OFFICE OF Information Technology

Information Resource Data and System Classification Standard

This standard leverages existing University of Alaska Data Classification, extends it to systems and adds the dimensions for availability and criticality. This classification and labeling of systems will be used to better communicate a systems role within the University's IT environment, the appropriate safeguards that apply to a system and inform disaster recovery and business continuity planning decisions.

Covered Systems

This classification is applicable to a wide variety of information resources that are part of the University of Alaska's (UA) information technology (IT) environment. A system may be any IT resource to which the security safeguards may be applied. Examples of systems include, but are not limited to:

1. Desktop, laptop, or server computers running general purpose or specialized operating systems such as Windows, Mac OS, and Unix
2. Network server applications, such as an FTP-server application
3. Web applications, such as a wiki
4. Databases
5. Network attached appliances that provide IT services
6. Hosted services operated by partners in support of UA

All of the above systems may perform their own authentication and authorization, logging and auditing, and have their own configurations that must be managed. Each of them is considered a compliance object to be protected.

Follow these steps to determine a system's classification:

1. Determine the *Data Classification* of the data stored on the system.
2. Determine the *Availability Requirements* of that system, including whether it is a server, or personal workstation.
3. Select the appropriate Classification from the *System Criticality Categories* table.

A system manager may choose to classify a system as higher criticality than that indicated by the table. However, if they choose to do so, the system must meet the security measures for that higher level. Systems hosting data or services at multiple classification levels will be assigned the highest classification level in the data, availability and criticality areas and must meet the security measures for that higher level.

Data Classification

The authoritative source of information on data classification at UA is University Regulation 02.07.090-094. It outlines three levels of data classification related to the impact of an unauthorized disclosure of the data. The data types are listed below along with descriptions and examples; however the policy document linked to above is the authoritative source of information on data classification.

Data Classification	Institutional Risk from Disclosure	Description	Examples

Restricted	High	Data whose unauthorized access or loss would seriously or adversely affect UA, students, employees, a partner, or the public.	• HIPAA • FERPA • Export controlled, ITAR covered data or software • Information required to be protected by contract • Human subjects identifiable research data • Trade secrets, intellectual property and/or proprietary research • Attorney/client privileged records • Payment Card Industry • University banking records • Restricted police records • Computer account passwords • Gramm-Leach-Bliley • Certain affirmative action related data • Alaska Personal Information Protection Act • Library records confidentiality
Internal Use	Medium	Data not restricted by law, regulation or formal agreement but that should be protected from general access.	• Employee Internet usage • Specific technical security measures • UA employee business-related email (including student employees, but only their work-related email) • Location of assets • Faculty promotion, tenure, evaluations • Supporting documents for UA business functions • Public research • Supporting documents for UA business functions • Aggregate human subjects research data • Animal research • Proposal records

Public	Low/None	All public data	• Campus promotional material • Annual reports • Press statements • Job titles • Job descriptions • Employee work phone numbers (with special exceptions) • University of Alaska business records • Employee work locations (with special exceptions) • Employee email addresses (with special exceptions)

Special Data Types

Some data comes with specific and externally mandated controls that must be applied for its protection.

- Credit Card numbers are subject to specific industry standards and thus may need to be handled differently in some situations.
- Other data covered by export controls are subject to additional rules on distribution, in particular sharing with non-U.S. persons.
- Personal Health Information (PHI) data can be subject to HIPAA protection requirements and HITECH Act enforcement.

System Classification

The system classification framework draws a distinction between systems storing data directly, systems with privileged access to data but do not store it directly, and systems that make general use of data, as follows:

- "**Storing**" data indicates that the data is available through normal file system access methods. For example, data residing in NFS mounts or Windows mapped drives (e.g., an X: drive) is considered to be stored on any client systems which actively mount the shares, as well as the system which physically houses the disks. However, data residing in a database is considered to be stored only on the database server itself since no file system access methods allow clients to obtain direct access to the data.
- "**Privileged access**" exists when there is a non-file system method of accessing data that is stored on another system. For example, a web server that connects to a separate back-end database server has privileged access to data stored on that system. Similarly, the workstation of a system administrator who commonly logs into both servers with administrator credentials has privileged access to both systems.
- "**General use**" includes access or processing of data by end-user workstations, using a non-privileged account.

Availability Requirements

There are three availability classifications representing the impact to the University if a given system were unable to perform tasks it is responsible for.

Availability Classification	Institutional Risk from Disclosure	Description	Examples
High Availability	High	Loss of access to the system would have a significant impact on UA, students, employees, a partner, or the public.	• Systems participate in a University-level disaster preparedness plan • Systems supporting automated or online business services • Systems responsible for delivery of or support for educational services • Systems have redundant hardware in separate geographic regions • Systems that serve 1,000 or more users
Medium Availability	Medium	Loss of access to the system could have a significant impact on a large number of users or multiple business units.	• Systems participate in the disaster preparedness plan of a large University unit • Systems have redundant hardware in a single geographic region
Standard Availability	Low	Loss of access to the system could have a significant impact on an individual user or unit.	• Systems do not participate in a disaster preparedness plan • Systems have no redundant hardware provisioned • Individual workstations, laptops or devices • Small workgroup servers

Server/Individual Context

- **Servers** are characterized by the presence of network accessible services and are typically accessed simultaneously by many remote users concurrently via the network services they provide.
- **Individual workstations, laptops or devices** typically do not have network accessible services, and are typically accessed by a single user at a time.

System Criticality Categories

System Criticality is determined according to the following table. When more than one category applies, the system should be classified in the highest applicable category.

System Classification	Classification Guidelines	Examples
High Criticality	Servers that store ***Restricted*** data OR servers that host ***High Availability*** applications	• A database which stores employee Social Security numbers • Institution home pages, which are designated as a channel for distributing information in the event of a campus emergency
Medium Criticality	Servers that store ***Internal Use*** *data* OR servers that have privileged access to systems that store ***Restricted*** data OR servers that host ***Medium Availability*** applications	• A departmental file server where salary and benefits information is stored • A web server that stores no data locally, but that runs an application that accesses a database stored on a separate database server that contains Social Security numbers • The web server for a school which is required to deliver e-learning service
Standard Criticality	Servers that store only ***Public*** data OR servers that have privileged access to systems that store ***Internal Use*** data OR servers that host ***Standard Availability*** applications OR individual workstations, laptops or devices	• All individual workstations, laptops or devices • All IT systems that are not classified as *Medium* or *High Criticality* • Workgroup servers that do not store *Protected* or *Restricted Data*

Related Policies

- University of Alaska Regulation 02.07.090-094 Data Classification Standards (http://www.alaska.edu/bor/policy/02-07.doc)
- Health Insurance Portability & Accountability Act (HIPAA) (http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html)
- Health Information Technology for Economic and Clinical Health Act (HITECH Act) (http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html)

Send questions or comments to: security@alaska.edu.

Effective Date

January 1, 2014