postings

Access to Internal Data does requires access authorization (at employee or contractor level), but should not be disseminated outside of **<Utility Name>** without prior authorization.

3.1.3 Sensitive Data

Sensitive Data is information that must be protected from unauthorized access, in order to safeguard the privacy or security of the organization.
Examples of Sensitive Data:

- Power grid diagrams and systems documentation
- Individual department share server folders (e.g. financial, HR)
- System design documentation

Access to Internal Data does requires access authorization (employee or contractor). Type of access (read, write, delete, etc.) to this data is controlled by RBAC (Role-Based Access Control). Sensitive Data shall be encrypted while at rest and in transit. Sensitive Data will not be disseminated to those who do not have access authorization to the data in question.

3.1.4 Confidential Data

Confidential Data is information that must be protected from unauthorized access to safeguard the privacy and/or security of the Utility's customers. Examples of Confidential Data:

- Billing and accounting data
- NDA and contracts documents

Access to Confidential Data does requires access authorization (employee or contractor). Type of access (read, write, delete, etc.) to this data is controlled by RBAC. Confidential data shall be encrypted while at rest and in transit. Confidential Data will not be disseminated to those who do not have access authorization to the data in question.

3.1.5 Regulated Data (PII, PHI, PCI CHD)

Due to federal, state and international regulations, some data requires special treatment. Examples of Regulated Data:

- PII - Personal Identification Data which is collected in CIS (Consumer Information System), GIS (Geographical Information System), etc.
- PHI - Personal Health Information
- CHD (Card Holder Data) as defined by PCI DSS (Payment Card Industry Data Security Standard)

Access to Regulated Data does requires access authorization (employee or contractor). Type of access (read, write, delete, etc.) to this data is controlled by RBAC. Regulated Data shall be encrypted at rest and in transit. Regulated Data will not be disseminated to those who do not have access authorization to the data in question.

3.2 Data Availability Classification

3.2.1 Supportive Data

Supportive data is necessary for day-to-day operations, but is not critical to the **<Utility Name>** mission, integrity or core functions.
Examples of Supportive Data:

- Announcements
- Meeting minutes
- Workstation images

3.2.2 Priority Data

Availability of Priority Data is necessary for departmental functions. Unavailability of this data may have an adverse impact on departmental missions, but would not significantly affect functions.
Examples of Priority Data:

- Reports
- Archived data
- Departmental meeting schedule

3.2.3 Critical Data

Critical Data has the highest need for availability. If this information is not available due to system downtime, modification, destruction, etc., functions and mission would be impacted. Availability of this information must be rigorously protected.
Examples or Critical Data:

- Billing
- SCADA
- OMS, etc.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

- FTC Red Flag Rules (https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business)

- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

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

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

7 Approval

_______________________________________ ____________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Data Protection & Availability Standard

1 Overview/Purpose

<Utility Name> transmits, produces, collects, and uses many different type of data in fulfilling its mission. Federal and state regulations mandate the privacy and protection of certain types of data. Availability of data processed is critical for **<Utility Name>**'s mission, integrity and core functions. The Data Protection & Availability Standards support the *Data Classification* Policy in determining how data should be protected.

2 Scope

These standards define the information assets inventory process, along with classifying data sensitivity and availability.

3 Standard

Data processed and stored at **<Utility Name>** is classified in terms of its need for protection and availability.

3.1 Data Assets Inventory

The Data Assets Inventory documents the data transmitted, collected and stored. The Data Protection & Availability Standards document should be reviewed on an annual basis or after any system changes such as:

- System retirement
- New system implementation

3.1.1 Data Assets Inventory Form

The Data Assets Inventory Form is a tracking spreadsheet that includes the following fields:

1. System
   The name of the system which is collecting and storing data (i.e., CIS, OMS, AMI).
2. System description
3. System owner

4. Data Protection Class (Public, Internal, Sensitive, Confidential, Regulated)
5. Data Availability Class (Standard, Priority, Critical)
6. Encryption methods
7. Target RTO (Recovery Time Objective)
8. Target RPO (Recovery Point Objective)
9. Current RTO (Recovery Time Objective)
10. Current RPO (Recovery Point Objective)
11. Access control methods (reference to Access Control List (ACL) if already designed and implemented)

3.2 Data Assets Protection

An employee's access to data assets is granted based on his/her organizational role at **<Utility Name>** (Role Based Access Control). The *Role Based Access Control Form* is used to design and capture the approved access level of an organizational role in each system. This form is reviewed on annual basis or after any organizational changes such as creating new position by <**person or group responsible for policy**>.

3.2.1 Master RBAC

Master RBAC is part of *Role Based Access Control Form* and document general structure of permissions to all systems.
The Master RBAC shall include the following fields:

- System name
- Organizational role name (i.e., CEO, Field Engineer, System Administrator, etc.)
- Access type (None, Read, Write, Administrator or other applicable)

3.2.2 System RBAC

A separate form is used for each system and contains defined users and separate access control structure.

The System RBAC shall include the following fields:

- System name
- Subsystem name or specific function type
- Organizational role name (i.e., CEO, Field Engineer, System Administrator, etc.)
- Access type (None, Read, Write, Administrator or other applicable)

Examples of those system may include:

- CIS application
- AMI application
- OMS
- Active Directory or file server for sharing files and printers

3.3 Data Assets Availability

The *Data Assets Inventory* provides requirements for data availability (Data Availability Class, RTO and RPO). This information helps to select the appropriate methods to satisfy RTO and RPO requirements.

3.3.1 Data Assets Availability Procedure

The Data Assets Availability Procedure shall describe:

[Explanatory Note: This procedure might very specific to the utility and template for this procedure is not provided.]

- How requested RTO and RPO are achieved (hardware and software)
- Availability monitoring
- Steps required to activate redundant resources when primary or secondary failed (if this is not automated)
- Steps required to return to normal configuration

4 Compliance

4.1 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 Responsible.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

(Cross references to industry standards)

- *Data Classification* Policy

6 Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed

IT Manager	CEO/GM	Legal COO CFO HR	All Employees

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

7 Approval

____ ____________________

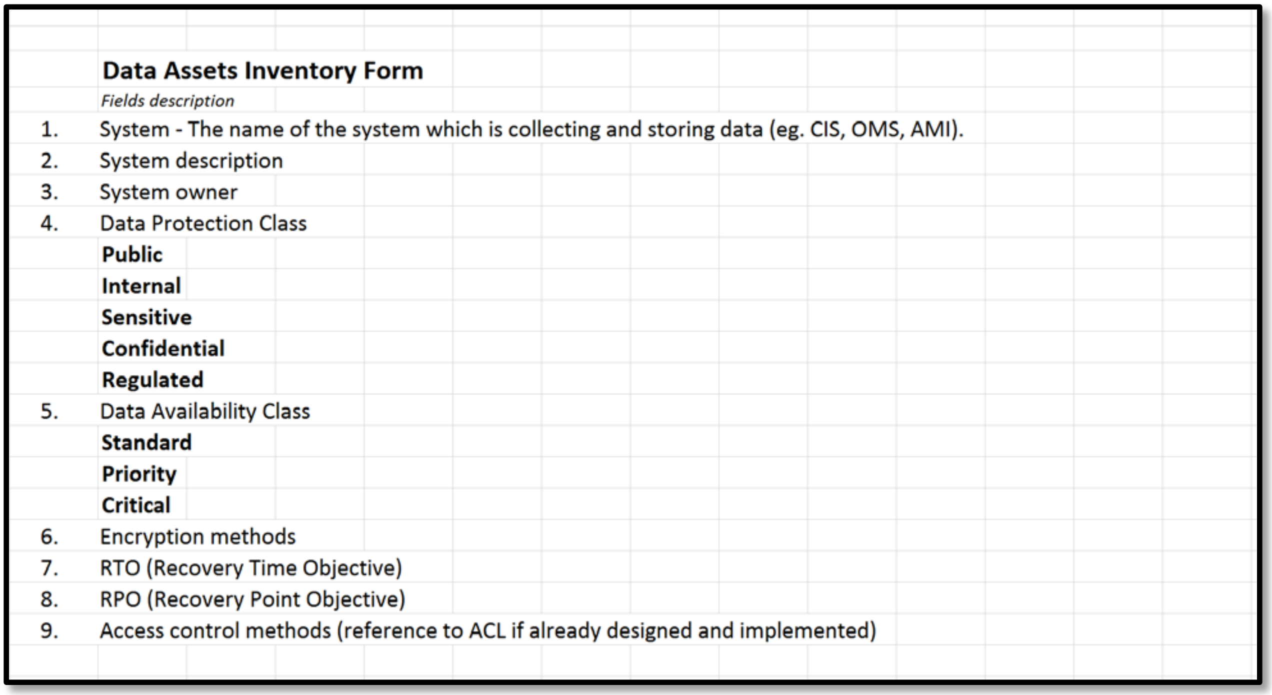
<Insert title of approver> Date

8 Revision History

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

Data Assets Inventory Form

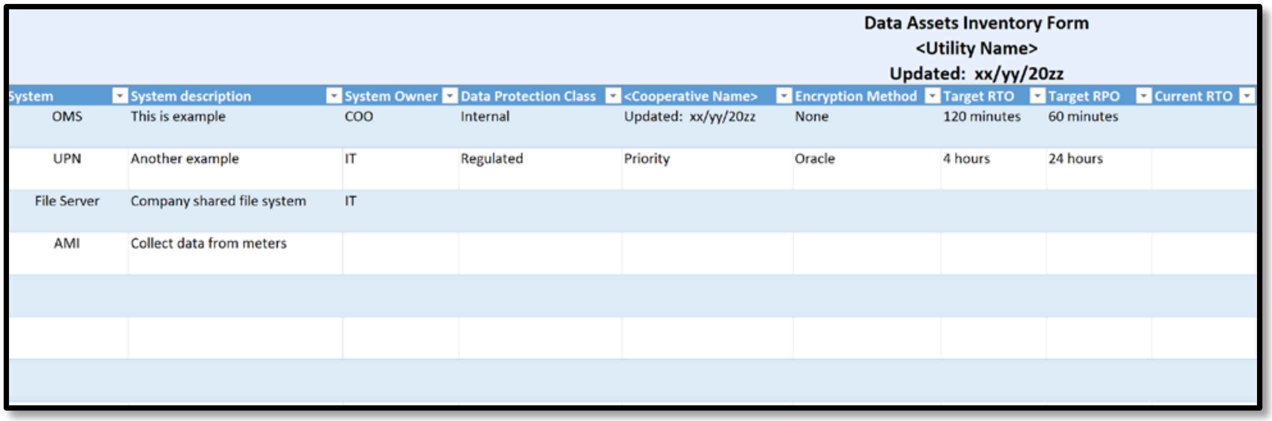
Screenshots from “Data Assets Inventory Form.xlsx”



Data Assets Inventory Form

Fields description

1. System - The name of the system which is collecting and storing data (eg. CIS, OMS, AMI).
2. System description
3. System owner
4. Data Protection Class
   - **Public**
   - **Internal**
   - **Sensitive**
   - **Confidential**
   - **Regulated**
5. Data Availability Class
   - **Standard**
   - **Priority**
   - **Critical**
6. Encryption methods
7. RTO (Recovery Time Objective)
8. RPO (Recovery Point Objective)
9. Access control methods (reference to ACL if already designed and implemented)

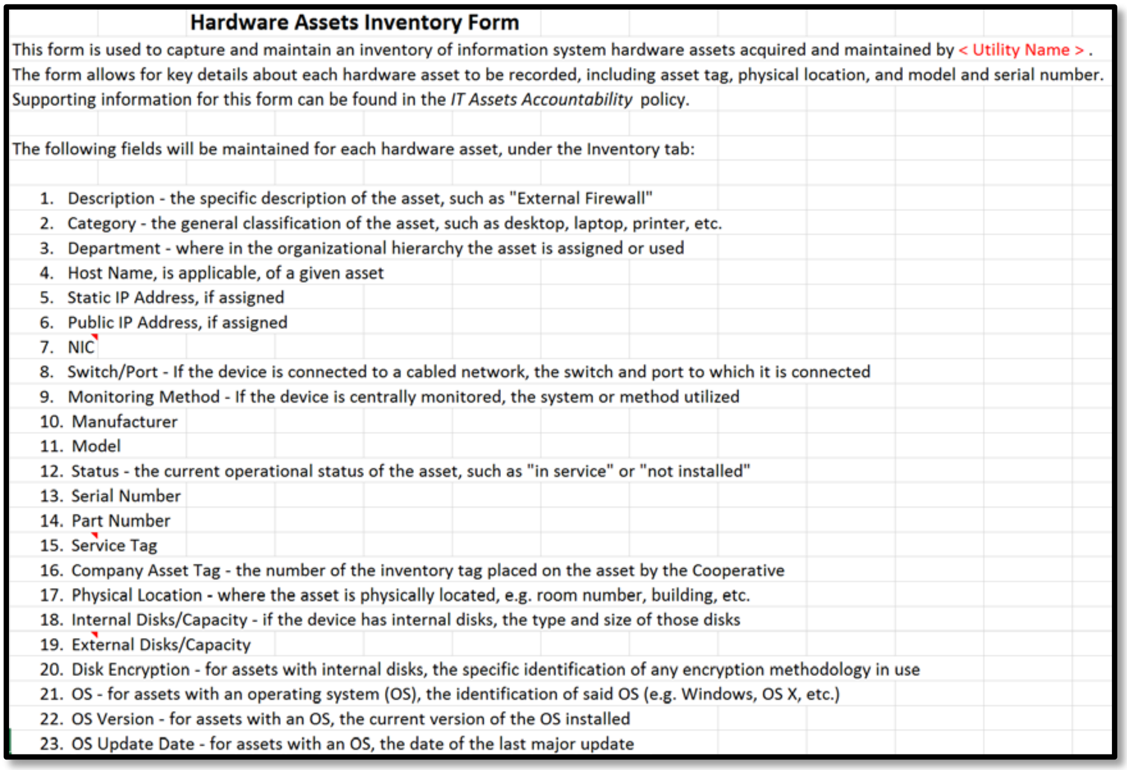


Data Assets Inventory Form
<Utility Name>
Updated: xx/yy/20zz

System	System description	System Owner	Data Protection Class	<Cooperative Name>	Encryption Method	Target RTO	Target RPO	Current RTO
OMS	This is example	COO	Internal	Updated: xx/yy/20zz	None	120 minutes	60 minutes	
UPN	Another example	IT	Regulated	Priority	Oracle	4 hours	24 hours	
File Server	Company shared file system	IT						
AMI	Collect data from meters							

IT Hardware Inventory Form

Screenshot from “IT Hardware Inventory Form.xlsx”

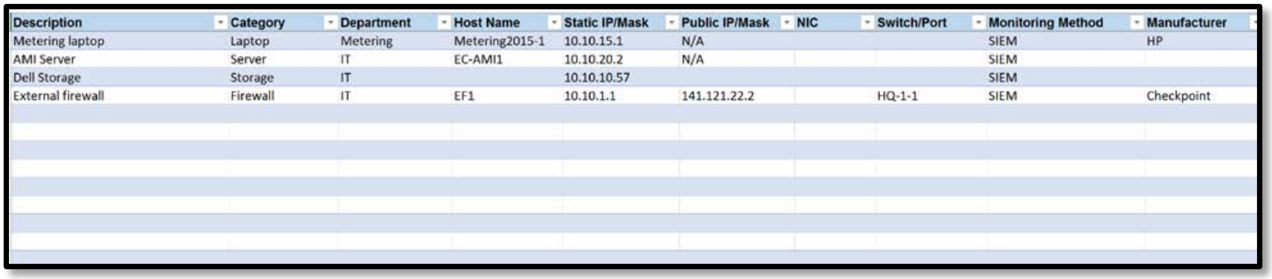


Hardware Assets Inventory Form

This form is used to capture and maintain an inventory of information system hardware assets acquired and maintained by < Utility Name > .
The form allows for key details about each hardware asset to be recorded, including asset tag, physical location, and model and serial number.
Supporting information for this form can be found in the *IT Assets Accountability* policy.

