UNIVERSITY OF
WISCONSIN SYSTEM

Enterprise Data Management Council

DECISION: Data classification of enterprise data according to risk

EDGC Decision Date: April 24, 2023

Background

The success of ATP/EAP/ASP projects depends, in part, on classifying enterprise data elements across enterprise systems in a standard way.

UW System Administrative Policy 1031 calls for data to be categorized as high, moderate, or low risk. It provides standards for classification and minimum protections for each level of risk. Data classification “determines the extent to which technical, administrative, and physical controls should be applied to protect the data from theft, alteration, loss of integrity, and/or misuse.” SYS 1031 is currently under revision.

UW-Madison employs a classification system with four categories: public, internal, sensitive, restricted (per UW Madison IT policy UW-504) spanning the spectrum of low to high risk. Many developers working with enterprise data across the ATP/EAP/ASP portfolio are from UW-Madison and are accustomed to UW-Madison's classification system. Data in UW-Madison's ancillary systems use UW-Madison’s classification system.

Lack of agreement on a single risk classification may result in developers applying different classifications in Workday vs. the data lake vs. ancillary systems. This reduces the opportunity to apply a common set of security roles across enterprise systems, and where possible, ancillary systems. And it could lead to inconsistent access and security of enterprise data.

Decision

APT/EAP/ASP apply the draft data classification schema (below) that brings together existing Madison and UW System policy in anticipation of the pending revision, noting that this **MAY** change by the time the policy revision is fully vetted.

Draft Data Classification Schema

Public (Low Risk)	**Sensitive (Moderate Risk)**	**Restricted (High Risk)**
Data is classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in **little or no risk** to the University and its affiliates. Public data requires no confidentiality, integrity, or security protections. Examples: Data approved for display on websites and/or made available to the public.	Data is classified as Sensitive when the unauthorized disclosure, alteration or destruction of that data could result in a **moderate level of risk** to the university or its affiliates. A reasonable level of security safeguards must be applied to sensitive data. Examples: By default, all institutional data that is not explicitly classified as Public or Restricted must be treated as Sensitive data.	Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a **high level of risk** to the university or its affiliates. Strong security controls must be applied restricted data and access will frequently be limited to a small number of individuals. Examples: Information protected by state or federal privacy regulations (e.g., FERPA, HIPAA), or by standard confidentiality agreements. **Sub-category: Highly Restricted -* Examples include data that may pose a threat to health and safety (e.g. bio toxins), Controlled Unclassified Information (CUI), export-controlled research information (e.g., ITAR and EAR), or research data associated with some Department of Defense contracts.

Who Developed the Recommendation?

- Joe Johnson, UWSA Director of Governance, Risk, and Compliance
- Lisa Johnston, UW-Madison Director of Data Governance

Who Was Consulted in the Development of the Recommendation?

The following stakeholders were consulted about the proposed data classifications, in the context of the forthcoming revision of SYS 1031. These stakeholders have supported the general direction being proposed and have not raised any initial concerns. However, the proposed data classification may change during the SYS 1031 revision over the coming months.

- Ed Murphy (UW System, AVP Information Security)
- Jim Treu (UW System, Director of Security Awareness and Outreach)
- Mike Bubolz (UW Breen Bay, Interim CIO)
- Patti Havlicek (UW-Madison, RMC Asst. Director)
- Other various Technology and Information Security Council (TISC) representatives
- UW Madison Data Stewards
- UW Madison IT Policy Advisory Team (subcommittee of Information Technology Council)