# WPI Data Classification and Usage Policy

## 1.0 Purpose

The purpose of this Policy is to establish a framework for classifying institutional data based on its level of sensitivity, value and criticality to the University. Classification of data will aid in determining baseline security controls and legal requirements for the protection of data.

## 2.0 Applicability

This Policy applies to all faculty, staff and third-party Agents of the University as well as any other University affiliate who is authorized to access Institutional Data.

## 3.0 Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of four sensitivity levels, or classifications: 1) Restricted Use; 2) Confidential; 3) Internal Use Only; 4) Unrestricted

## 4.0 Definitions

**Restricted Use:** Data should be classified as Restricted Use when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. Examples of Restricted Use data include data protected by state or federal regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted Use data. Restricted Use data includes:

a. Social Security Number;
b. Driver's License Number or state-issued identification card number, including passports;
c. Financial account number (bank, investment, 403B), or credit or debit card number;
d. Health care information protected under HIPAA, including patient billing or medical records, information about physical or psychological state of health, counseling records,

disease, medical history, medical treatment, drugs, therapies, genetic test results, family health or morbidity history;

e. Biometric data including fingerprints, voiceprints, retina image, iris image, or other unique physical representation, with the exception of the fingerprints associated with individual fingerprint readers used for securing laptop or desktop computers.

f. Export Controlled Materials including materials defined as any information subject to United States export control regulations including, but not limited to, the Export Administration Regulations (EAR) published by the U.S. Department of Commerce and the International Traffic in Arms Regulations (ITAR) published by the U.S. Department of State.

g. Controlled Technical Information (CTI): "technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination" per DFARS 252.204-7012.

**Rules for Usage of Restricted Use Data**

a. Restricted Use data shall be stored in institutionally supported applications residing in the WPI Data Center or a contracted cloud service, but not in Word, Excel or Access (with the exception of information required for critical business purposes and stored in an approved, encrypted area). Restricted Use data can also reside in approved third party hosted applications, but those applications must be approved by the CIO. Hard copy data shall be stored in locked receptacles and rooms. Access to this electronic data shall only be gained through authenticated access on the WPI network or approved VPN access, and only to those authorized to access the data. Hard copy data shall only be accessed when business requires such use and all storage receptacles and rooms shall be appropriately designed to allow for authorized access only.

b. Employees shall not store or copy this data to laptop or desktop computers (whether institutionally-owned or personally owned), smart phones, USB devices or other portable or cloud based media (e.g. OneDrive, Dropbox). In addition, this data shall not be transmitted via e-mail, instant message, chat or other social media technologies, with the exception of approved third party vendors with appropriate encryption in place. If data is transmitted on a recurring basis to external vendors, it shall be sent via a secure transmission, such as secure FTP (SFTP).

c. When stored in the cloud, Restricted Use data will require multi-factor authentication. Employees with access to Restricted Use data in the cloud will also be required to install software that can monitor the activity on Restricted Use data in motion or at rest.

d. Electronic and hard copy data shall be destroyed in accordance with WPI's Data Retention and Destruction Policy, and shall be rendered unreadable in paper or electronic form. All departments shall have policies in place and periodically review electronic storage areas and their hard copy storage areas to insure that data is being destroyed in a timely and effective manner.

**Confidential:** This includes data protected by state or federal law, contractual agreements and proprietary information against unauthorized use, disclosure, modification and destruction. Confidential data includes the following:

a. Student records, including date of birth, place of birth, mother's maiden name, official grades recorded on a student's permanent record, academic information, race, judicial information and other information relative to a student's permanent record (i.e. official grades, judicial records, etc.).
b. Human Resources data including employment records, salary, benefits, personnel evaluations, date of birth, place of birth, mother's maiden name, race and other records pertaining to personnel files (i.e. payroll reports, yearly merit increase data, etc.).
c. Academic Affairs information relating to non-public research and promotion and tenure files (i.e. notes relating to tenure decisions).
d. Alumni or donor information, including date of birth, place of birth, mother's maiden name, donation amount and assets (i.e. Daily Giving Reports, Donor Profiles, etc.).
e. Corporate records including Board of Trustee minutes, Board of Trustee votes and other confidential information dispersed at Board meetings and/or shared with Board members.
f. Sensitive Personal Information including credit checks, criminal background checks, visa numbers, sexual behaviors and criminal convictions (i.e. CORI/SORI reports).
g. Information security data, including administrator passwords used by Information Technology staff and other data associated with security-related incidents occurring at WPI.
h. Research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq).

