DATA SECURITY CLASSIFICATIONS POLICY

SCOPE: This policy applies to all information systems containing University Information.

PURPOSE: Define the classifications of data and the required security controls associated with the data classification. This policy is not intended to supersede the law or specific policies hyperlinked below, and any conflicts will be controlled by the specific policies and not this one.

DATA CLASSIFICATIONS: University Information will be classified as Legally Restricted, Confidential, Internal or Public, as defined below. Data should be held at the highest classification until classified otherwise. Collections of data (e.g. database, document repositories, web servers, etc.) should be treated at the highest classification of any data contained within the collection. If you have a question on the classification of data, please contact your Chief Information Security Officer or Office of Legal Counsel.

LEGALLY RESTRICTED

What it is: information for which use and access is restricted by law. The breach of this type of information may result in criminal or civil fines and liabilities for the University. Law may require notification on any breach of this type of data. Examples include:

- Protected Health Information (PHI)
- Social Security Number (SSN)
- Employee Personally Identifiable Information (PII)
- State issued driver's license or non-driver ID
- Passport numbers
- Criminal, civil and regulatory investigations
- Payment Card Information (i.e. credit or debit cards)
- Bank account numbers
- Regulated data (i.e. FISMA contracts)

CONFIDENTIAL

What it is: information that is sensitive or proprietary which is kept on a strictly need-to-know basis. Some examples may include:

- Personnel records
- De-identified PHI data marked confidential by researchers
- Educational Records (FERPA) except Directory Information as defined by the FERPA Policy
- Records and communication of the Board of Trustees
- University Audit reports and work papers
- Internal investigations into violations of law and University policies
- Information the University has agreed to hold confidential under a contract or grant
- Patent applications, or other unpublished intellectual property, if designated as confidential by the Principal Investigator (PI)

INTERNAL

What it is: Information which is necessary for people to perform their work at the University and is properly available to others at the University, but is not appropriate to be known by the general public. Access to this type of data requires authentication, (i.e. a username and password) in order to access the data. Examples include:

- De-identified PHI
- Research not containing legally restricted or confidential data
- Administrative data not containing legally restricted or confidential data

PUBLIC

What it is: Information that is available to all members of the University and may be made available to the general public. The University reserves the right to control the content and format of Public data. This type of information is frequently accessible from the Internet that does not require authentication

- Publications
- Audited financial statements
- Annual reports
- Student Directory Information
- Employee Directory Information

DEFINITIONS:

University Information is any University business or academic information created or managed by students, staff, faculty, contractors, consultants, temporary employees, guests, volunteers and others affiliated with the University.

Breach: The unauthorized acquisition, access, use, or disclosure of sensitive information which compromises the security or privacy of such information.

Protected Health Information (PHI) is health information (oral or recorded) that associates an individual with a health care provider, a health condition or diagnosis, a health care facility, or a health care plan. Because this information is so prevalent in the health care and research operations of the University, it is recommended that staff who work in these areas assume that most communication contains PHI. Some examples of PHI:

1. Information is considered to be de-identified under HIPAA if all of the following 18 identifiers are removed:
    a. Names;
    b. All geographic subdivisions smaller than a State, including: street address, city, county, precinct, zip codes and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly-available data from the Bureau of Census:
        (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000; and

(2) the initial three digits of the zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

c. All elements of dates (except year) for dates directly related to an individual, including: birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
d. Telephone numbers;
e. Fax numbers;
f. E-mail addresses;
g. Social Security numbers;
h. Medical record numbers;
i. Health plan beneficiary numbers;
j. Account numbers;
k. Certificate/license numbers;
l. Vehicle identifiers and serial numbers, including license plate numbers;
m. Device identifiers and serial numbers;
n. Web Universal Resource Locators (URLs);
o. Internet Protocol (IP) address numbers;
p. Biometric identifiers, including finger and voice prints;
q. Full face photographic images and any comparable images; and
r. Any other unique identifying numbers, characteristics or codes

In order to de-identify PHI, please follow the requirements in Policy 0P30.

Employee Personally Identifiable Information (PII) is a group of personal data points. When data points are combined, personal identity theft or forgery is possible. The University safeguards PII of all University employees and defines PII as the following:

- SSN
- Bank account information
- Credit or debit card information
- Home address
- Home telephone number
- Personal email address
- Internet identification name or password
- Parent's surname prior to marriage
- Driver's license number or non-driver identification number

Payment Card Information is the 16-digit number on a credit or debit card, the security code, an individual's PIN, the expiration date of the card and the individual card holder's name. This information must comply with the the Credit Card Policy https://www.rochester.edu/adminfinance/treasury/docs/PolicyCreditCard.pdf.

FERPA (Federal Education Rights and Privacy Act of 1974) is federal legislation that protects the privacy of students' records.

FERPA Education Records are any records that are directly related to a student and maintained by the Universitiy. For more information see the University's FERPA Policy https://www.rochester.edu/bulletin/policies/ferpa/.

Student Directory Information: The University considers the following to be student directory information: name, campus address, email address, major, University phone number, dates of attendance, participation in activities and sports, height and weight of athtletic team members, degrees and awards received, date of birth, most recent insitution attended, enrolment status, photographs, previous educational agencies or institutions attended, and other similar information . It cannot include race, gender, SSN, grades, GPA, country of citizenship, or religion.

Employee Directory Information: The University considers the following to be employee directory information: name, office address, University email address, University phone number, job title, and department. It cannot include any data points defined in Employee PII.

Personnel Records is any information that holds records related to employment at the University. These can include:

- Hire and appointment letters
- Salary information
- Performance reviews
- Warnings and disciplinary documents
- Attendance records
- Background investigations
- Immunizations

APPENDIX A: This appendix provides examples of how common types of information may be classified based on the classification of data contained within the information source.

Legally Restricted	Confidential	Internal	Public
• Human subjects records • Grant documents with regulated data • Employee tax forms • I-9 forms • Records of payroll deductions • Financial aid records (SSN) • Medical records	• Invention disclosures • Grant documents without regulated data • Licensing agreements • Employment contracts • Appointment letters • Individual salary and benefits • Salary records & performance appraisals • Financial aid records (excluding SSN) • Student loan records • Student applications, transcripts, grades • Construction drawings for nonpublic or confidential areas	• Financial statements - unaudited • Purchase orders • Budgets (excluding individual salaries/benefits) • Travel reimbursements • Organizational charts with names • Search committee records • Tenure/promotion cases • Affirmative action plans • Environmental monitoring records • Real estate materials • Construction drawings for public/non-confidential spaces. • Alumni data • Gift records	• Faculty, staff, student directory • Press releases • Charter and By-Laws • Organizational charts without names • Job descriptions • Athletic schedules • Course schedules • Commencement programs • Public websites and social media