

Data Classification Policy

# 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.

# Scope

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

# Policy

## Data Protection Classification

### 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

### 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.

### 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.

### 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.

### 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.

## Data Availability Classification

### 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

### 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

### 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.

# Compliance

## Compliance Measurement

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

## Exceptions

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

## Non-Compliance

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

# Related Standards, Policies, and Processes

* 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>)

# 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.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

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