**Rules for Usage of Confidential Data**

Confidential data shall be stored in institutionally supported applications located in WPIcontracted Cloud services, WPI's Data Center, institutionally supported shared drives, or approved third party hosted applications. Confidential data can be stored on Institute-owned laptop or desktop computers, but **shall not be** copied to non-WPI computers, USB devices or other portable media. Hard copy data shall be maintained in as few receptacles and rooms as business dictates. Copies of this data shall not generally be made unless business requires it.

To this end, employees are permitted to store data on institutionally-owned laptop or desktop computers and shared drives; however, the dissemination of this data shall be done securely. Data shall not be transferred via e-mail unless encrypted. If data is transmitted on a recurring basis to external vendors, it is preferable to send this data through secure transmissions such as secure FTP (SFTP).

Electronic data shall be destroyed in accordance with WPI's Data Retention and Destruction Policy, and shall be rendered unreadable in paper or electronic form. All departments shall have policies in place and periodically review electronic storage areas and their hard copy storage areas to insure that data is being destroyed in a timely and effective manner.

**Internal Use Only:** This includes information that requires protection from unauthorized use, disclosure, modification, or destruction, but is not subject to any of the items listed in the Restricted Use or Confidential definitions above. Internal Use Only data includes: a. Student ID

b. Data related to WPI operations, finances, legal matters, audits, or other activities that are not public in nature, but not classified as Restricted Use or Confidential.
c. Faculty grade worksheets (i.e. Excel files used to track student grading prior to submitting to the Registrar's Office).
d. Personal white page, business white page or professional employment information for students, alumni or donors. This includes name, business name, business address, home address, e-mail, cell phone numbers, business phone numbers, home phone numbers, occupations and titles, but not classified as Restricted Use or Confidential.
e. Personal white page information for faculty and staff. This includes home address, cell phone, home phone, home fax and personal e-mail, but not classified as Restricted Use or Confidential.

f. Personal characteristics such as gender, height, weight, marital status, nationality, personal interests, photographs and names of children and other demographic information that is not classified as Restricted Use or Confidential.
g. Internal WPI data, the distribution of which is limited by intention of the author, owner, or administrator, but not classified as Restricted Use or Confidential.

**Rules for Usage of Internal Use Data**

Internal Use data can be stored in institutionally supported applications located in a WPIcontracted Cloud service, the WPI Data Center, institutionally supported shared drives, third party hosted applications and laptop or desktop computers (both WPI issued and personally owned). This data can be copied to smartphones, USB devices or other portable media. Hard copy data shall be maintained in as few receptacles and rooms as business dictates. Copies of this data shall not generally be made unless business requires it.

To this end, employees are permitted to transmit this data via unencrypted e-mail. Electronic data can be destroyed using traditional application delete functionality. Hard copy information can be destroyed in accordance with an employee's personal or departmental policy.

**Unrestricted:** This includes data that can be disclosed to any individual or entity inside or outside of WPI. Security measures may or may not be needed to control the dissemination of this type of data. Unrestricted data includes:

a. Content and images on WPI's public web sites (i.e. www.WPI.edu).
b. Publically released press statements
c. Course catalogue
d. Business White Page information for faculty and staff, unless otherwise restricted. This includes name, title, department, office location, office phone and WPI e-mail.
e. Published financial statements

**Rules for Usage of Unrestricted Data**

All information, whether in paper or electronic form, can reside in the public domain and is available to all students, faculty and staff; but, it is subject to WPI's Acceptable Usage Policy and federal copyright laws.

## 4.0 Policy Enforcement

Any person that violates any of the policies found in this policy will be subject to the same disciplinary actions as outlined in WPI's Confidentiality Agreement.

## 5.0 Approval and Revisions

**Policy Category**: Institutional Risk & Compliance

**Policy Approved By:** Approved by WPI's Information Security, Risk and Compliance Committee on 7/9/18.

**Policy Reviewed Annually By**: John Schwartz – Chief Information Security Officer (CISO)

**Related University Policies**: None

**Last Modified**: 10/30/19