The following fields will be maintained for each hardware asset, under the Inventory tab:

1. Description - the specific description of the asset, such as "External Firewall"
2. Category - the general classification of the asset, such as desktop, laptop, printer, etc.
3. Department - where in the organizational hierarchy the asset is assigned or used
4. Host Name, is applicable, of a given asset
5. Static IP Address, if assigned
6. Public IP Address, if assigned
7. NIC
8. Switch/Port - If the device is connected to a cabled network, the switch and port to which it is connected
9. Monitoring Method - If the device is centrally monitored, the system or method utilized
10. Manufacturer
11. Model
12. Status - the current operational status of the asset, such as "in service" or "not installed"
13. Serial Number
14. Part Number
15. Service Tag
16. Company Asset Tag - the number of the inventory tag placed on the asset by the Cooperative
17. Physical Location - where the asset is physically located, e.g. room number, building, etc.
18. Internal Disks/Capacity - if the device has internal disks, the type and size of those disks
19. External Disks/Capacity
20. Disk Encryption - for assets with internal disks, the specific identification of any encryption methodology in use
21. OS - for assets with an operating system (OS), the identification of said OS (e.g. Windows, OS X, etc.)
22. OS Version - for assets with an OS, the current version of the OS installed
23. OS Update Date - for assets with an OS, the date of the last major update



Description	Category	Department	Host Name	Static IP/Mask	Public IP/Mask	NIC	Switch/Port	Monitoring Method	Manufacturer
Metering laptop	Laptop	Metering	Metering2015-1	10.10.15.1	N/A			SIEM	HP
AMI Server	Server	IT	EC-AMI1	10.10.20.2	N/A			SIEM	
Dell Storage	Storage	IT		10.10.10.57				SIEM	
External firewall	Firewall	IT	EF1	10.10.1.1	141.121.22.2		HQ-1-1	SIEM	Checkpoint

Insert
Utility
logo
here

IT Risk Management Policy

1 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.

2 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.

3 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.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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

6 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.]

7 Approval

______________________________ ______________________________

<Insert title of Accountable> Date

8 Revision History

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

Insert
Utility
logo
here

IT Risk Assessment Procedure

1 Overview/Purpose

In accordance with the *IT Risk Management Policy*, the following procedure outlines the Risk Assessment (RA) process which will be followed by **<Utility Name>**.

2 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.

3 Procedure

3.1 Risk Assessment Sequence

The RA process will be conducted using asset, threat, vulnerability model, in the following sequence:

Asset → Threat → Vulnerability = Risk

A mitigation plan will be developed for any risks with a score beyond a specified threshold. Risk Assessment can be conducted by using the *Risk Register Form*.

3.2. Asset Identification

The data asset inventory maintained under the *Data Classification Policy* will be used for the RA. Similar assets may be aggregated as appropriate for the RA process.

3.2 Threat Identification

Threats may include people, the systems they use, and conditions that could cause harm to an organization. Personnel at different levels of the organization will have different perspectives and can provide information about the risk which was not previously considered.
Some examples of threats include:

- Accidental data corruption
- Denial of service attack
- Physical theft

Threats should be related to the applicable assets and vulnerabilities.

3.3 Vulnerabilities

A vulnerability is a weakness that can be exploited by a threat and may originate from technology, the organization, the environment, or a business process.
Examples of vulnerabilities include:

- Backup restore failure
- Firewall rule error
- Not patched operating system
- Improper confidential waste disposal

Each vulnerability should be related to the impacting threat(s) and assets. Additionally, any controls that offer protection from a vulnerability should be noted. The adequacy of the controls should be estimated for each vulnerability, and considered as part of the vulnerability score.

3.4 Potential Outcome

Once the threat list has been established, each entry should have possible outcome/risk. Then risk can be scored in the following categories:

- **Asset Value** – Low (0) to Critical (4)
- **Likelihood of Threat** – Low (0) to High (2)
- **Ease of Exploitation** – Low (0) to High (2)

A total score should be produced for each threat, which is the sum of the scores given for each category.

3.5 Existing Controls

This list will primarily consist of active policies and technologies such as:

- Password change policy
- Backup policy
- Firewall

3.6 Mitigation Plan

Any vulnerabilities with a risk score of 6 or above should be listed on the mitigation plan. For each entry, a mitigation strategy should be developed. In cases where no practical mitigation strategy can be found, the risk can be accepted. If any mitigation is under way, the status of said mitigation should be shown.

The IT Manager will convene a meeting of appropriate personnel, and develop plans for mitigating risk of score 3 to 5. In the case of a temporary mitigation strategy, a long-term approach should be developed and listed as well.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

- PCI DSS Risk Assessment Guidelines
- Data Classification Policy
- Data Protection and Availability Standards

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
CIO	**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.]

7 Approval

______________________________ ______________________

<Insert title of Accountable> Date

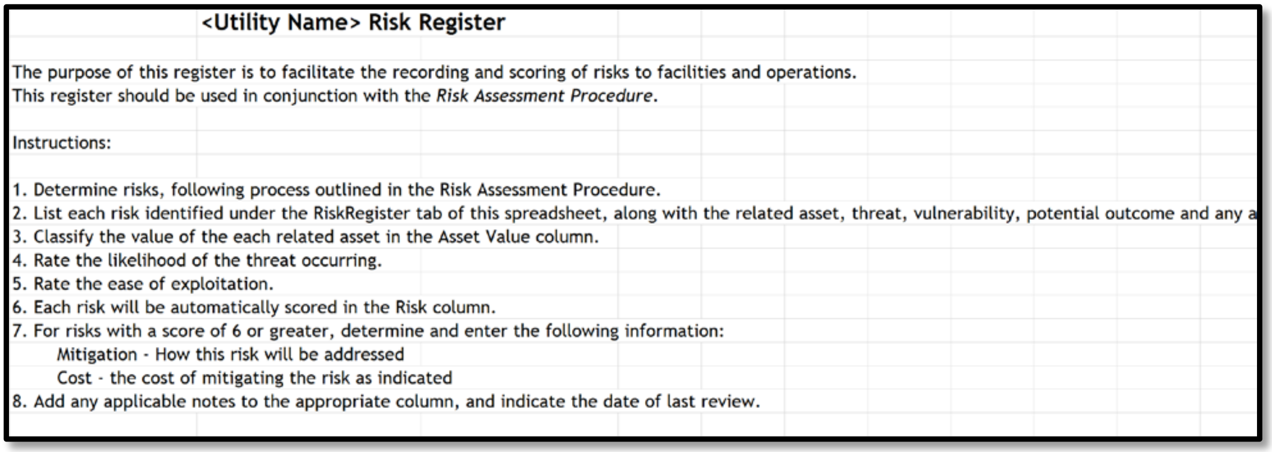
8 Revision History

Date of	Revised by	Summary of Change(s)

Change(s)		

Risk Register Form

Screenshots from “Risk Register Form.xslx”

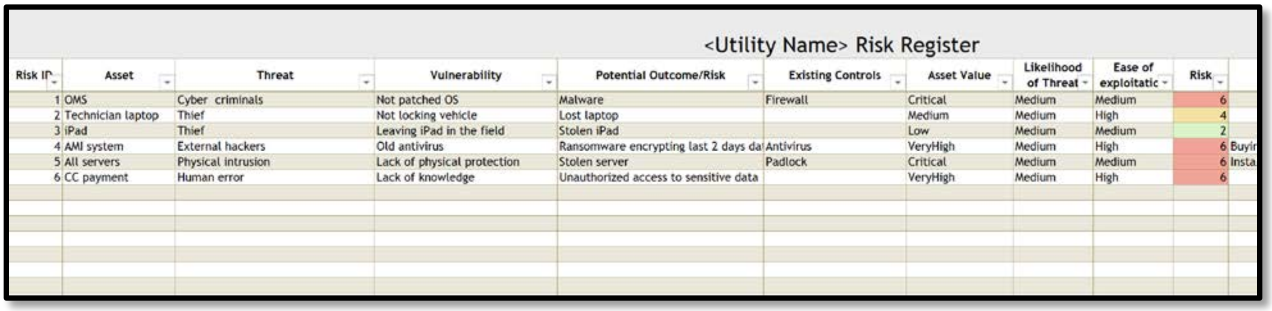


<Utility Name> Risk Register

The purpose of this register is to facilitate the recording and scoring of risks to facilities and operations.
This register should be used in conjunction with the *Risk Assessment Procedure*.

Instructions:

1. Determine risks, following process outlined in the Risk Assessment Procedure.
2. List each risk identified under the RiskRegister tab of this spreadsheet, along with the related asset, threat, vulnerability, potential outcome and any a
3. Classify the value of the each related asset in the Asset Value column.
4. Rate the likelihood of the threat occurring.
5. Rate the ease of exploitation.
6. Each risk will be automatically scored in the Risk column.
7. For risks with a score of 6 or greater, determine and enter the following information:
   Mitigation - How this risk will be addressed
   Cost - the cost of mitigating the risk as indicated
8. Add any applicable notes to the appropriate column, and indicate the date of last review.



<Utility Name> Risk Register

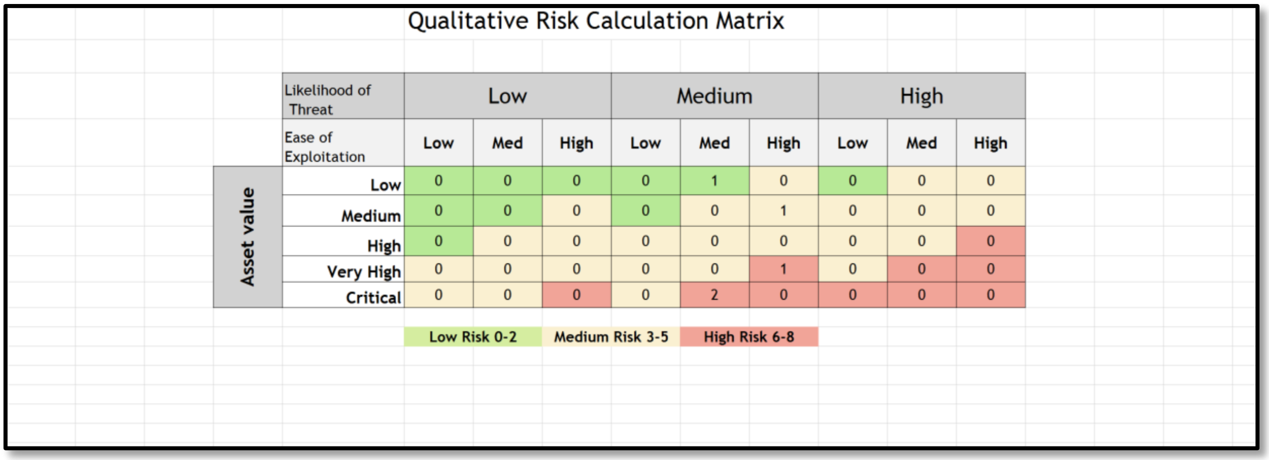
Risk ID	Asset	Threat	Vulnerability	Potential Outcome/Risk	Existing Controls	Asset Value	Likelihood of Threat	Ease of exploitatic	Risk	
1	OMS	Cyber criminals	Not patched OS	Malware	Firewall	Critical	Medium	Medium	6	
2	Technician laptop	Thief	Not locking vehicle	Lost laptop		Medium	Medium	High	4	
3	iPad	Thief	Leaving iPad in the field	Stolen iPad		Low	Medium	Medium	2	
4	AMI system	External hackers	Old antivirus	Ransomware encrypting last 2 days da	Antivirus	VeryHigh	Medium	High	6	Buyir
5	All servers	Physical intrusion	Lack of physical protection	Stolen server	Padlock	Critical	Medium	Medium	6	Insta
6	CC payment	Human error	Lack of knowledge	Unauthorized access to sensitive data		VeryHigh	Medium	High	6	

Asset Value – Low to Critical with numeric value from 0 to 4

Likelihood of Threat – Low to High with numeric value from 0 to 2

Ease of exploitation – Low to High with numeric value from 0 to 2

Risk is calculated as a sum of Asset Value, Likelihood of Threat and Ease of exploitation



Qualitative Risk Calculation Matrix

	Likelihood of Threat	Low			Medium			High		
	Ease of Exploitation	Low	Med	High	Low	Med	High	Low	Med	High
Asset value	Low	0	0	0	0	1	0	0	0	0
	Medium	0	0	0	0	0	1	0	0	0
	High	0	0	0	0	0	0	0	0	0
	Very High	0	0	0	0	0	1	0	0	0
	Critical	0	0	0	0	2	0	0	0	0

Low Risk 0-2 Medium Risk 3-5 High Risk 6-8

Insert Utility logo here

Cybersecurity Awareness Training Policy

1 Overview/Purpose

<Utility Name> recognizes that properly educated employees are an important means of cybersecurity defense. This document establishes a formal program for ongoing cybersecurity awareness training within **<Utility Name>**.

2 Scope

On an annual basis, all **<Utility Name>** employees will receive cybersecurity awareness training.

3 Policy

The Information Security Steering Committee (ISSC) defines the content of the cybersecurity awareness training, which must be updated at least yearly to account for changes in threats and industry best practices.

Training topics shall meet the following requirements:

- PCI DSS 12.6
- Red Flag Rule
- NERC CIP (if applicable)
- RUS ERP

Training should be provided in a format appropriate to the **<Utility Name>**, preferably in short segments (no longer than 10 minutes each), in the form of Computer Based Training, which should support mobile devices.

Cybersecurity Awareness training can be created in-house by **<Utility Name>** or can make use of external, commercially available content. The training shall include reporting features to ensure that employees attended and satisfactorily complete training.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

- PCI DSS Requirements 12.6 (https://www.pcisecuritystandards.org/document_library)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**HR**	**All employees**

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

7 Approval

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

Internet Access Policy

1 Overview/Purpose

<Utility Name> is committed to protecting its employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This Internet Access Policy defines the acceptable use of the Internet by employees, contractors, consultants, temporaries and other workers, including all personnel affiliated with third parties, while using utility-owned or leased equipment, facilities, Internet addresses, or domain names registered to **<Utility Name>**. The intent for publishing an Internet Access Policy is not to impose restrictions that are contrary to established culture of openness, trust and integrity.

2 Scope

This policy is intended to detail the rules of conduct for Internet use from a **<Utility Name>** computer or through corporate network and applies to all employees, contractors, consultants, temporaries and other workers, including all personnel affiliated with third parties.

3 Policy

Access to the Internet is available to employees, contractors, subcontractors, and business partners, whose duties require it for the conduct of company business. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy. Internet access may also be limited by user, to specific domains and websites or during predetermined hours, at management's discretion.

3.1 Acceptable Use

<Utility Name> provides Internet access to facilitate the conduct of company business. Occasional and incidental personal Internet use is permitted for individuals whose duties otherwise require Internet access, if such use does not interfere with their work, the company’s ability to perform its mission, does not directly or indirectly interfere with business operations, IT facilities or electronic mail services, and meets the conditions outlined in official company policies.

3.2 Prohibited Use

Prohibited Internet activities, whether during normal working hours or on personal time, using company equipment include, but are not limited to, the following:

- Browsing explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that the company has determined to be inappropriate.
- Accessing, retrieving, or printing text and graphical information which exceeds the bounds of generally accepted standards of good taste and ethics.
- Posting, sending or acquiring sexually explicit or sexually oriented material, hate based material, hacker-related material, or other material determined by **<Utility Name>** to be inappropriate.
- Posting or sending sensitive information outside of the company without management authorization.
- Using other services available on the Internet such as File Transfer Protocol (FTP) or Telnet, on systems for which the user does not have a named account.
- Posting commercial announcements of advertising material without management authorization.
- Promoting or maintaining a personal or private business, including offering services or merchandise for sale.
- Receiving news feeds and push data updates, unless the material is required for company business.
- Accessing or transferring information that is a violation of local, state, federal, or international copyright laws, or that contradicts the intent and spirit of these policies or procedures.
- Downloading any applications or software that are not specifically authorized by **<IT Manager>**.
- Engaging in any activity, which would compromise the security and integrity of any company computer or system.
- Engaging in any fund raising activity, endorsing any product or services, participating in any lobbying activity, or engaging in any political activity without management authorization.
- Downloading any file from the Internet without prior approval, unless the download is from an authorized business partner. All requests will be sent through <**person or group responsible for policy**> to verify the source and security of the download. The access may be approved for only a single download or the user may be granted permanent download rights, depending on the business requirements. Once download access is granted, all aspects of this policy apply. Users are not to download screen savers, animated cursors, weather alert programs or other software programs from the Internet that can introduce spyware, ad-ware, and viruses or impact computer performance.

