

Data Protection & Availability Standard

# 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.

# Scope

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

# Standard

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

## 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

### 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)

## 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**>.

### 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)

### 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

## 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.

### 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

# Compliance

## Compliance Measurement

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

## Exceptions

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

## Non-Compliance

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

# Related Standards, Policies, and Processes

(Cross references to industry standards)

* *Data Classification* Policy

# 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.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

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