Data Classification Standards and Guidance

Data Classification
Standards and Guidance

Effective: August 1, 2015
Contact: Information Technology Services

Contents

Purpose
1. Classification
2. Guidance on the Classification of Data
3. Example Classifications of Common Data elements
4. Resources

Purpose

The Data Classification Standards and Guidance provides instructions for complying with the Data Classification policy.

1. Classification

Data are classified in four categories depending on sensitivity and importance. Subsets of data shall have the same classification level and utilize the same protective measures as the original data in the system of record. Data must be consistently protected throughout its life cycle in a manner commensurate with its sensitivity, regardless of where it resides or what purpose(s) it serves.

1.1. Restricted

Data that are required to be protected by applicable law, statute (e.g., Iowa Code 22.7, HIPAA, ITAR, or other statute) or university policy, or which, if disclosed to the public could expose the university to legal or financial obligations. This level also represents information for which the Data Steward has exercised their right to restrict access.

1.2. High

Data that are protected by the Family Educational Rights and Privacy Act (FERPA) or Iowa Code 22.7(1) regarding student records and which has been classified by the Office of the Registrar as confidential student information. It also includes information that would otherwise be classified as “Restricted”, but it has been determined by the Data Governance Committee that handling and storing of this data using standards for “Restricted” would significantly reduce faculty/staff/student effectiveness when acting in support of Iowa State University’s mission and/or it is specifically listed in the table of examples below.

1.3. Moderate

Data for which access must be guarded due to proprietary, ethical, or privacy considerations. This classification applies even though there may not be a civil statute requiring this protection. This information is not intended for public dissemination, but its disclosure is not restricted by federal or state law. It also includes information that would otherwise be classified as “High”, but it has been determined by the Data Governance Committee that handling and storing of this data using standards for “High” would significantly reduce faculty/staff/student effectiveness when acting in support of Iowa State University’s mission and/or it is specifically listed in the examples below.

1.4. Low

Data which may or must be open to the general public. This information is not restricted by local, state, national, or international statute regarding disclosure or use. top

2. Guidance on the Classification of Data

If the appropriate classification is not prescribed elsewhere in this document, the Data Steward shall consider each security objective and may use the following table as a guide. It is an excerpt from Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

Security Objective	LIMITED IMPACT	SERIOUS IMPACT	SEVERE IMPACT
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.

As the potential impact to the university increases, data should be more restrictively classified, moving from Low to Restricted. Typically data involving severe or catastrophic impact would be classified as restricted. If an appropriate classification is still unclear after considering these points, the Data Stewards shall contact the Information Security Office for assistance. top

3. Example Classifications of Common Data Elements

Data for which a data steward cannot make a determination or for which a data steward cannot be identified may be referred to the Data Classification Committee for classification. For a comprehensive list of prescribed data classifications refer to the Classifications of University Data.

Restricted	High	Moderate	Low
Social security numbers Credit card numbers Financial account numbers, such as checking or investment account numbers Driver's license numbers Health insurance policy ID numbers Health information, including protected health information (PHI) Passport and visa numbers Export controlled information under U.S. laws Authentication credentials or identity verification information	Confidential student records University ID numbers Student class schedules ID card photographs Disciplinary files Admission applications Authoritative copy of directory information as defined by the registrar under FERPA	Research data (electronic and physical) Faculty/staff employment applications, personnel files, benefits information, and birth date Privileged attorney-client communications Authoritative copy of university schedule of classes Authoritative copy of approved census facts	Directory information, as defined by the registrar under FERPA. University schedule of classes Approved census facts

Once data is classified, data stewards are responsible for applying the university Minimum Security Standards and Guidance which describe the appropriate steps for protecting data based on the data classification. top

4. Resources

Data Classification Policy
Minimum Security Standards and Guidance
Data Governance Committee [DOCX] (link pending)
Information Security Office (email) (link pending)
Information Technology Security Policy
IT Security Incident Reporting Policy
IT Glossary of Terms (link pending)
Classifications of University Data (link pending)
Classifications of Common University Services (link pending)