3.3 User Responsibilities

Use of computer equipment and Internet access to accomplish job responsibilities will always have priority over incidental personal use. To avoid capacity problems and to reduce the susceptibility of information technology resources to malware, Internet users shall comply with the following guidelines:

- Files obtained via the Internet may only be stored on individual PC hard drives, or on file server shares, after they have been scanned for viruses.
- Video and voice files may not be downloaded from the Internet except when they will be used to serve an approved business function.
- Streaming Video and Music greatly impact corporate network bandwidth and access speeds and may not be initiated except when they will be used to serve an approved business function.
- Users shall follow existing security policies, and procedures in the use of Internet services, and shall refrain from any practices, which might jeopardize computer systems and data files, including but not limited to malware attacks, when downloading files from the Internet.
- It is suggested that users learn about, and adhere to Internet etiquette, customs, and courtesies, including those procedures and guidelines to be followed when using remote computer services and transferring files from other computers.
- Users shall conduct themselves in a way that reflects positively on **<Utility Name>**, since they are identified as company employees on the Internet.

3.4 Expectation of Privacy

The computers,computer accounts, and network and Internet resources that are provided for users are intended to assist them in the performance of their jobs. Users should not have expectation of privacy while using any such resources. Users of the Internet should be aware that most sessions on the Internet are not private.

3.5 System Monitoring

<Utility Name> has the right to monitor any and all aspects of its computer systems and networks, including but not limited to, adherence to the Internet Access policy. Circumvention of any monitoring software or tools is prohibited and is subject to the same penalties as any other violation of the Internet access policy.

3.6 **<Utility Name>** Liability

<Utility Name> has no liability for any issues employee may experience with personal accounts (banking for example) while accessing Internet from company network or using company mobile devices.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

4.4 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.

- Adapted from "Internet Usage Policy" (http://www.sans.org/security-resources/policies/retired/doc/internet-usage-policy)

5 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**		**All Employees**

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

6 Approval

______________________________ ______________

<Insert title of approver> Date

7 Revision History

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

Insert
Utility
logo
here

Acceptable Use Policy

1 Overview/ Purpose

<Utility Name> is committed to protecting its employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. All systems and accounts, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet Web browsing, and FTP, are the property of the utility. These systems and accounts are to be used for business purposes in serving the interests of the company, and our customers in the course of normal operations, except where incidental personal use is explicitly permitted. **<Utility Name>**'s intentions in publishing an Acceptable Use Policy are not to impose restrictions that are contrary to **<Utility Name>**'s established culture of openness, trust and integrity.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every system user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment and the Information Technology (IT) infrastructure at. These rules are in place to protect the employees and **<Utility Name>.** Inappropriate use exposes the utility to risks including computer malware attacks, compromise of network systems and services, and legal/compliance issues. The policy balances the employee's ability to benefit fully from information technology with the company's need for secure and effectively allocated IT resources.

2 Scope

This policy applies to employees, contractors, consultants, temporaries and other workers, including all personnel affiliated with third parties. This policy applies to all equipment, software and/or applications that is owned, leased, or used by **<Utility Name>**.

3 Policy

3.1 General Use and Ownership

3.1.1. While the network administration team seeks to provide a reasonable level of privacy, users should be aware that data they create on corporate systems remains the property of the company. Because of the need to continually monitor the internal network in order to protect **<Utility Name>**'s IT resources and information, management cannot guarantee the confidentiality of personal information stored on any device belonging to the utility or in files on the network.

3.1.2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of company systems and networks, unless such personal use is otherwise defined in overall company policies. In the absence of such policies, Company owned IT equipment, computers, networks, and related services may be used for incidental personal use purposes provided that:

- Usage is reasonable and does not interfere with work productivity.
- Usage does not directly or indirectly interfere with business operations, IT facilities or electronic mail services.
- Usage does not burden the utility with noticeable incremental cost.

If there is any uncertainty as to what constitutes acceptable personal use, employees should consult their supervisor or manager, who will make the final determination.

3.1.3. Since all Internet, network, and system activities may be monitored, all personnel accessing such systems shall have no expectation of privacy.

3.2 General Use and Ownership

3.2.1. Users may not encrypt any emails without obtaining written permission from their supervisor and **<person or group responsible for policy>**. If approved, the encryption key(s) must be made known to **<person or group responsible for policy>.**

3.2.2. Data residing on corporate IT systems may be classified as either confidential or not confidential, as defined by the company's *Data Classification* Policy. Examples of confidential information include but are not limited to: company private, corporate strategies, sensitive competitive information, trade secrets, specifications, and customer details and lists. Employees should take all necessary steps to prevent unauthorized access to this information.

3.2.3. For security, network maintenance, and policy compliance purposes, authorized individuals may monitor equipment, systems and network traffic at any time, per the *System Logging and Monitoring* Policy.

3.2.4. Employees must use extreme caution when opening email attachments received from unknown senders which may contain various forms of malware. Although **<Utility Name>** utilizes Anti-Virus software on each workstation and server {as well as filtering all inbound email through an outside security service,} some unsafe attachments may still find their way through the defenses. If attachments are received that were not expected, their validity should be confirmed with the sender via phone, prior to opening them. If any questions or uncertainty exist, please contact **<person or group responsible for policy>** prior to opening the attachment.

3.2.5. Because information contained on portable and laptop computers is especially vulnerable, special care should be exercised to protect both the computer and its information.

3.2.6. Employees shall not use company email, or other facilities to post to news groups, message boards, or websites unless the posting is in the course of assigned business duties.

3.3 Passwords

Please refer to the Password Policy.

3.4 Anti-Virus Protection and Prevention

All workstations will be equipped with anti-virus software that cannot be disabled by non-IT staff members. Employees will be educated about safe anti-malware practices such as, but not limited to;

- Opening unexpected attachments or following links included in emails
- Downloading files from unknown sources
- Deleting spam, chain mails, junk emails
- NOT trusting any source for virus protection patches than those provided by the IT Department.

3.5 Unacceptable Use

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

3.5.1 System and Network Activities

- Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal, or international law, while utilizing company-owned resources.
- Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by **<Utility Name>**.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, or the installation of any copyrighted software for which the utility or the end user does not have an active license.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g., viruses, worms,, or other forms of malware)
- Using company computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any company account.
- Making statements about warranty, expressly or implied, unless it is a part of assigned job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an authorized user, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of assigned duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service (DOS), and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to **<person or group responsible for policy>** is made.
- Executing any form of network monitoring which will intercept data not intended for the intercepting employee, unless the activity is a part of the employee's assigned duties.
- Circumventing user authentication or the security of any computer, network, or account.
- Interfering with or denying service to any user (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind with the intent to interfere with, or disable, a user's usage of any system, network, or application, via any means.
- Providing information about, or lists of, employees to parties outside **<Utility Name>** without Human Resources Department approval.

3.5.2 Email and Communications Activities

The Email system is the property of the utility, and as such shall not be misused in any way, including but not limited to the following:

- Sending unsolicited Email messages, including the sending of "junk email" or other advertising material to individuals who did not specifically request such material (spam), unless part of a company-approved targeted marketing campaign.
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Sending or forwarding inappropriate emails, including any of the following: disruptive or offensive messages, still images, audio, or video images, including but not limited to offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or

national origin. If you receive an email of this nature, promptly notify your immediate supervisor or manager.

- Forging or attempting to forge email messages.
- Disguising or attempting to disguise your identity when sending email.
- Sending email messages using another person's e-mail account unless authorized to do so.
- Copying a message or attachment belonging to another user without permission of the originator.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of Usenet Newsgroups or message boards.

For additional information please refer to the the *E-Mail Use Policy*

3.5.3 Internet Access Activities

The following uses of the Internet, either during working hours or personal time, using company equipment or facilities, are strictly prohibited:

- Accessing, retrieving, or printing text and graphical information which exceeds the bounds of generally accepted standards of good taste and ethics.
- Using the Internet to access other systems for which the user has no authorization.
- Using Internet or Internet connections to access or transfer information that is in violation of local, state, federal, international, or copyright laws, or in a way that contradicts the intent or spirit of these policies and procedures.
- Engaging in personal commercial activities on the Internet, including offering services or merchandise for sale.
- Engaging in any activity which would compromise the security of any company computer or system.
- Endorsing any product or services, participating in any lobbying activity, or engaging in any political activity. The prohibition against engaging in any political activity or fundraising activity does not apply to employees that have authorization.
- Initiating non-work-related Internet sessions using company information resources from remote locations. That is, employees shall not connect into company resources from home or other noncompany locations for the purpose of participating in non-job-related Internet activities.
- Engaging in the transmittal of **<Utility Name>** information or data for non-business purposes and/or personal gain or benefit.

For additional information please refer to the Internet Access Policy

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from "Acceptable Use Policy" (http://www.sans.org/security-resources/policies/general/doc/acceptable-use-policy)

6 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.]

7 Approval

______________________________ ______________________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Password Policy

1 Overview/Purpose

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of **<Utility Name>**'s resources. All users, including contractors and vendors with access to **<Utility Name>** systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides in any **<Utility Name>** facility, or is used to conduct company business.

3 Policy

3.1 Password Creation

1. All user-level and system-level passwords must conform to the Password Construction Guidelines.
2. Users shall never use the same password for an account that is used for other non-company access (for example, personal ISP account, option trading, benefits, etc.).
3. Excluding Single Sign-On, users must not use the same password for multiple systems.
4. User accounts that have administrator/system-level privileges must have a unique password from all other accounts held by that user.
5. All default passwords must be changed on any devices before they are installed at a **<Utility Name>** facility.
6. All User Accounts will be created with a random, single-use password. The user will be required to change the password at their first login.

3.2 Password Change

1. All system-level passwords (for example, root, enable, application administration accounts, etc.) must be changed on a reasonable periodic basis.

2. All user-level passwords (for example, email, web, desktop computer, etc.) must be changed at least every 90 days.

3. Password cracking or guessing audits may be performed on a periodic or random basis by the **<person or group responsible for policy>**. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the *Password Construction Guidelines*.

4. Password changes may be required upon identification or notification of a cybersecurity incident or threat.

   [If utility is processing credit cards, passwords should be changed every 90 days to satisfy PCI DSS requirements]

3.3 Password Protection

1. Passwords must not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, IT, and/or family members.

2. Passwords must not be inserted into email messages or other forms of electronic communication.

3. Passwords must not be revealed over the phone to anyone.

4. Passwords must not be revealed on questionnaires or security forms.

5. Hints should never be provided as to the format of a password (for example, "my family name").

6. Passwords must not be written down or stored anywhere in an office, home, or any other location. Passwords must not be stored in a file on a computer system or mobile devices (phone, tablet) in clear text.

7. The "Remember Password" feature of applications must not be used (for example, web-based systems).

8. Any user suspecting that his/her password may have been compromised must report the incident to **<person or group responsible for policy>**, and change all passwords immediately.

3.4 Storing passwords

<Utility Name> may provide their employees with a password vaulting or identity management system for storing passwords to different systems. Password for accessing these programs shall use the same rule for password structure. Employee may be permitted to store also their personal passwords in such a system, but access to that system cannot be shared.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from "Password Protection Policy" (http://www.sans.org/security-resources/policies/general/pdf/password-protection-policy)

- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
CIO	**CEO/GM**		**All Employees**

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

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Password Construction Guidelines

1 Overview/Purpose

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the Cisco network. This guideline provides best practices for creating secure passwords

The purpose of this guidelines is to provide best practices for the created of strong passwords.

2 Scope

This guideline applies to employees, contractors, consultants, temporary and other workers at Cisco, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

3 Statement of Guidelines

3.1 Passwords

All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.

- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”
- You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.
- (NOTE: Do not use either of these examples as passwords!)

3.2 Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

- Adapted from SANS "Password Construction Guidelines" (https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines)

- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**		**All Employees**

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

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

User Account Management Policy

1 Overview/Purpose

User Accounts control access to <**Utility Name**>'s technology resources, including networks, systems, and software applications. The proper creation, control, and supervision of all User Accounts is vital to <**Utility Name**>'s security and ability to maintain its operations.

The purpose of this policy is to establish a formal process to ensure that User Accounts are appropriately created, securely used, and terminated as required in a timely fashion. This policy is necessary to safeguard the confidentiality and integrity of <**Utility Name**>'s information, and to protect its customers.

2 Scope

All employees, contractors, consultants, temporary and other workers at <**Utility Name**> and its subsidiaries must adhere to this policy. This policy applies to IT systems that are owned, operated, or leased by **<Utility Name>** or registered under a company-owned network domain.

3 Policy

3.1 General

The <**person or group responsible for policy**> is responsible for ensuring that this policy is adhered to. All authorized users will be provided one or unique User Accounts for their sole use. All such accounts must be uniquely identifiable by an assigned user name. All accounts must have a password that complies with the *Password Policy*.

3.1.1 Individual Accounts

Individual, named accounts are required when accessing IT resources. Users are accountable for their actions, which can be reviewed via audit trails maintained by the systems to which they have access rights. Individual users must adhere to the terms and conditions of the *Acceptable Use Policy*.

3.1.2 Administration (Privileged) Accounts

IT Administrative staff can be granted privileged accounts that permit elevated access rights for specific systems and/or applications, as needed for support and maintenance. Generic/built-in privileged accounts (e.g. Windows domain and local administrator, etc.) shall not be used for daily systems administration. A named, privileged account must be used instead.

3.1.3 Application-Specific Accounts

An application-specific account controls access to an individual application Access rights and privileges are configured within each application. These accounts will typically have the same name as the user's primary account.

3.1.4 Guest/Group Accounts

Guest/group accounts are not permitted on **<Utility Name>**'s systems or applications. All users, permanent or temporary, must have a unique, named account.

3.2 Account Creation

3.2.1 New employee account

When a new employee is hired, the hiring Manager will submit an *IT Employee Change Form* which specifies the Organizational Role of new employee. Based on the Organizational Role, the IT Department will create permissions using Role Based Access Control (RBAC) procedures, and a unique temporary password.

A user is not permitted, under any circumstances, to inherit a User Account that was originally assigned to another user. Before access is given to an account, all users should be provided with the **<Utility Name>** Acceptable Use Policy. {Or any other policy that might pertain to using the Coop’s IT resources}

3.2.2 New software applications

While implementing a new application, the IT Department will create an RBAC structure in coordination with system owner. User Accounts for the new system shall be added based on the new RBAC structure.

3.3 Account Deletion

A user’s manager must immediately notify IT or HR. of changes in a user’s employment status (departure, extended leave) and submit *IT Employee Change Form*. The IT Department will then immediately disable or remove all associated User Accounts.

3.4 Account Management

The IT Department will:

- Ensure that disabled User Accounts are not re-issued to another user.
- Leave the associated User Account disabled for 30 days to facilitate the disposition of files or other resources assigned to the Account. (The User Account will be deleted after 30 days).
- Modify User Accounts in response to events like name changes, accounting changes, permission changes, or office transfers.

- Remove, after consultation with a user's manager, redundant User Accounts that are no longer required.
- Periodically review existing User Accounts for validity.
- Grant Supervisors access to an account if an employee is involuntarily removed from a position to ensure continuity of communication for business purposes. Also, upon special request, a supervisor will be granted access to the account after an employee voluntarily terminates their employment.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from SANS , "Inventory of Authorized and Unauthorized Devices" (http://www.sans.org/critical-security-controls/control/1) and "Inventory of Authorized and Unauthorized Software" (http://www.sans.org/critical-security-controls/control/2)

6 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.]

