|  |  |
| --- | --- |
| **Data Governance Policy** | **No. z** **IS-7** |
|  | **Effective Date:** March 30, 2023 |

# **Overview**

Data contained on the [Organization Name] network and connected endpoint devices should be classified in a way to help determine the method of protection. This is very challenging in the [Organization Name] since the mission of the organization puts the [Organization Name] in contact with high level executives to conduct its work and the data exchanged will often be confidential or restricted. And the information that is contained on [Organization Name] networks and endpoint devices can range from public to private to highly confidential. Until the network or endpoint device is examined, it will be important to treat all data bearing devices as containing the highly confidential data.

# **Purpose**

The purpose of this Guideline is to establish a framework for classifying institutional data based on its level of sensitivity, value, and criticality to the [Organization Name]. Classification of data will aid in determining baseline security controls for the protection of data.

# **Scope**

Data governance focuses on improving data quality, protecting access to data, establishing definitions, maintaining data, and documenting data policies. The [Organization Name] data is an asset and must be maintained and protected. The data must remain accurate to be trusted by the entire team to make follow on decisions at all levels of the organization.

The National Institute of Standards and Technology (NIST) defines three levels of Risk for data classification. They are as follows.

**3.1 Low**

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

**3.2 Moderate**

The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

**3.3 High**

The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **POTENTIAL IMPACT** | | |
| **Security Objective** | **LOW** | **MODERATE** | **HIGH** |
| **Confidentiality** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity** Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability** Ensuring timely and reliable access to and use of information. | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

# **Policy**

## **4.1 Data Classification**

Data Classification is required for all [Organization Name] information. Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the [Organization Name] should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels, or classifications:

## **4.1.1 Default classification of data**

Any data that contains PII concerning any individual or that is covered by local, state, or Federal regulations is classified as Restricted data by default. All other data is classified as Private data by default.

All other [Organization Name] data should be classified into one of three sensitivity levels, or classifications:

## **4.1.2 Restricted Data**

Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the [Organization Name] or its affiliates. The highest level of security controls should be applied to Restricted data. Restricted data is any data that contains personally identifiable information (PII) concerning any individual, as well as any data that contains PII that is regulated by local, state, or Federal privacy regulations. These regulations may include, but are not limited to:

|  |  |  |
| --- | --- | --- |
|  | **Set of Regulations** | **Industry Category** |
| FERPA | Family Educational Rights and Privacy Act | Education |
| GLBA | Gramm-Leach-Bliley Act | Financial |
| HIPAA | Health Insurance Portability and Accountability Act | Healthcare |
| NERC | North American Electric Reliability Corporation | Electric Power |
| PCI DSS | Payment Card Industry Data Security Standards | Retail |
| SOX | Sarbanes-Oxley Act | Security Exchange Comm |
| GDPR | General Data Protection Regulation | European |

**4.1.3 Private Data**

Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the [Organization Name] or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data.  A reasonable level of security controls should be applied to Private data.

**4.1.4 Public Data**

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the [Organization Name] and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

## **4.2 Reclassification**

On a periodic basis, it is important to reevaluate the classification of Institutional Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the [Organization Name]. Conducting an evaluation on an annual basis. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

## **4.3 Governing Institutional Data**

The following principles are set forth as minimum standards to govern the appropriate use and management of institutional data:

**4.3.1** Institutional data is the property of the [Organization Name] and shall be managed as a key asset.

**4.3.2** Unnecessary duplication of institutional data is discouraged.

**4.3.3** Institutional data shall be protected.

**4.3.4** Institutional data shall be accessible according to defined needs and roles.

**4.3.5** Institutional representatives will be held accountable to their roles and responsibilities.

**4.3.6** Necessarymaintenance of institutional data shall be defined.

**4.3.7** Resolution of issues related to institutional data shall follow consistent processes.

**4.3.8** OhCR Reservists are responsible for the subset of data in their charge.

# **Policy Compliance**

* 1. **Compliance Measurement**

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

# **Exceptions**

Any exception to the policy must be approved by the Infosec team in advance.

# **Non-Compliance**

An end user found to have violated this policy may be subject to disciplinary action, up to and including termination of appointment to the [Organization Name].

# **Related Standards, Policies and Processes**

United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008

# **Definitions and Terms**

**Confidential Data**

Term that typically represents data classified as Restricted. This term is often used interchangeably with sensitive data.

**Institutional Data**

All data owned or licensed by the [Organization Name].

**Non-public Information**

Any information that is classified as Private or Restricted Information according to the data classification scheme defined in this Guideline.

**Sensitive Data**

Represents data classified as Restricted. This term is often used interchangeably with confidential data.

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
| March 30, 2023 | [Organization Name] | Created initial draft |
|  |  |  |