University of Maine System

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Data Classification

I. PURPOSE AND OVERVIEW

University data is information that is either wholly or partially owned by the University, has been entrusted to the University, or is generated by or for the University. University data may exist in any format (i.e., electronic, paper, film, audio) and includes, but is not limited to, academic, research and administrative data, and any other data that support the functions and operation of the University.

All University information is assigned one of the following four protection levels based on confidentiality, integrity and availability requirements, and commensurate with the risks of financial loss, reputational damage, operational disruptions, legal ramifications, or other risk to entit(ies) or individual(s) in the event of unauthorized use, access, disclosure, modification, or loss:

- Restricted
- Confidential
- Internal
- Public

All individuals working on behalf of the University are responsible for understanding the protection levels for University data, and ensuring compliance with all applicable regulation, statute, University policy, contractual or other requirements, and incident response.

To the extent that particular data types are not explicitly addressed within this APL, each business unit or department shall classify its data by considering the potential for harm to individuals or the University in the event of unintended access, use, disclosure, modification, loss or destruction; and in consultation with the University Information Security Office.

II. CLASSIFICATION LEVELS

A. Restricted

Information classified as Restricted has specified requirements for the control of confidentiality, integrity, or availability of the data due to regulation, statute, contract or other requirement or agreement; or that may pose a severe risk to the University in the event of

unauthorized use, access, disclosure, modification or loss. Restricted data includes, but is not limited to, personal information as defined in 10 M.R.S.A § 1347, regulatory research information, information that requires protection under regulation, statute or agreement (i.e., EAR/ITAR, HIPAA, PCI, GLBA), and high-risk operational data.

Stringent or prescribed requirements exist for restricted data, including special permissions, training, hardware, software, and incident response. Restricted data should be used only when no alternative exists and must be carefully protected. Any unauthorized access, use, disclosure, modification, or loss or destruction of Restricted data must be reported and in accordance with regulation, statute, contract, University policy, and any other requirement or agreement.

Examples of Restricted data include:

1. Personally Identifiable Information (PII), meaning, an individual's first name (or initial) and last name in combination with any one or more of data elements: social security number, driver's license number, account number, password, access code, or other information that uniquely identifies an individual
2. Student Federal Student Aid including FAFSA data, ISIR data, key processing results, expected family contribution, awards, the student's financial aid history as reflected in NSLDS, ISIR-derived student aid eligibility and resultant award and distribution, and information from the Common Origination and Disbursement (COD) System.
3. Personally identifiable health or genetic information whether or not subject to the Health Insurance Portability and Privacy Act (HIPAA) and/or the Genetic Information Nondiscrimination Act (GINA)
4. Personal health or genetic information that is used in research, such as human subjects data, unless otherwise classified by an Institutional Review Board (IRB)
5. Human resources and personnel data, including criminal background checks, disability, medical or genetic, tax and payroll records
6. Financial, credit card, and other account numbers subject to the Payment Card Industry Data Security Standard (PCI DSS)
7. Technical or research data controlled by U.S. Export Control regulation such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR)
8. Criminal Justice information Services (CJIS)
9. Identification and authentication information used to access electronic resources
10. System security information, access codes and devices
11. Emergency protocols
12. Protection protocols for and location of radioactive, explosive, chemical or other hazard class materials
13. Any information which could permit a person or persons to harm or attempt to harm the University or individual(s) or assume the identity of an individual.

B. Confidential

Confidential information may adversely affect individuals or the business of the University in the event of unauthorized access, use, disclosure, modification, loss or destruction; or is required to be kept confidential by regulation, statute, or other contractual confidentiality obligation such as with a third party. Confidential data shall be used only when necessary for business purposes and shall be protected when in use and while being stored or transported.

Requirements may exist for Confidential data that include special permissions, hardware, software, training, and incident response.

Examples of Confidential data include:

1. Student information covered by the Family Educational Rights and Privacy Act (FERPA)
2. Information protected under the General Data Protection Regulation (GDPR)
3. University financial information, including donor information and records
4. University student or employee identification numbers, especially when stored with other identifiable information such as name and email address
5. Individual employment information, benefits and performance appraisals for current, former, and prospective employees
6. Attorney-Client privileged information
7. Student special services and accommodations records
8. Financial Aid data collected through a source other than the FAFSA such as the CSS profile.
9. Exam questions and answers
10. Information that is the subject of a contractual confidentiality obligation that is not otherwise classified as Restricted

C. Internal

Internal data is information that is potentially sensitive and is not intended to be readily available to the public. The dean, department head, or another individual authorized to direct data classification shall determine which information is Internal and prescribe the methods for managing Internal data. Questions regarding Internal data should be first directed to such authorized individuals.

Examples of Internal data include:

1. Unpublished research, patent applications, work papers, and intellectual property, unless otherwise designated as Restricted or Confidential
2. Email and calendar events, unless otherwise designated as Restricted or Confidential
3. Meeting minutes
4. Contact lists that contain information that is not publicly available
5. Internal use survey and/or webform data

6. Marketing plans
7. Departmental procedural documentation that is generally private

D. Public

Public data is information that may be disclosed to any person regardless of their affiliation with the University.

Note: While Public data may be shared broadly within and outside the University, employees should generally still protect Public data from unauthorized modification or loss.

Examples of Public data include:

1. Press releases and marketing materials
2. Directory information of students and employees (except where students have placed a hold on specific directory information in accordance with FERPA. FERPA Guidelines are published as Section 304.5 to the UMS Academic Affairs Administrative Procedures Manual)
3. Course catalogs
4. External facing website information
5. Public events & event calendars
6. Published research

III. Contact information

For questions or comments about this policy, please contact the Information Security Office at infosecurity@maine.edu, or 207-581-9105.