7 Approval

____ ______________________

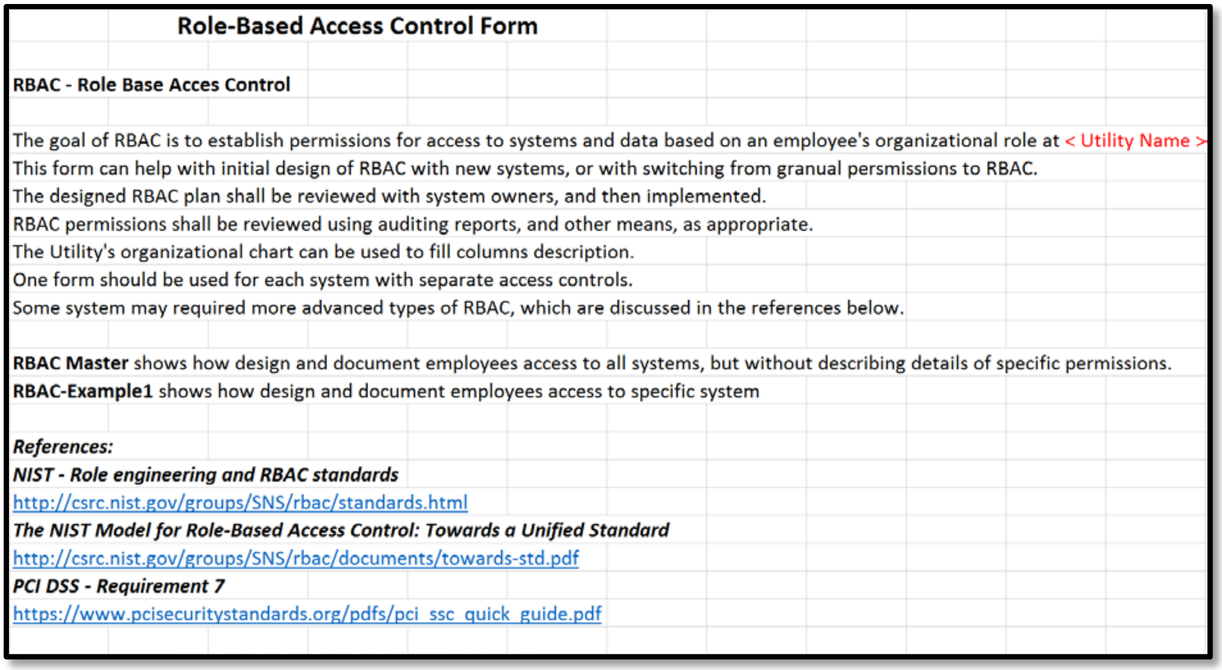
<Insert title of approver> Date

8 Revision History

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

Role-Based Access Control Form

Screenshot from “Role-Based Access Control Form.xslx”



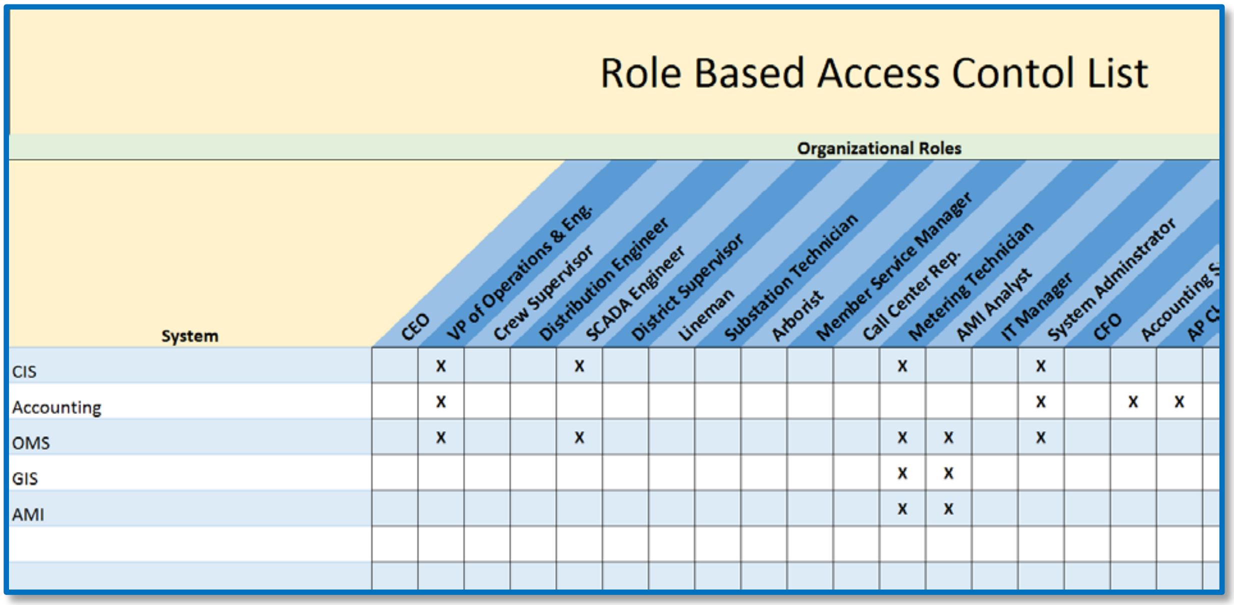
Role-Based Access Control Form

RBAC - Role Base Acces Control

The goal of RBAC is to establish permissions for access to systems and data based on an employee's organizational role at < Utility Name >
This form can help with initial design of RBAC with new systems, or with switching from granual persmissions to RBAC.
The designed RBAC plan shall be reviewed with system owners, and then implemented.
RBAC permissions shall be reviewed using auditing reports, and other means, as appropriate.
The Utility's organizational chart can be used to fill columns description.
One form should be used for each system with separate access controls.
Some system may required more advanced types of RBAC, which are discussed in the references below.

RBAC Master shows how design and document employees access to all systems, but without describing details of specific permissions.
RBAC-Example1 shows how design and document employees access to specific system

References:
NIST - Role engineering and RBAC standards
http://csrc.nist.gov/groups/SNS/rbac/standards.html
The NIST Model for Role-Based Access Control: Towards a Unified Standard
http://csrc.nist.gov/groups/SNS/rbac/documents/towards-std.pdf
PCI DSS - Requirement 7
https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf



Role Based Access Contol List

	Organizational Roles																	
System	CEO	VP of Operations & Eng.	Crew Supervisor	Distribution Engineer	SCADA Engineer	District Supervisor	Lineman	Substation Technician	Arborist	Member Service Manager	Call Center Rep.	Metering Technician	AMI Analyst	IT Manager	System Adminstrator	CFO	Accounting S	AP Cl
CIS		X			X							X			X			
Accounting		X													X		X	X
OMS		X			X							X	X		X			
GIS												X	X					
AMI												X	X					

Insert Utility logo here

Personnel Security Policy

1 Overview/Purpose

Understanding the importance of cyber and personnel security via individual responsibilities and accountability is paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific, training as well as personnel background verifications. The security awareness and training information needs to be continuously updated and reinforced.

The purpose of this Policy is to establish the background check requirements and processes for **<Utility Name>** prospective employees, current employees, volunteers and contractors in order to protect employees, membership, board members, and other associated parties, and to establish basic awareness training requirements. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with computer users.

2 Scope

This Policy applies to all employees, vendors, contractors, partners, collaborators, interns, and any others, henceforth referred to as an Applicant, who will be employed by or conduct business for **<Utility Name>** that are in contact with financially sensitive information and/or security sensitive information.

3 Policy

The **<HR Department Name>** is solely authorized to conduct and oversee the background check process pursuant to this policy on behalf of **<Utility Name>.**

<HR Department Name> may work with law enforcement or contract with outside agencies in executing any of the obligations set forth in this Policy. **<HR Department Name>** is responsible for making decisions regarding what type of background check is appropriate, interpreting background check records and information, determining whether an Applicant is eligible for employment, and for making personnel recommendations to the Hiring Authorities.

Notwithstanding this Policy, nothing precludes **<HR Department Name>** from conducting a background check on any individual when **<HR Department Name>,** in consultation with the Hiring Authority and Legal Counsel, determine that a background check is necessary.

Hiring Authorities are responsible for initiating the background check process by contacting **<HR Department Name>**.

Applicants must consent to a background check to be considered for a position. Any Applicant who refuses to consent to the background check, refuses to provide information necessary to conduct the background check, or provides false or misleading information will not be considered for the position for which s/he has applied. Any Applicant, or current employee, who is found to have provided false or misleading information related to the background check, may be subject to disciplinary action, up to and including termination.

All **<HR Department Name>** employees are responsible for ensuring the integrity and confidentiality of the background check process. The **<HR Department Name>** shall define all positions that meet the criteria for financial sensitivity, security sensitivity and shall develop a program for periodically following up on hired individuals to assure there have been no events requiring a revocation of privileges.

3.1 Security Requirements

3.1.1 Reference checks

Reference checks must be completed for all final applicants. The **<HR Department Name>** is responsible for conducting reference checks.

3.1.2 Criminal screening

A criminal history check must be conducted for all final applicants, unless a criminal history check has been conducted within the previous three years while employed with **<Utility Name>**.

3.1.3 Financial screening

Financial history check must be conducted for final applicants for positions that have access to any sensitive information.

3.1.4 Employee self-disclosure requirements - criminal conviction or felony charge

Current employees are required to self-disclose criminal convictions or felony charges against them that occur on or after the effective date of this policy within (2) two business days of the conviction or felony charges. This information should be reported to **<HR Department Name>**. Employees failing to self-disclose may be subject to disciplinary action, up to and including termination.

The **<person or group responsible for this Policy>** in coordination with the **<HR Department Name>** will implement a program communicating **<Utility Name>** expectations relating to cybersecurity. This program shall include periodic training and formal acceptance of computer use polices.

3.2 Training Requirements

3.2.1. All new users must attend an **<Utility Name>** approved security awareness training class, prior to, or at least within 14 business days of being granted access to any information systems.

3.2.2. All users must sign an acknowledgement stating they have read and understand **<Utility Name>** requirements regarding computer security policies and procedures.

3.2.3. All users (employees, contractors, interns, vendors, consultants, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect **<Utility Name>** information resources.

3.2.4. **<person or group responsible for policy at Utility >** must prepare, maintain, and distribute one or more information security manuals that concisely describe **<Utility Name>** information security policies and procedures.

3.2.5. All users must attend computer security compliance training annually, and pass the associated examination, if applicable.

3.2.6. **<person or group responsible for policy at Utility>** must develop and maintain a process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

4 Compliance

4.1 Compliance Measurement

The <**person or group responsible for policy at Utility**> 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from University of Colorado Boulder Background Check Policy

- ISO 27001 Outsourcing Security Policy Section 5.4
  www.iso27001security.com/ISO27k_Model_policy_on_outsourcing.docx

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
HR	**CEO/GM**	**CIO** **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.]

7 Approval

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Email Use Policy

1 Overview/Purpose

<Utility Name> is committed to protecting its employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This email Policy defines the proper use of the electronic mail system (Email), and the uses of it that **<Utility Name>** deems as acceptable and unacceptable. Users shall make every effort to prevent tarnishing the utility's public image and themselves. When email is sent out from **<Utility Name>**, the general public will tend to view that message as an official policy statement from the company. **<Utility Name>**'s intentions in publishing an Email Use Policy are not to impose restrictions that are contrary to **<Utility Name>**'s established culture of openness, trust and integrity.

2 Scope

This policy is intended to detail the rules of conduct for Email sent from a **<Utility Name>** Email address or through the company's Email server, and applies to all employees, contractors, consultants, temporaries and other workers, including all personnel affiliated with third parties.

3 Policy

3.1 Prohibited Use

The Email system referenced in this policy is the property of **<Utility Name>** and shall not be used for the creation or distribution of any of the following:

- Sending or forwarding Emails consisting of any of the following: disruptive or offensive messages, including but not limited to offensive comments about race, gender, color, disabilities, age, sexual orientation, pornography, obscenity, religious beliefs and practice, political beliefs, or national origin. If you receive an Email of this nature, notify your immediate supervisor.
- Forging or attempting to forge Email messages.
- Disguising or attempting to disguise your identity when sending Email.
- Sending Email using another person's account.
- Sending chain letters or offensive joke emails from a company Email account.
- Forwarding of company confidential messages to external Email addresses.

- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.
- Accessing copyrighted information in a way that violates copyright laws.
- Breaking into the company's or another organization's systems, or unauthorized use of a password/mailbox.
- Transmitting unsolicited commercial or advertising material unless part of a company-approved targeted marketing campaign.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus or malware into the corporate network.

Email generated and sent from a **<Utility Name>** Email account should be limited to business content only. Emails shall not contain content, signature lines, or images promoting unsolicited personal views on social, political, religious or other non-business related matters.

3.2 Best Practices

<Utility Name> considers Email as an important means of communications and recognizes the importance of proper Email content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an Email as they would for any other communication. Therefore, the company requires users to adhere to the following guidelines.

3.2.1 Writing Emails:

- Write well-structured Emails, and use short, descriptive subjects.
- **<Utility Name>**'s Email style is informal. Use of common salutations is acceptable such as “Hi” or “Dear” and the name of the person, and ending with “Best Regards”.
- Signatures should include pertinent information relative to your job classification such as your name, job title, company name, and company logo's only. A disclaimer will be added underneath your signature, as described below. Signature lines shall not contain statements conveying religious, political, or other such references.
- Users should spell check all emails prior to sending. This can be set to be performed automatically by most Email programs.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending.
- Do not write in ALL CAPITAL LETTERS.
- Do not use Blind Carbon Copy (bcc) fields unless the bcc recipient is aware you will be copying the message to him/her and knows what action, if any, to take. The bcc recipient should be aware that they were copied without other recipient's knowledge.
- If you forward Emails, state clearly what actions you expect the recipient to take.

- Only send Emails for which the content could be displayed publicly. If they cannot be displayed publicly in their current state, consider rephrasing the Email or using another means of communication.
- Only mark Emails as important if they really are important.
- Don't set every Email to require a read receipt, only those that really require it.
  <IT Manager can add guidelines as to what kind of Emails requires a read receipt>

3.2.2 Replying to Emails:

- Emails should be answered in a timely manner.
- Users should endeavor to answer priority Emails as soon as possible.
- Priority Emails are Emails from customers and business partners.

3.3 Personal Use

<Utility Name> Email services may be used for incidental personal purposes, provided that:

- Usage is reasonable and does not interfere with work productivity.
- Non-work related Email is saved in a separate folder from work-related Email.
- Such use does not directly or indirectly interfere with business operations, IT facilities or Email services.

It is recommended that anyone using Email for personal reasons have a separate Internet Email account such as Google Gmail, Yahoo Mail, or Hotmail. This will put fewer burdens on the **<Utility Name>** Email servers allowing the system to work more efficiently.

3.4 Conducting <Utility Name> business using personal Email accounts

No business activities related to **<Utility Name>** will be conducted using a personal email account. All company business involving the sending or receipt of Email will take place using as assigned company Email account.

3.5 Email Retention

Email retention is subject to the Data Retention Policy.

3.6 Expectation of Privacy

The Email accounts and systems provided for company users are intended to assist them in the performance of their jobs. Users should not have any expectation of privacy while using **<Utility Name>**'s Email system.

3.7 Encryption

Users may not encrypt any Emails without obtaining written permission from their supervisor and **<person or group responsible for policy>**. If approved, the encryption key(s) must be made known to **<person or group responsible for policy>**.

3.8 Disclaimer

The following disclaimer will be added to each outgoing Email:

> ***Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, copy, use, disclosure, or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply Email and destroy all copies of the original message.***

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from "Remote Access Policy"
  http://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed

IT Manager	**CEO/GM**		**All Employees**

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

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

System Acceptance and Configuration Policy

1 Overview/Purpose

This policy establishes the requirement that security measures and configuration settings must be applied to all devices connecting to the network, including new devices as well as vendor and contractor devices that physically or remotely connect to the network.

2 Scope

This policy applies to all technology resources owned or operated by **<Utility Name>.** All users (employees, contractors, vendors or others) of technology resources are responsible for adhering to this policy.

3 Policy

Devices such as workstations, servers, network components, and mobile devices, as well as standard software deployments, such web servers or databases, should each have a standard configuration baseline maintained by the **<person or group for policy >**.

The baseline configuration should be reviewed and updated when required due to a significant configuration change, such as an operating system upgrade or hardware change, or a demonstrated vulnerability; as part of a system component installation or upgrade; or at least on a yearly basis.

At minimum, the baseline configuration for each category of device shall include:

- Standard operating system/installed applications with current version numbers
- Standard software configuration for workstations, servers, network components, and mobile devices and laptops, for each internal division
- Up-to-date patch level information
- Security configuration, including disabled services, ports, etc.

The configuration baseline may be less formal for devices or systems of limited size and scope, such as cell phones and tablets.

Additionally, **<person or group responsible for policy >** shall:

1. Monitor systems for configuration baseline and policy compliance. Automated tools should be used to apply initial configurations, and to efficiently identify when a system is not consistent with the approved baseline configuration and when remediation actions are necessary.
2. Reapply all baseline configurations to systems, as appropriate, when a system undergoes a material change, such as an operating system upgrade.
3. Modify individual system configurations or baseline configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning and/or security audits.
4. Before a system is placed into production, **<person or group responsible for policy >** shall implement the baseline configuration settings; identify, document, and approve exceptions from the baseline configuration settings for individual systems based on explicit operational requirements; and certify that system complies with baseline security configurations.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

6 Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**System Admin** **Network Admin**	**IT Department**

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

7 Approval

____ ____________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Computer Configuration Baseline Standard

1 Overview/Purpose

<Utility Name> uses servers and workstations to support data processes in fulfilling its mission. Servers and workstations that are not configured properly are vulnerable to hacking, and various forms of malware, including rootkits and botnets. This standard define baselines for new servers and workstation configuration.

2 Scope

This standard apply to:

- Servers and workstations configured by IT Department.
- Servers and workstations configured by vendors contracted by **<Utility Name>**.

3 Standard

The IT Department shall use benchmarks published by the Center for Internet Security as a baseline for new computers configuration. These benchmarks are available at Center for Internet Security https://benchmarks.cisecurity.org/downloads/multiform/.
Benchmarks currently in use by the Utility shall be documented using the *Computer Configuration Benchmarks* Form. If benchmarks are not available for new system, the IT Manager is responsible for creating temporarily benchmarks.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

- Center for Internet Security
  Secure Configuration Benchmarks
  (https://benchmarks.cisecurity.org/)

6 Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**IT Administrator**	**IT Department**

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

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

System Patching Policy

1 Overview/Purpose

<Utility Name> is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. **<Utility Name>** has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the systems or data stored on the systems. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

This document describes **<Utility Name>**'s requirements for maintaining up-to-date operating system security patches on all owned and managed workstations and servers.

2 Scope

This policy applies to the following equipment, systems, and applications owned or used by **<Utility Name>**:

- Computers - servers and workstations (including laptops)
- Mobile devices – smartphones, tablets
- Network equipment – firewalls, routers, switches, network protocol converters
- Software applications

3 Policy

Computers, mobile devices, network equipment, and software applications owned or used by **<Utility Name>** must have up-to-date (as defined by <**person or group responsible for policy at Utility**> minimum baseline standards) system patches installed to protect the asset from known vulnerabilities. This includes updating applications, operating systems and firmware as required**.** Patching priority is adjusted according to severity level of the vulnerability which the patch addresses.

3.1 Patching Priority

Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System (CVSS). *See more information about CVSS in the Glossary section.*

A CVSS score of 7-10 is considered a Priority 1 vulnerability, a CVSS score of 4-6.9 is considered a Priority 2 vulnerability and a CVSS of 0.1-3.9 is considered a Priority 3.

Priority	CVSS Score	Patching Completion
1	7 - 10	Max 2 weeks
2	4 – 6.9	Max 4 weeks
3	0.1 – 3.9	Next patching cycle (3-6 months)
4	0	Discretionary

IT Manager can assign Priority 1 to a vulnerability if the vendor has issued an emergency patch (CVSS might be not published yet) or other information indicate high probability of exploitation.

3.2 Workstations

Desktops, laptops, and tablets must have automatic updates enabled for operating system patches, where available. This will be the default configuration for all workstations built by **<Utility Name>**. As possible, all software applications installed on workstations will be set to download and install patches automatically. Any exception to the policy must be documented and forwarded to the <**person or group responsible for policy** > for review. See Section 4.2 on Exceptions.

3.3 Servers

Servers must comply with the minimum baseline requirements that have been approved by the <**person or group responsible for policy** >. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the **<Utility Name>** server and the data that resides on it. Any exception to the policy must be documented and forwarded to the <**person or group responsible for policy** > for review.

3.4 Roles and responsibilities

IT Manager shall use the *Systems Patching Form* to assign responsibility for patching:

- Unix/Linux servers on the network,
- Microsoft Windows servers on the network,
- Workstations on the network,
- Applications.

IT Manager is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.

The System Patching Form is also used for:

- Approving emergency patches (no CVSS score),

- Reporting applied patches
  (if reports are not collected by log management system).

3.5 Monitoring and reporting

Active patching teams noted in Section 3.3 are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Information Security and Internal Audit personnel upon request.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

- FIRST - Forum of Incident Response and Security Teams
  Example of CVSS based Patching Policy
  (https://www.first.org/cvss/cvss-based-patch-policy.pdf)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**IT Administrator**	**All Employees**

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

7 Approval

_______________________________________ _______________________

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

Backup and Recovery Policy

1 Overview/Purpose

<Utility Name> is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly, and protecting the Utility's data from alteration or destruction due to equipment failure and other causes. **<Utility Name>**'s intentions for publishing a Backup and Recovery Policy are not to impose restrictions that are contrary to **<Utility Name>**'s established culture of openness, trust and integrity.

The purpose of the Backup Policy is to establish rules and outline the use of media systems and network servers for the storage, backup and recovery of electronic information in **<Utility Name>**'s Information Technology environment. Electronic backups are a business requirement to enable recovery of data and applications in the case of events such as natural disasters, system drive failures, espionage, data entry errors, or systems operations errors.

2 Scope

<Person or group responsible for policy at Utility> personnel, in coordination with respective departments, are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. These backup provisions will allow **<Utility Name>** business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of data backups should be maintained.

Federal and state regulations pertaining to the long-term retention of data (e.g., financial records) will be met using separate archive policies and procedures, determined by the Department responsible for the information. Backups are not primarily intended to archive data for future reference, but rather for system restoration. Data stored locally on desktop computers is not backed up, nor is data backed on systems that are not managed by **<person or group responsible for policy at Utility>**. Long-term archive requirements are beyond the scope of this policy.

3 Policy

<Utility Name> requires that computer systems be backed up on a regular basis, with backup media being stored in a secure off-site location. The purpose of the these backups is to provide a means to restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, to provide a measure of protection against human error or the inadvertent deletion of important files, and to secure data against possible deletion or alteration as part of a security incident. System backups are not intended to serve as an archival copy or to meet records retention requirements.

- Data stored on backup media shall be encrypted accordingly to the *Encryption Policy*.
- The frequency and extent of backups must be appropriate to the importance of the information and the acceptable risk as determined by the **<Utility Name>** department for each data set.
- **<Utility Name>** Information Technology backup and recovery processes for each system and service should be reviewed annually by the responsible business owner and the **<person or group responsible for policy >** personnel.
- Backup recovery procedures should be periodically tested to ensure that data is recoverable, and that restored data is identical to what was originally saved.
- Procedures for the offsite backup storage should be reviewed periodically.
- Backup media must be readily identified by appropriate labeling, with notes in a centralized log as to physical storage location for each media element.
- All critical or unique utility information stored locally on workstations must be placed on networked file server drives for backup.

3.1 Network storage structure

<Utility Name> has network servers in place in **<Identified Locations>.** Management and staff have file storage folders allocated for their account on network servers. These storage areas are usually referred to as the user's "X: drive", where X denotes a mapped storage area on a network server as described below:

X: Drive - User's personal folder on the network server

When the user successfully logs onto their workstation, network connections are established to these folders which can then be accessed as the "X: Drive" in Windows Explorer, Microsoft Word, Excel, and other software programs. Files can be copied from the user's workstation to their "X Drive", or software programs may be configured to save files directly to these mapped drives. These mapped drives are backed up to removable media. The removable media shall be rotated to an off-site storage facility and securely stored to provide for security and disaster recovery.

[Explanatory Note: This specific application of a network storage structure from utility to utility will vary. This information is provided only as a guide.]

3.2 Storage of user data files

In order to be able to recover lost data, management and staff should store essential data files requiring backup, to one of the network mapped drives. Data files on the user's local workstation may not be recoverable if the drive fails. Appropriate use of network storage will ensure ample capacity for archival storage of user data files. Users should store and maintain data files (or current copies) which are important to the company and which would be costly or impossible to recreate, on the network mapped drives. Users should not store non-business or non-essential data files on the network drives. Types of data files to be stored and their locations will be determined on a departmental level, and should be documented in a department level data backup guideline to be communicated with the **<person or group responsible for policy >**.

3.3 Backup Schedule

Systems backups will consist of regular full and incremental backups in accordance with the **<Utility Name>** *Backup Procedure*.

3.4 Documentation

<Utility Name> IT backup and recovery processes for each system and service must be documented by the **<person or group responsible for policy >** with assistance from the department for the related system or data set.

- Backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.
- Documentation of the restoration process must include procedures for the recovery from single-system or application failures as well as a total data center disaster scenario.
- Backup and recovery documentation will be reviewed and updated at least annually to account for new technology, business changes, and migration of applications to alternative platforms. Recovery procedures will be tested on an annual basis, where feasible.

3.5 Backup verification

Test restores from backup archives must be performed at least annually, where feasible. This ensures that both the archive media and backup/restore procedures work properly. It must be proven at least once that complete data restoration is possible. This testing ensures that:

- Data restoration is possible;
- The data backup procedure is practical;
- There is sufficient documentation of the data backup/restore process to allow a person unfamiliar with the procedure to carry out a data restoration, if necessary;
- The time required for the data restoration meets the availability requirements.

3.6 Offsite Storage

In order to provide disaster recovery capabilities, backup media are rotated to an offsite storage location from the backup source. Backup media are maintained in offsite storage according to the schedule outlined in *Backup Schedule Form*.

3.7 File Recovery

In order to have a file restored from a backup, the user should contact **<person or group responsible for policy>,** and provide complete details, including the date of the last known good version of the file – this will help identify the set of backup media to use in attempting to restore the file.

Files can usually be restored within a few hours or less, depending on the time required to obtain media from the offsite storage location. The **<person or group responsible for policy>** cannot restore data files which were not archived on the network servers. Given that backup media is reused, users should request restoration of data files as soon as possible to prevent data being overwritten on the backup media.

3.8 Open Data Files

The creation of accurate backups is not always possible if the files being backed up are open at the time of the backup. As such, users should ensure that all files are closed at the end of their business day. For applications running beyond normal business hours, arrangements should be made with the **<person or group responsible for policy >** to use an alternate approach to obtain backups.

3.9 Backup Failure

All backup failures will be logged and investigated as soon as practical upon detection.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

6 Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**System Admin** **Network Admin**	**IT Department**

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

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

Vulnerability Management Policy

1 Overview/Purpose

Vulnerability management is an essential component of any information security program. The process of vulnerability assessment is vital to effective vulnerability management.

2 Scope

Vulnerability assessment consists of scanning to identify networked assets, determining potential vulnerabilities, and assessment of potential vulnerabilities. Remediation of the vulnerabilities is another facet of vulnerability management.

3 Policy

3.1 Vulnerability Reports

All identified vulnerabilities will be assigned a risk ranking from Low to High based on industry best practices such as the CVSS base score. The results of vulnerability reviews will be documented on the vulnerability report. Mitigation actions are prioritize based on vulnerability ranking.

3.2 Vulnerability Scans Frequency

As part of the PCI DSS Compliance requirements, **<Utility Name>** will run internal and external network vulnerability scans at least quarterly, and after any significant change to networks and systems (new application installation, new firewall or router installation, network equipment replacement, new server or workstation installation).

Quarterly internal vulnerability scans must be performed by the **<Utility Name>** IT department or a 3rd party vendor. The scan process must include rescans, to be repeated until passing results obtained, or all High vulnerabilities as defined in PCI DSS Requirements 6.2 are resolved.

Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by the PCI Security Standards Council (SSC). Scans conducted after network changes may be performed by **<Utility Name>** IT department. The scan process should include re-scans until passing results are obtained.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

- Adopted from https://www.sans.edu/student-files/projects/vulnerability-assessment-policy.pdf
- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**IT Department**	**All Employees**

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

7 Approval

____________________________________ __________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Remote Access Policy

1 Overview/Purpose

The purpose of this policy is to define standards for connecting to **<Utility Name>**'s network from external networks.

2 Scope

This policy applies to all employees, contractors, vendors and agents with a **<Utility Name>**-owned or personally-owned computers or mobile devices used to connect to the **<Utility Name>** network. This policy applies to remote access connections used to do work on behalf of **<Utility Name>**, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to VPN, and VPN over SSH.

3 Policy

It is the responsibility of employees, contractors, vendors and agents with remote access privileges to the company's network to ensure that their remote access connection meets all requirements outlined in this policy.

Remote access by individuals without specific company authorization is prohibited. The employee associated with a remote access account bears responsibility for any misuse.

Please review the following policies for details of protecting information when accessing the network via remote access methods, and acceptable use of **<Utility Name>**'s network:

- Encryption Policy
- Network Configuration Standard
- Acceptable Use Policy

3.1 Requirements

3.1.1 Secure remote access must be strictly controlled with use of Multi Factor Authentication or certificates deployed by a MDM (Mobile Devices

Management) system.

3.1.2 At no time should any employee provide their remote access credentials to anyone, including family members.

3.1.3 All systems that are connected to internal networks via remote access technologies must use the most up-to-date version available of an anti-virus software package approved by the IT Manager.

3.1.4 Authorized employees may also access the internal network from mobile devices. In this case, Multi Factor Authentication is required, and the mobile device must have the MDM application deployed.

3.1.5 Third party connections must comply with requirements as stated in the *Third Party Access* Policy.

3.1.6 Organizations or individuals who wish to implement non-standard Remote Access solutions to the production network must obtain prior approval from <**person or group responsible for policy**>.

3.1.7 Wireless access within the <**Utility Name**> facilities shall be treated as remote access.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from “Remote Access Policy” (http://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy)
- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
CIO	**CEO/GM**		**All Employees**

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

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

System Logging and Monitoring Policy

1 Overview/Purpose

Monitoring and logging is an essential information security control that is used to identify, respond to, and prevent operational problems, security incidents, policy violations, and fraudulent activity.

The purpose of this policy is to establish requirements and parameters for creating, maintaining, storing, and accessing **<Utility Name>** computer and communication device logs. The logs shall be used to assist in troubleshooting, monitoring changes to system performance, recording the actions of users when necessary to properly maintain security, track and investigate security incidents, and provide data useful for investigating malicious activity. Additionally, logs may be used to assist in business recovery activities, and to comply with federal, state, and local laws and regulations.

2 Scope

All employees, contractors, consultants, temporary and other workers and its subsidiaries must adhere to this policy. This policy applies to technology, as defined in the Introduction herein, that is owned, operated, or leased by **<Utility Name>** or registered under a **<Utility Name>**-owned internal network domain.

3 Policy

3.1 General Requirements

3.1.1. The time settings of all systems generating log files will be synchronized to an authoritative time source, using an application such as the Network Time Protocol (NTP) Service. Synchronizing time stamps for log events will help to facilitate the investigation of issues involving more than one system.

3.1.2. **<Utility Name>** will use a centralized system for log collection and correlation. All network devices, servers, workstations shall provide log data to the centralized logging system. This system should also collect data from wireless access points and intrusion detection devices.

The level of information detail contained in a log will be determined by the IT Manager based on the risks to the relevant technology and underlying data, and shall be determined in accordance with the risk management policy.

3.1.3. Log files must be examined on a regular basis in order to protect technology. The frequency and nature of log monitoring and review depends on the risks to the relevant technology and underlying data and shall be commensurate with the risk management policy. To satisfy PCI DSS requirements, logs will be review on daily basis when collecting data from protective devices and applications such as IDS, IPS (standalone or built into firewall), and antivirus consoles.

3.1.4. The following list of events shall be logged for PCI DSS compliance:

- Directory Service Access Attempts
- Directory Service Access - Success/Failure
- Logon Failures – Active Directory
- Logon Failures – Local Logons
- Object Access Attempts – Success/Failure
- Object Deletions
- Password Reset Attempts by Administrators or Account Operators
- Process (Program) Usage
- User Activity in Auditing Categories
- Successful Network Logons – Workstations and Servers
- Policy Change - Success/Failure
- Account Management – Success/Failure
- Directory Service Access - Success/Failure
- System Events - Success/Failure

(This list of logged information needs to be verified periodically against the current PCI DSS standard.)

3.1.5. Log files may contain confidential data, and thus must be handled in a manner that is consistent with the **<Utility Name>**’s policy for such data. Logging facilities and log information should be protected against tampering, modification, destruction, and unauthorized access. When technically feasible, system administrators should not have permission to erase, deactivate, or modify logs of their own activities.

3.1.6. Log files will be maintained only as necessary to comply with the record retention policy or as required to support analysis of misuse, incident reconstruction, or other investigations. To satisfy PCI DSS requirements, logs need to be maintained for one year, with logs for three years readily available.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- See also, "Maintenance, Monitoring, and Analysis of Audit Logs" (http://www.sans.org/critical-security-controls/control/14) and "Account Monitoring and Control" (http://www.sans.org/critical-security-controls/control/16)

- PCI DSS Requirements
  https://www.pcisecuritystandards.org/document_library

6 Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**System Admin** **Network Admin**	**IT Department**

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

7 Approval

<Insert title of approver>

Date

8 Revision History

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

Insert
Utility
logo
here

Data Encryption Policy

1 Overview/Purpose

This policy sets guidelines for the use of encryption to ensure that **<Utility Name>** can leverage cryptographic software and techniques to safeguard our member data and our operations, while mitigating the attendant risks.

2 Scope

This policy shall apply to all uses of encryption within **<Utility Name>**.

3 Policy

It is the responsibility of employees, contractors, vendors and agents with access to the network to ensure that confidential data is encrypted at rest and in transit, whenever practical. Confidential data shall be encrypted at rest, and when it leaves the utility's premises. This includes:

- Databases with PII data or other confidential information accordingly to data classification,
- Laptops and other mobile devices,
- Portable data storage devices,
- Off-site backups.

3.1 Transport layer security

The use of Transport Layer Security is strongly encouraged for all employee and contractor web browsing and for use on web servers. All non-console administration access to cardholder data will require the use of strong transmission encryption. Such data should never be transmitted via end-user messaging technologies, including email and text messages.

<Utility Name> web servers should be configured to use most recent TLS, but no earlier than TLS 1.2.

3.2 Database and shared storage device encryption

Databases and shared storage devices such as server, SAN, or NAS disks, shall utilize data encryption either made available by the database vendor, or by using third party solutions. The encryption methodology implemented should meet or exceed the requirements in NIST 800-111, Guide to Storage Encryption Technologies for End User Devices.

3.3 Full disk encryption

Every workstation, laptop and mobile device should have full disk encryption enabled and configured, according to best practices for that platform.

Suspend-to-ram (S3 or “sleep”) shall be disabled for platforms which hold encryption keys in memory while suspended. This includes Windows, Linux and Android operating systems, and excludes Apple OS X and iOS devices as well as Google Chromebooks.

3.4 Procuring secure encryption software

All encryption software used must be approved for use by **<person or department responsible for this policy>**.

Encryption software must be actively supported and audited for security to be eligible for approval. The **<person or department responsible for this policy>** is responsible for determining whether a piece of cryptographic software meets these criteria, and for maintaining a list of approved encryption software.

3.5 Key Management

All secret key material (keys, passphrases, etc.) used by employees and contractors must be stored securely and redundantly. Employees and contractors must submit secret key information to the IT Manager or their designee, for storage in an offline key repository.

Keys shall be stored offline, in a secure location, such as a safe. The offline key repository must not be accessible from a network-connected computer. Access to the repository must be limited to the minimum personnel necessary.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- NIST 800-111, Guide to Storage Encryption Technologies for End User Devices (http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**		**All Employees**

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

7 Approval

______________________________ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Network Configuration Standard

1 Overview/Purpose

Network equipment plays an important role in protecting the network and data assets.

2 Scope

This standard is intended to define rules for network equipment configuration, configuration modification, and documenting changes.
{This document requires modification to include specific network equipment used by utility such as private radio or fiber network}

3 Standard

3.1 Network Documentation

<Utility Name> maintains a current network diagram which identifies all physical connections. The network diagram will be kept updated by the network administrator to reflect changes in the network, with a date indicating when the most recent update was made.

3.2 Firewalls and routers

- Firewalls must be implemented between each internet connection and any demilitarized zone (DMZ), and the internal company network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols, and ports allowed, including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the cardholder data environment (CDE).
- Stateful firewall technology must be implemented where the Internet enters the CDE to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments.
- All inbound and outbound traffic must be restricted to that which is required for the CDE.

- All inbound network traffic should be blocked by default, unless explicitly allowed. Any rules set to allow inbound traffic must be documented, including the appropriate justification.
- All outbound traffic has to be authorized by management. Any rules to allow outbound traffic must be documented.
- **<Utility Name>** will deploy firewalls between any wireless networks and the CDE.
- **<Utility Name>** will quarantine wireless users into a DMZ, where they will be authenticated and firewalled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment must be documented, and must be updated in accordance to the changes in the network.
- The firewall rules will be reviewed every 6 months to ensure that they are consistent with the rules previously approved.
- No direct connections from Internet to CDE are permitted.
  All traffic must traverse through a firewall.
- Firewall configuration changes are conducted according to *Firewall Configuration Procedure* and documented in *Firewall Configuration Change Form*.
- The *Firewall Rules Design Form* is used for:
  - Initial design of firewall rules
  - Documenting business requirements for allowing specific traffic

3.3 Wireless devices

3.3.1 Office Wireless Device Requirements

All office wireless infrastructure devices must adhere to the following:

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the networks or environments is prohibited, except as specifically authorized by IT Department.
- Stateful packet inspection firewalls are to be used to block wireless traffic from entering the networks. Firewall connected to wireless network are must use IDS/IPS.
- VLANs are not used for segmentation with MAC address filters for segmenting wireless networks.
- A wireless analyzer (or a wireless IDS/IPS) should be used at least every 6 months to detect unauthorized/rogue wireless devices that could be connected to the network at all locations.
- Automatic alerts and containment mechanisms are to be used on the wireless IPS to eliminate rogue and unauthorized wireless connections into the network.
- If any violation of this standard is discovered as a result of the normal audit processes, the IT Manager has the authorization to remove the offending device immediately.
- If the need arises to use wireless technology, it should be approved through the *IT Change Request Procedure,* with the following wireless standards to be applied:

1. Default SNMP community strings and passwords, passphrases, encryption keys, and other security-related vendor defaults (if applicable) should be changed immediately after the installation of the device. Any such settings should be changed when a person with knowledge of them leaves the company
2. The firmware on each wireless devices must be updated promptly following release by the vendor.
3. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
4. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of cardholder data.

3.3.2 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must use the following settings:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS;
- When enabling WPA-PSK, a complex shared secret key (at least 20 characters) must be used on the wireless client and the wireless access point;
- Disable broadcast of SSID;
- Change the default SSID name;
- Change the default login and password.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-compliance

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

5 Related Standards, Policies, and Processes

- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)
    - (Requirement 1.1.2)
    - (Requirement 1.1.4)

- o (Requirement 1.1.6)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
CIO	**CEO/GM**	**IT Department**	

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

7 Approval

______________________________ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

Change Management Policy

1 Overview/Purpose

Change Management is a formal, systematic process for dealing with change, both from the perspective of the organization, and on an individual level. The intent of Change Management is to ensure that any hardware/software changes implemented are properly planned, tested, and implemented, so as to minimize any resulting disruption. It is the policy of **<Utility Name>** to follow a formal, documented process for implementing significant changes to systems, network, and applications, as documented in the *IT Change Request* Procedure.

2 Scope

This policy applies to employees, contractors, and other individuals requesting changes to systems, networks, or applications. IT Manager and IT staff are responsible for following this Policy and related procedures.

3 Policy

3.1 Process

The Change Management process shall:

- Ensure that significant requests for changes to systems, networks, and applications are formally documented and submitted is accordance with the *IT Change Request Procedure*;
- Require that the IT Manager, and his/her designees, process change requests using the following steps:
  - Submission - only accepting change requests using a formal, documented process, excluding verbal or ad-hoc requests;
  - Impact Evaluation - careful consideration of the potential impact of the requested change to **<Utility Name>**'s operations.
  - Design and Planning - for an approved request, the preparation of an Implementation plan that is sufficiently detailed to ensure that the change is completed according to determinations made during the Impact Evaluation;
  - Implementation - carrying out the change in strict accordance with the details determined in the Design and Planning phase;
  - Results Evaluation - the careful review of the changed system, and all inter-related systems, following the Implementation to ensure that: a) the desired change was

implemented successfully; b) there were no unanticipated impacts to other systems as a result of Implementation.

3.2 Scope

The Change Management process includes, but it not limited to, the following requests:

- New hardware such as computer, mobile devices, printers, etc.;
- New software – server, desktop applications, and mobile applications might be included as well if the change requires server installation;
- Change in application or network permissions system;
- Change in the configuration or functionality of the network, including Internet connections, firewall functionality, etc. Note that for firewall, router, and switch modifications, the change should be requested using the Firewall Configuration Change Form;
- Changes to existing processes used by IT Department (policy, procedures, forms).

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
CIO	**CEO/GM**	**IT Department**	**All Employees**

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

7 Approval

____ ____________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

IT Change Request Procedure

1 Overview/Purpose

Change Management is the formal, systematic process followed by **<Utility Name>** for dealing with change, both from the perspective of the organization, and on an individual level. The intent of Change Management is to ensure that any hardware/software changes implemented by the **<Utility Name>** are properly planned, tested, and implemented, so as to minimize any resulting disruption to the company's operations.

This procedure defines the changes that are in and out of scope to the Change Management process, and how the changes within scope are requested, evaluated for risks, tested, and implemented.

2 Scope

This procedure governs, but is not limited to, changes made to hardware, software and procedures in production.

The following are examples of IT requests are not scope of Change Management Process:

- Password change;
- Unlocking account;
- Repair of computer or other equipment delivered and maintained by IT;
- Other routine IT activities provided on regular basis.

The following IT requests are in the scope of Change Management process:

- New hardware such as computer, mobile devices, printers, etc.;
- New software – server, desktop applications, and mobile applications might be included as well if the change requires server installation;
- Change in application or network permissions;
- Change in the configuration or functionality of the network, including Internet connections, firewall functionality, etc. Note that for firewall, router, and switch modifications, the change should be requested using the *Firewall Configuration Change Form;*
- Changes to existing processes used by IT Department (policy, procedures, forms.)

3 Procedure

The Change Request procedure uses the *IT Change Request Form*, included in this library. Any firewall, router, and switch changes should be requested using the *Firewall Configuration Change Form*, but such changes will otherwise follow this process. Each step of change request process shall be documented on this form.

Submitted Change Requests may have one of the following statuses:

- Open – Change Request received but has not been assigned for evaluation
- In Progress – Scope and risk assessment is in progress
- Approved – The assessments have been completed, preparing for implementation
- Deferred – Out of IT budget or high risk, needs to be reviewed by Steering Committee
- Rejected – The change has been rejected
- Implementation – Change Request is being implemented
- Closed – Implementation completed, the change request has been closed
- Canceled – The change request has been canceled

The Change Request process include the following phases:

- Submission
- Impact Evaluation
- Design and Planning
- Implementation
- Results Evaluation

3.1 Submission

Change Requests can be submitted by supervisors or managers, and shall include the following information:

- Reason for changing configuration
  (What business processes requires this change?)
- Implementation timeline
  (When does this change needs to be completed?)
- Priority
  - **Emergency** – A change that must be introduced as soon as possible to resolve major incident or implement a security patch (Priority 1 and CVSS 10),
  - **Urgent** – A change to apply a security patch (Priority 1 – CVSS 8-9) or implement important change for Utility services.
  - **Routine** – A change requested to modify/improve service but is not time sensitive

3.2 Impact Evaluation

After receiving Change Request, the IT Manager will evaluate:

- Impact including cost, resources, time requirements
- Risk associated with change

A submitted Change Request has OPEN status until impact evaluation is completed.

3.3 Design and Planning

Approved Change Requests require preparation for implementation, including:

- Design,
- Purchasing new hardware or software,
- Scheduling implementation,
- Preparing evaluation criteria.

3.4 Implementation

Once the design and planning aspects of a change have been considered and documented, the change can be implemented. When planning for the final implementation, the following factors need to be considered:

- Will the change impact active operations; is implementation during off-hours required?
- Will the change has a direct impact on the workforce, and if so, do they need to be notified, trained, etc.?
- In the event of an unexpected issue resulting from the change, what process will be followed to reverse the change?

After implementing new configuration, all related documentation needs to be updated.

3.5 Results Evaluation

Once change implementation has been completed, appropriate testing is required to ensure that the change is working as desired, and that no unexpected impact to **<Utility Name>** operations has occurred. Primary testing of the change itself should be referred to the requestor. The IT Manager will evaluate any inter-related systems to ensure that no unexpected impact has occurred.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 Related Standards, Policies, and Processes

- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**IT Department**	

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

7 Approval

_______________________________________ _______________________

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

Firewall Configuration Change Form

{The Firewall Configuration Change Form is provide as a template for documenting process of changing firewall configuration. This type of change documentation can implemented by using Sharepoint or other tools as well. This form can be used for documenting configuration changes for other equipment such as routers, phone switches, communication appliances, etc., as appropriate.}

1 Change Request

Item	Description
Request #	
Date	
Priority **(Emergency, Urgent, Routine, Low)**	
Requesting Employee	
Change Reason	
Change Description	
Change Request Status (date)	

Status:

- Open – CR received but has not been assigned
- In-Progress – Scope and risk assessment is in progress.
- Approved – The assessments have been completed, preparing for implementation.
- Rejected – The change has been rejected.
- Closed – Implementation completed; the change request has been closed.
- Canceled – The change request has been canceled.

2 Risk Assessment & Approval

Item	Description
Date	
IT Manager	
Risk Assessment	
Tests Requirements	
Comments	

3 New Configuration Tests

Item	Description
Date	
Tested by	
Test Scope	
Tests Results	
Comments	

4 Implementation

Item	Description
Date	
Implemented by	
Final Configuration	
Documents Updated	
Comments	

5 Form Revision History

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

Insert
Utility
logo
here

IT Change Request Form

{The IT Change Request Form is provided as an example for documenting change request process. This documentation can implemented by using Sharepoint or other tools.}

1 IT Change Request

Item	Description
Request #	
Date	
Priority **(Emergency, Urgent, Routine, Low)**	
Requesting Employee	
Change Reason	*New deployment of hardware or software* *New functionality of existing hardware or software* *Security hardware or software fixes* *Upgrade - hardware or software upgrades* *Other – None of above.*
Change Description	
Change Request Status (date)	

Status:

- Open – CR received but has not been assigned for evaluation
- In-Progress – Scope and risk assessment is in progress.
- Approved – The assessments have been completed, preparing for implementation.
- Deferred – Out of IT budget or high risk, needs to be reviewed by Steering Committee
- Rejected – The change has been rejected.
- Implementation – Change Request is being implemented
- Closed – Implementation completed, the change request has been closed.
- Canceled – The change request has been canceled.

2 Impact Evaluation

Item	Description
Date	
IT Manager	
Risk Assessment	
Cost Assessment	
Purchase Requirements	
Tests Requirements	
Comments	

3 Design and Planning

Item	Description
Date	
Designed by	
Design Description	
Implementation Plan	
Testing Plan	
Comments	

4 Implementation

Item	Description
Date	
Implemented by	
Final Configuration	
Documents Updated	
Comments	

5 Results Evaluation

Item	Description
Date	
Evaluated by	
Evaluation Methods	
Evaluation Results	
Comments	

6 Form Revision History

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

Insert Utility logo here

IT Employee Change Form

1 Employee information

First, Last Name	Employee ID	Old Org. Role	New Org. Role

2 Change Reason

New Employee: ☐ Position change: ☐ Employee Termination: ☐

3 IT Equipment

3.1 Desktop Computer

Add: □ Remove: □ Replace: □

Request details (specify computer requirements):

IT Comments:

3.2 Laptop Computer

Add: □ Remove: □ Replace: □

Request details (specify computer requirements):

IT Comments:

3.3 Mobile Devices (cellphone, tablet, etc.)

Add: □ Remove: □ Replace: □

Request details (specify computer requirements):

IT Comments:

3.4 Multifactor Authentication Token

Add: □ Remove: □ Replace: □

Request details (specify computer requirements):

IT Comments:

4 Permissions Change

IT Comments:

System	Account(*) (date)	Role Assigned (date)	Modified by (IT Admin)
UPN			
OMS			
SCADA			
GIS			

Account: Create, Suspend, Remove

5 Other Request

Request details:

IT Comments:

6 Manager Approval

Manager Name and signature Date

7 IT Approval

IT Manager Name and signature Date

Comments:

8 Completion Report

Comments:

9 Revision History

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

Insert Utility logo here

Third Party Access Policy

1 Overview/Purpose

This policy covers outside entities or individuals, such as software providers, hardware technical support personnel, or any other outside personnel, known as Third Parties, who have a need to access **<Utility Name>**-owned IT systems or applications in order to provide a service to the utility.

The purpose of this policy is to define standards for connecting to networks from any host. These standards are designed to minimize the potential exposure to the company from damages which may result from unauthorized use of resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

2 Scope

This policy applies to all Third Parties with a **<Utility Name>** owned or personally owned computer or workstation used to connect to the network. This policy applies to remote access connections used to do work on behalf of **<Utility Name>**, including reading or sending email and viewing intranet web resources, or any other activity involving the utility's systems or applications. Remote access implementations that are covered by this policy include, but are not limited to VPN, VPN over SSH, or other means.

3 Policy

3.1 General Requirements

It is the responsibility of Third Parties with remote access privileges to the network to ensure that their remote access connection meets all security policies and requirements. General access to the Internet via the network for recreational use, or unrelated outside business interests, is not permitted. The Third Parties, and the individuals which they employ, are responsible for the consequences should the access be misused. Please review the following policies for details of protecting information when accessing the network via remote access methods, and acceptable use of the network:

- *Encryption* Policy
- *Remote Access* Policy

- *Acceptable Use* Policy

3.2 Requirements

3.2.1. Third party connections must comply with requirements as stated in the Third Party Agreement, to be signed by any Third Party accessing **<Utility Name>** Systems or Applications.
[***NOTE:*** *Not included as part of this package.]*

3.2.2. The IT manager should use the Third Party Access Procedure for granting Third Party access to the network.

3.2.3. Connectivity details, restriction and access termination is documented in the Third Party Access Form.

3.2.4. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with a strong passphrases.

3.2.5. At no time should any employee provide their User Account or email password to anyone, including family members.

3.2.6. Third Parties with remote access privileges to the network must not use non-**<Utility Name>** email accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct company business, thereby ensuring that official business is never confused with personal business.

3.2.7. Reconfiguration of equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

3.2.8. Personal equipment that is used to connect to networks must meet the same requirements as utility-owned equipment for remote access.

3.2.9. Organizations or individuals who wish to implement non-standard Remote Access solutions to the production network must obtain prior approval from <**person or group responsible for policy**>.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from SANS "Remote Access Policy" template(https://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy)

6 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.]

7 Approval

_____________________________________ _____________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Outsourced Information Processing Policy

1 Overview/Purpose

In order to fully leverage the advantages of the most up-to-date technology available, **<Utility Name>** may contract with outside sources to provide that technological advantage as opposed to developing solutions internally. This approach provides many advantages to include cost savings, faster implementation, and expertise often not available internally. While providing the aforementioned advantages, **<Utility Name>** must also be cognizant of the inherent risk involved in allowing third-party providers access to our internal systems and take the necessary precautions to safeguard confidential information.

This policy sets out principles and expectations pertaining to the security of IT resources that are accessed, or provided, by third parties.

2 Scope

This policy applies to all contractors, vendors and agents who may have a legitimate business-related need to connect to the network. This may include hardware/software support and maintenance staff, consultants; IT and/or business process outsourcing firms, or temporary staff hired for a specific project. This policy applies to remote access connections as well as on-site access used to do work on behalf of **<Utility Name>**, including reading or sending Email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to, DSL, VPN, SSH, and/or remote web sessions.

3 Policy

3.1 Assessing Outsourcing Risks

Management shall nominate a suitable < owner for each business function/process outsourced. The owner, with help from the **<person or group responsible for policy>,** shall assess the risks before the function/process is outsourced, using standard risk assessment processes.

3.2 Contracts

3.2.1. A formal contract between **<Utility Name>** and the outsourcer should exist.

3.2.2. All contracts shall be submitted to **<person or group responsible for policy>** for accurate content, language and presentation.

3.3 Hiring and training of employees

3.3.1. Outsourced employees, contractors and consultants working on behalf of **<Utility Name>** may be subjected to background checks equivalent to those performed on employees.

3.3.2. Companies providing contractors/consultants directly to **company** to outsourcers shall perform at least the same standard of background checks as those indicated above.

3.3.3. Suitable information security awareness, training and education shall be provided to all employees and third parties working on the contract, clarifying their responsibilities relating to information security policies, standards, procedures and guidelines (e.g. privacy policy, acceptable use policy, procedure for reporting information security incidents etc.) and all relevant obligations defined in the contract.

3.4 Security audits

3.4.1. If applicable, the outsourcer will provide SOC 1 and SOC 2 Reports, or agree to **<Utility Name>**'s right to audit.

3.4.2. The frequency of audit shall be determined by **<person or group responsible for policy>.**

4 Compliance

4.1 Compliance Measurement

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

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from ISO 27001 Security – "Information Security Policy on Outsourcing" (www.iso27001security.com/ISO27k_Model_policy_on_outsourcing.docx)

6 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.]

7 Approval

______________________________________ ____________________

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

Compliance Requirements Policy

1 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.

2 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.

3 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.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

6 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.]

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

Business Continuity and Disaster Recovery

1 Overview/ Purpose

Since disasters happen so rarely, many organizations fail to plan in advance their immediate response to a disaster, referred to as a Disaster Recovery Plan, or the resumption and continuation of their operations after a disaster, called Business Continuity Planning. It is important to realize that having a Disaster Recovery/Contingency Plan in the event of a disaster gives a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended disruption in or delay of service should be considered. The Disaster Recovery Plan should be part of the overall Business Continuity Plan.

This policy defines the requirement for a baseline Disaster Recovery Plan to be developed and implemented by <**Utility Name**> that will describe the process to recover IT systems, applications and data from any type of disaster that causes a disruption to business processes or access to critical data and IT services. Additionally, this policy defines a requirement for a Business Continuity plan, which provides guidance for the resumption of normal operations following a disaster.

2 Scope

This policy is directed to the **<person or group responsible for the policy>** who are accountable for ensuring that the Business Continuity/Disaster Recovery Plans are developed, tested and kept up-to-date. The purpose of this policy is solely to state the requirement to have Business Continuity/Disaster Recovery Plans; it does not define the specific contents of these plans, or the process for their development.

3 Policy

3.1 General Requirements

The following contingency plans, which comprise the overall Business Continuity/Disaster Recovery Plans, must be created to include, at a minimum:

3.1.1. Emergency Response Plan: The level of emergency, the process of recovery and how business continues during the emergency are defined.
3.1.2. Chain of Command: Define the order of responsibility when normal staff is unavailable to perform duties.
3.1.3. Data Study: Detail the data stored on the systems, criticality, and level of confidentiality. This should follow the *Data Classification* policy and the *Data Assets Inventory*.
3.1.4. Criticality of Service List: List all the services provided in their order of importance.
3.1.5. Explain the order of recovery in both short-term and long-term timeframes.
3.1.6. Data Backup and Restoration Plan: Detail what data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered. This should follow the *Backup and Recovery* policy.
3.1.7. Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
3.1.8. Mass Media Management: Define the accountability for corporate spokesperson and development of messages for communications to public and consumers.

3.2 Table Top Exercise Requirements

After creating the plans, it is important to practice them to the extent possible. Management, including key staff, should set aside time to test the Disaster Recovery and Business Continuity Plans. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences. The Plans are revised and updated to reflect outcomes of the table top exercises.

3.3 Review Schedule

At a minimum, the plans should be reviewed and updated on an annual basis.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.
- Adapted from “Disaster Recovery Plan Policy
  http://www.sans.org/security-resources/policies/general/pdf/disaster-recovery-plan-policy

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**CFO**	**All Employees**

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

7 Approval

______________________________________ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert
Utility
logo
here

Incident Management Policy

1 Overview/Purpose

Cyber incidents occur frequently. It is important to realize that having an incident response and management policy allows **<Utility Name>** to protect its information, as well as its reputation. This policy requires <**person or group responsible for policy**> to develop the appropriate procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy to allow the staff to successfully understand, manage, and recover from a cyber incident.

This policy defines the requirement for a baseline incident response and management plan to be developed and implemented that will describe the process to investigate a suspected incident, discover an attack and then effectively contain the damage, eradicating the attacker's presence, and restore the integrity of the network and system.

2 Scope

This policy is intended to state the requirement to have an incident response and management plan, along with the phases of incident management, and categories of incidents. It is not intended to specify what goes into the plan or sub-plans.

3 Policy

The Incident Response Plan shall:

- Ensure that there is a written incident response plan that includes a definition of personnel roles for handling incidents.
  The plan shall define the following phases of incident handling:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication and Recovery
  - Post Incident Analysis & Forensics
- Use incident prioritization by determining incident impact:
  - Functional impact – how systems were affected functionality
  - Information impact – what information was accessed
  - Recoverability – how quickly systems can be recovered
  - Define responsibilities during incident response
- Assign job titles and duties for handling computer and network incidents to specific individuals.

- Define management personnel who will support the incident handling process by acting in key decision-making roles.
- Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.
- Define standards and processes for notifying the appropriate legal and/or regulatory organizations.
- Provide instructions on how to report computer anomalies and incidents. Such information should be included in routine employee awareness training and activities.
- Conduct periodic incident handling drills.
- Review the Plan on a periodic basis.

4 Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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

5 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.

- Adapted from “Incident Response and Management” (http://www.sans.org/critical-security-controls/control/18)
- Adapted from NIST 800-61r2 – Computer Security Incident Handling Guide (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

6 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO/GM**	**COO** **CFO**	**All Employees**

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

7 Approval

____ ______________________

<Insert title of approver> Date

8 Revision History

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

Insert Utility logo here

Information Security Incident Response Plan

1 Overview/Purpose

The **<Utility Name>** incident response plan defines the preparation for the handling of incidents, and outlines the incident response phases.

2 Scope

Proper response to information security incidents requires:

- A designated team with assigned roles
- Internal and external communication lists
- Metrics for determining incident impact
- Testing and response maturing plan
- Defined phases of incident response

{Some utilities may create SIRT (Security Incident Response Team). The other option is to use ICS (Incident Command System) structure, which several Coops are already using. The advantage of this approach is that the same ICS can be used to handle different types of incidents}

3 Incident Preparation

3.1 Incident Response Team and Roles

Role	Description	Primary Person	Backup Person
Incident Manager	Analyze event information and estimate incident impact. Coordinate Team effort in all phases of response.	IT Manager	IT Administrator
Incident Response Team Member	Reports to Incident Manager	IT Administrator, GIS Technician,	IT Administrator, GIS Technician, E&O technician
CEO	Provide management support		
Legal Counsel	Provide legal support		
External Communication	Communicate with BOD, regulators, media	Public Relations or Marketing	
Logistics	Provide logistic support for longer incidents	Clerical or administrative employees	

3.2 Contact List and Tools

(Information Security Response Plan - Forms Examples)

3.2.1 Internal contact list

Internal contact list shows who should be notified internally in case of an incident.

3.2.2 External contact list

External contact list shows who should be notified externally in case of an incident.

3.2.3 Tools

Effective response to incident requires preparing OS images, spare hardware, etc.

3.3 Incident Response Improvements

On quarterly basis, the Incident Response Team should review response to one of the threats listed in risk register or one the scenarios included in document *Incident Examples*. The goal of this exercise is to review existing documentation and create more detailed procedures, if needed.

3.4 Table Top Exercises

On annual basis, **<Utility Name>** should conduct a Table Top Exercise (TTE) to review Emergency Restoration Plan and Information Security Incident Response Plan.

4 Incident Detection and Analysis

All **<Utility Name>** employee shall report suspicious activities related to information technology.

Incident indication may also come from local monitoring systems (SIEM, file integrity monitoring) or from external sources.

Reports should be submitted to the Incident Manager, who will use the *Information Security Incident Response Form,* and analyze the incident.

Incident analysis factors:

- Sensitivity classification of involved data: Public, Internal, Sensitive, Confidential or Regulated
- Availability classification of involved data: Supportive, Priority or Critical
- What systems are affected by the incident?
- How many computers are affected by the incident?
- What is potential damage caused by the incident?
- What is the estimated time to recover from the incident?

By using these factors, the Incident Manager can determine incident impact:

- Functional impact – how incident affected systems functionality
- Information impact – what information was accessed, modified, and/or deleted
- Recoverability – how quickly systems can be recovered

Since during incident some information technology systems might be not available, this procedure and form should also be kept on mobile devices and as paper copy as well.

{The impact level of incident can be aligned with RUS Emergency Restoration Plan which uses the following levels: Catastrophic, Critical, Marginal, Insignificant or Remote}

Functional Impact Categories

Category	Definition	Examples
None	No effect to the organization's ability to provide all services to all users	• Single computer affected by virus
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	• Two workstations affected by ransomware • Several laptops were affected by virus
Medium	Organization has lost the ability to provide a critical service to a subset of system users	• GIS server affected by exploit, maps not updated • AVL affected by DDoS, vehicle locations not updated
High	Organization is no longer able to provide some critical services to any users	• OMS and AMI affected by APT • Firewall firmware was changed affecting communication with the Internet

Information Impact Categories

Category	Definition	Examples
None	No information was exfiltrated, changed, deleted, or otherwise compromised	• Single computer affected by virus
Privacy Breach	Sensitive personally identifiable information (PII) of Members or employees was accessed or exfiltrated	• Employees (PII) data was extracted and found on dark web
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated	• Diagrams of fiber communication and substations was accessed from IP address in Iran
Integrity Loss	Sensitive or proprietary information was changed or deleted	• Documentation with distribution lines protection settings were changed

Recoverability Effort Categories

Category	Definition	Examples
Regular	Time to recovery is predictable with existing resources, and will meet RTO	• Affected workstations will be restored in 4 hours
Supplemented	Time to recovery is predictable with additional resources and, will exceed RTO	• Restoring systems affected by ransomware require systems and application images
Extended	Time to recovery is unpredictable; additional resources and outside help are needed	• Repeated DDoS require ISP support and changing DNS pointers • Software vendor assistance is require in restoring OMS
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation	• Member's PII information published by hackers

5 Containment, Eradication and Recovery

5.1 Containment

The goal of the containment phase is to regain control by limiting the extent of the damage:

- Consider isolating the compromised system(s)
- Analyze business impact of isolating the compromised system(s)
- Prepare for isolation
- Perform isolation and make system backup, if possible

5.2 Eradication

The goal of eradication phase is removing elements of the threat from the systems and networks:

- Consider reloading operating systems and applications
- Applying latest patches
- Disabling unnecessary services
- Consider activating additional monitoring features
- Validating completion of eradication phase

5.3 Recovery

The goal of recovery phase is to return all systems to original functionality:
{Some Coops may use Emergency Recovery Plan for recovering specific systems such as phone switch, Outage Management System, UPN, GIS, etc.}

- Consider restoring system(s) from latest pre-incident backup
- Estimate data loss and verify RPO
- Prepare plan for handling data loss (credit card transaction, outage information, AMI readings, emails)

6 Post Incident Analysis & Forensic

The objective of a post incident analysis is to perform a detailed investigation of the incident, to devise approaches for prevention of similar incidents in the future.

Consider using the following options:

	In-house	Law enforcement	Forensics Company
Cost	Least expensive	Expensive	Most expensive
Response Time	Quick	Might be not available, could cause slow response time	Quick response time
Skills of investigators	May not have the relevant skills	Dependent on the local law enforcement	Skilled staff
Preservation of evidence	Does not ensure evidence integrity	Preserve evidence integrity, acceptable in court	Preserve evidence integrity, acceptable in court
Reputation impact	Minimal impact	Potential loss of reputation if certain incident reach the public	Potential loss of reputation if certain incident reach the public

7 Related Standards, Policies, and Processes

- PCI DSS Requirements
(https://www.pcisecuritystandards.org/document_library)

- Adapted from NIST 800-61r2 – Computer Security Incident Handling Guide
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

8 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed

IT Manager	CEO/GM	IT Department	

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

9 Approval

____ ______________________

<Insert title of approver> Date

10 Revision History

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

Insert
Utility
logo
here

Information Security Incident Response Form

1 Incident Detection & Analysis

Item	Description
Incident #	
Date	
Incident Indicators **(employee report, SIEM, IDS or others)**	
Determine whether an incident has occurred	
Affected Systems (which systems are affected)	
Attack Vectors (how systems were affected)	(External/Removable Media, Attrition, Web, Email, Impersonation, Improper Usage, Equipment Loss or Others)
Incident Actors (whose actions affected system)	
Functional Impact (how significant is the system impact)	(None, Low, Medium, High)
Information Impact	(None, Privacy Breach, Proprietary Breach, Integrity Loss)
Recoverability Effort	(Regular, Supplemented, Extended, Not Recoverable)
Internal Notification (list internal notifications that have been made)	
External Notification	

(list external notifications that have been made)	
Other information	

2 Containment, Eradication and Recovery

2.1 Containment

Item	Description
Incident Status	
Integrity Assessment	
Containment Measures	

2.2 Eradication

Item	Description
Incident Status	
Vulnerability Assessment	
Eradication Measures	

2.3 Recovery

Item	Description
Incident Status	
Recovery Plan	

Recovery Process Documentation	
Validation	

3 Post Incident Analysis & Forensic

Item	Description
Collected Forensic Data	
Evaluation Process	
Lessons Learned	
Action Items	

Incident Handling Checklist

Action		Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the Incident Manager believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Reference: *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*

4 Revision History

Date of Change(s)	Revised by	Summary of Change(s)
		Original version

Insert
Utility
logo
here

PCI Compliance Policy

1 Overview/Purpose

<Utility Name> is processing credit card payments for their Members; convenience. The PCI Security Standards Council, an organization established by the payment card industry, established Data Security Standard (DSS) which defines strict requirements for the processing, storage, and transmission of credit card data. **<Utility Name>** will meet these requirements by training employees and implementing appropriate policies and technology.

2 Scope

PCI DSS requirements are addressed by many policies, procedures and standards of Information Security Program implemented by **<Utility Name>.** This policy addresses specific PCI DSS requirements only applicable to credit card payment processing.

3 Policy

3.1 Protect Stored Cardholder Data

3.1.1 Prohibited Data

Payment systems must not store of sensitive authentication data in any form after authorization (even if encrypted), beyond the life of the authorization transaction. Sensitive authentication data is defined as the following:

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. *(PCI Requirement 3.2.1)*
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance*. (PCI Requirement 3.2.2)*
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. *(PCI Requirement 3.2.3)*

No cardholder data of any type should be stored beyond that for which a legitimate business requirement exists. (*PCI Requirement 3.1)*

3.1.2 Displaying PAN

<Utility Name> will mask the display of Primary Account Numbers (PANs) and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: *(PCI requirement 3.3)*

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access;
- PANs must be masked when displayed such that only personnel with a legitimate business need can see the full PAN;
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

3.2 Restrict Access to Cardholder Data by Business Need to Know

3.2.1 Limit Access to Cardholder Data

- Access to **<Utility Name>** cardholder system components and data is limited to only those individuals whose jobs require such access. *(PCI Requirement 7.1)*
- Access limitations must include the following:
  - Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. *(PCI Requirement 7.1.2)*
  - Privileges must be assigned to individuals based on job classification and function (also called “role-based access control). *(PCI Requirement 7.1.3)*
  - *Query access to databases containing cardholder data must be restricted to authorized database administrators. (PCI Requirement 8.7)*

3.3 Assign a Unique ID to Each Person with Computer Access

3.3.1 Remote Access

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the **<Utility Name>** network) to the network by employees, administrators, and third parties. *(PCI Requirement 8.3)* Remote access tokens or devices must be assigned to a specific account, and not used generically. (*PCI Requirement 8.6)*

3.3.2 Access from Personal Devices

Any user-owned PCs or mobile devices used to access cardholder data must use personal firewall and anti-virus software acceptable to **<Utility Name>**. *(PCI Requirement 1.4)*

3.3.3 Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. *(PCI Requirement 8.1.5)*

3.3.4 User Accounts

For in-scope user accounts (those associated with the payment process), group, shared, or generic IDs, passwords must not be used. Additionally, the following authentication restrictions must be observed. *(PCI Requirement 8.5)*

- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

3.4 Physically Secure All Areas and Media Containing Cardholder Data

- All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel. *(PCI requirement 9.1.2)*
- Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:
  - All media must be physically secured. *(PCI requirement 9.5)*
  - Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. *(PCI Requirement 9.6)*
  - Media must be classified so the sensitivity of the data can be determined*.* *(PCI Requirement 9.6.1)*
  - Media must be sent by a secure carrier or other delivery method that can be accurately tracked. *(PCI Requirement 9.6.2)*
  - Management approval must be obtained prior to moving the media from the secured area. *(PCI Requirement 9.6.3)*
  - Strict control must be maintained over the storage and accessibility of media containing cardholder data. *(PCI Requirement 9.7)*

3.5 Destruction of Data

Cardholder data for which a business need no longer exists will be deleted at least every 6 months.

All media containing cardholder data must be securely destroyed when no longer needed for business or legal reasons. *(PCI requirement 9.8)*

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. *(PCI requirement 9.8.1.a)*

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. *(PCI requirement 9.8.1.b)*

3.6 Protection of Payment Devices

Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted*. (PCI requirement 9.9)*

<Utility Name> must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: *(PCI requirement 9.9.1)*

- Make and model of all devices.
- Location of each device (for example, the address of the site or facility where the device is located).
- Device serial number or other method of unique identification.

The payment devices must be periodically inspected, including checks of surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). *(PCI requirement 9.9.2)*

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: *(PCI requirement 9.9.3)*

- Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

3.7 Service Providers

<Utility Name> shall implement and maintain policies and procedures to manage service providers. *(PCI requirement 12.8)*

This process must include the following:

- The maintaining of a list of service providers. *(PCI requirement 12.8.1)*
- The maintaining of a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess. *(PCI requirement 12.8.2)*
- The implementation of a process to perform proper due diligence prior to engaging a service provider. *(PCI requirement 12.8.3)*
- The monitoring of service providers' PCI DSS compliance status. *(PCI requirement 12.8.4)* The maintaining of information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity*. (PCI requirement 12.8.5)*

4 Related Standards, Policies, and Processes

- PCI DSS Requirements (https://www.pcisecuritystandards.org/document_library)

5 Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

Responsible	Accountable	Consulted	Informed
IT Manager	**CEO**	**CFO** **CSR** **HR**	**All Employees**

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

6 Approval

<Insert title of approver> Date

7 Revision History

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

Insert
Utility
logo
here

Glossary

- **Access Point** – an electronic device that serves as a common connection point for devices seeking to use radio frequency waves to connect to a wired network. Wireless access points provide shared bandwidth such that as the number of users connected to an access point increases, the bandwidth available to each user decreases.

- **ACL** - a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file object has an ACL that contains (Alice: read, write; Bob: read), this would give Alice permission to read and write the file and Bob to only read it.

- **Chain Letter –** Chain letter (Email) is a term used to describe Emails that encourage you to forward them onto someone else

- **CHD** - Cardholder Data, which refers to data related to a credit card transaction.

- **CVSS** - Common Vulnerability Scoring System is a free and open industry standard for assessing the severity of computer system security vulnerabilities. As of April 2005 the Forum of Incident Response and Security Teams (FIRST) is the custodian of CVSS for future development.
  Scoring is the process of combining all the metric values according to specific formulas. Base Scoring is computed by the vendor or originator with the intention of being published and once set, is not expected to change. It is computed from the big three confidentiality, integrity and availability. This is the foundation which is modified by the Temporal and Environmental metrics. The base score has the largest bearing on the final score and represents vulnerability severity. More information about CVSS you can find at FIRST http://www.first.org/cvss/use-design

- **Demilitarized Zone (DMZ)** - is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.

- **Dual Homing** - A computer with two or more network interfaces. A dual-homed host can act as a simple firewall on a small network as long as there is no direct IP traffic between the Internet and the internal network. In such a case, all Internet applications are run only on the dual-homed host.

- **PHI** - Personal Health Information, is individually identifiable health information, as defined by 45 CFR 160.103, known as HIPAA.

- **PII** - is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

- **Ponzi –** A Ponzi scheme is a fraudulent investment operation that involves paying returns to investors out of the money raised from subsequent investors.

- **Pyramid Scheme –** A fraudulent scheme in which people are recruited to make payments to the person who recruits them while expecting payments from the persons they recruit.

- **RPO** - A Recovery Point Objective is the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.

- **RTO** - Recovery Time Objective is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.

- **Spam** – The unauthorized and/or unsolicited electronic mass mailings

- **Split Tunneling** - A computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application.

- **System owner -** The system owner is responsible for every stage in the lifecycle of an information system including procurement, integration, modification, operation, maintenance, retirement.

- **Rogue Access Point** - A Rogue Access Point is any device that adds an unauthorized (and therefore unmanaged and unsecured) Wireless LAN (WLAN) to the organization’s network. A rogue AP could be added by inserting a WLAN card into a back office server, attaching an unknown WLAN router to the network, or by various other means.

- **VPN** – extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus benefit from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.

Appendix A: PCI DSS Mapping

Mapping between PCI DSS Requirements and ISPL

Req #	Requirement	ISPL Document
1	**Secure network and systems**	
1.1	Firewall and router configuration standards; identify all connections to cardholder data; network diagram; data flows for cardholder data; configuration review every 6 months; testing after configuration change	Network Configuration Standards IT Change Management Procedure Firewall Configuration Change From
1.2	Deny all inbound and outbound traffic to cardholder data network; allow only that which is required	Network Configuration Standards
1.3	Prevent direct traffic from the Internet to the CDE	Network Configuration Standards
1.4	Personal firewall on any mobile or employee-owned devices	PCI Compliance Policy
1.5	Related security policies documented, in use, and known to affected parties	Information Security Policy
2	**Do not use vendor defaults for passwords and other security parameters**	
2.1	Always change vendor defaults, and remove unnecessary accounts, including wireless devices	Password Policy Network Configuration Standard
2.2	Configuration standards for all components to address known vulnerabilities; update configurations as new vulnerabilities are discovered.	Network Configuration Standard
2.3	Encrypt all non-console admin traffic using strong cryptography	Data Encryption Policy
2.4	Maintain an inventory of all components in scope for PCI DSS	PCI Compliance Policy
2.5	Related security policies documented, in use, and known to affected parties	
3	**Protect stored Cardholder Data**	
3.1	Limit CD stored to the amount needed, and the retention time required; purge unnecessary data at least quarterly.	PCI Compliance Policy
3.2	Do not store sensitive authentication data	PCI Compliance Policy
3.3	Mask PAN when displayed; limit full display to essential personnel.	PCI Compliance Policy
3.4	Render PAN unreadable when stored.	PCI Compliance Policy
3.5	Procedures to protect keys used for encryption from disclosure and misuse.	Data Encryption Policy
3.6	Fully document key management processes	Data Encryption Policy
3.7	Related security policies documented, in use, and known to affected parties	

4	**Encrypt transmission of CHD across open, public networks**	
4.1	Use strong cryptography and security protocols when transmitting CHD across open, public networks; Use industry best practices.	Data Encryption Policy
4.2	Never send PAN via end-user messaging (email, SMS, etc)	Data Encryption Policy
4.3	Related security policies documented, in use, and known to affected parties	
5	**Protect all systems against malware, and regularly update anti-virus software**	
5.1	Deploy anti-virus software on all systems subject to malware	Acceptable Use Policy
5.2	Ensure that anti-virus mechanisms are kept current	Acceptable Use Policy
5.3	Ensure that anti-virus mechanisms are actively running, and cannot be disabled by users	Acceptable Use Policy
5.4	Related security policies documented, in use, and known to affected parties	
6	**Develop and maintain secure systems and applications**	
6.1	Identify security vulnerabilities using a reputable outside source; assign a risk ranking.	System Acceptance and Configuration Policy
6.2	Install applicable vendor-supplied security patches; install critical patches within one month.	System Patching Policy
6.3	Securely develop internal and external software applications in accordance with PCI requirements and industry best practices	
6.4	Follow change control processes/procedures for all changes to system components.	IT Change Management Procedure
6.5	Prevent common coding vulnerabilities by training developers in secure coding techniques	
6.6	Protect public-facing web applications by application assessments quarterly of after changes, or using automated means	Vulnerability Management Policy
6.7	Related security policies documented, in use, and known to affected parties	
7	**Restrict access to CHD to those with a need to know**	
7.1	Limit CHD access to those who require such access to do their jobs	PCI Compliance Policy
7.2	Establish access control system; set to deny all, unless specifically required	PCI Compliance Policy
7.3	Related security policies documented, in use, and known to affected parties	
8	**Identify and authenticate access to system components**	
8.1	Policies and procedures to ensure proper user identification management, including unique user names	PCI Compliance Policy
8.2	Employ at least one to authenticate all users: 1) Something you know; 2) Something you have; 3) Something you are.	User Account Management Policy
8.3	Use two-factor authentication for all remote access.	Remote Access Policy

8.4	Develop, implement, and communicate authentication policies and procedures to all users.	
8.5	Do not use group, shared, or generic user ids	PCI Compliance Policy
8.6	Use of authentication methods, such as tokens, must be assigned to specific user ids	PCI Compliance Policy
8.7	Access to databases containing CHD must be restricted; only DBAs may have direct query access	PCI Compliance Policy
8.8	Related security policies documented, in use, and known to affected parties	
9	**Restrict physical access to CHD**	
9.1	Use facility entry controls to restrict and track access to systems with CHD	PCI Compliance Policy
9.2	Use ID badges or other means to distinguish visitors from employees.	Physical and Environmental Security Policy
9.3	Control physical access by employees based on job function; revoke access immediately upon termination.	Physical and Environmental Security Policy
9.4	Ensure that visitors are authorized before entering areas with CHD; use tokens to identify that expire and are revoked when leaving; use a visitor log, and retain for at least 3 months.	Physical and Environmental Security Policy
9.5	Physically secure media; store backups securely, preferably offsite.	Backup and Recovery Policy
9.6	Strictly control media distribution.	IT Asset Accountability Policy
9.7	Strictly control media storage and accessibility.	Backup and Recovery Policy
9.9	Protect devices with interact with cards from tampering and substitution; periodically inspect POS devices; train personnel to spot suspicious activity.	PCI Compliance Policy
9.10	Related security policies documented, in use, and known to affected parties	
10	**Track and monitor all access to network resources and CHD**	
10.1	Implement audit trails to link access attempts to each individual user.	User Account Management Policy
10.2	Implement audit trails to all reconstruction of key events, such as access by an individual with admin access	User Account Management Policy
10.3	Record for each event the user id, type of event, date/time, success/failure, origination, name/identity of system or resource	System Logging and Monitoring Policy
10.4	Synchronize time clocks	System Logging and Monitoring Policy
10.5	Secure audit trails so they cannot be altered	System Logging and Monitoring Policy
10.6	Review logs and security events; perform critical log reviews daily.	System Logging and Monitoring Policy
10.7	Retain audit trails for one year, with three months readily available	System Logging and Monitoring Policy

10.8	Protect devices with interact with cards from tampering and substitution; periodically inspect POS devices; train personnel to spot suspicious activity.	PCI Compliance Policy
11	**Regularly test security systems and processes**	
11.1	Inventory and test for wireless access points	Network Configuration Standard
11.2	Run internal and external network vulnerability scans quarterly, and after a significant change; quarterly scans must be done by an ASV; correct issues and re-run scans until clean	Vulnerability Management Policy
11.3	Run penetration scans at least annually, and after a major change; test network segmentation designed to reduce PCI scope	Vulnerability Management Policy
11.4	Use IDS/IPS to detect and prevent network intrusions	Network Configuration Standard
11.5	Implement a change detection methodology, such as file integrity monitoring	Physical and Environmental Security Policy
11.6	Related security policies documented, in use, and known to affected parties	
12	**Maintain a policy that addresses information security for all personnel**	
12.1	Establish, maintain, and publish a security policy; update manually, or after significant changes	Information Security Policy
12.2	Implement a risk assessment process, performed at least annually	IT Risk Management Policy
12.3	Implement an acceptable use policy for critical technologies, such as laptops, remote access, etc	Acceptable Use Policy
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel	Information Security Policy
12.5	Assign information security responsibilities to an individual or group	Information Security Policy
12.6	Implement a formal security awareness program	Cybersecurity Awareness Training Policy
12.7	Screen candidates prior to hiring	Personnel Security Policy
12.8	Implement a program to manage service providers with access to PCI data	PCI Compliance Policy
12.9	N/A	
12.10	Implement an incident response plan	Incident Management Policy