WPI Data Classification and Data 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. For the purposes of this policy, definitions of 'research data' and 'intellectual property' are excluded as they are covered by separate policies. References to these policies can be found here:

Intellectual Property Policy

Research Policies

An employee's own personal information (such as information relating to pay, benefits, or employment status), when accessed by the employee as the data subject, is not subject to this Policy. Employees are authorized to access and use their personal data in whatever manner they see fit

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 five sensitivity levels, or classifications: 1) CUI; 2) Restricted; 3) Restricted-Specific; 4) Private; 5) Public

4.0 Definitions

CUI: Controlled Unclassified Information (CUI) Data should be classified as CUI when it is created, received, maintained, or transmitted on behalf of the Federal Government and requires safeguarding or dissemination controls in accordance with federal law, regulation, or government-wide policy (e.g., the CUI Registry, DFARS 252.204-7012, or NIST SP 800-171). CUI is defined as unclassified information that requires protection under federal requirements and must be handled, marked, and safeguarded in accordance with those requirements. The highest level of security controls shall be applied in alignment with applicable federal standards. CUI designation is determined by federal requirements and is not based solely on institutional risk classification. Not all federally regulated data is classified as CUI; classification is determined based on explicit federal designation or contractual requirement.

CUI data includes:

- Export-controlled research data (ITAR/EAR) - 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.
- Sensitive research data that includes DFARS 252.204-7012 and/or requires NIST 800-171 compliance.
- Controlled Technical Information (CTI): "technical information with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination" per DFARS 252.204-7012.
- Data identified in the CUI Registry such as Legal files and agreements, Energy related information, Department of Defense (DoE) information.
- Federal Tax Information (FTI) is associated with student financial aid, tax returns, and other federal taxpayer information.

Rules for Usage of CUI Data

a. CUI shall only be stored in approved environments that meet NIST SP 800-171 requirements, including institutionally approved secure research enclaves or cloud services that meet equivalent federal security standards (e.g., FedRAMP Moderate or higher), as applicable to the type of CUI.
b. Hard copy data shall be stored in locked receptacles and locked rooms. 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.

c. Access to CUI electronic data shall be limited to authorized users and performed through approved, authenticated access methods within defined security boundaries.
d. Access to CUI systems shall require uniquely assigned credentials and multi-factor authentication. Credentials must be kept confidential and managed in accordance with institutional identity and access management standards.
e. CUI shall only be stored or accessed on institutionally managed and approved systems within authorized security boundaries. Storage on endpoints or portable devices is prohibited unless explicitly authorized, managed, encrypted, and compliant with CUI security requirements.
f. CUI data shall only be transmitted using secure, encrypted transmission methods within approved systems or to authorized third parties in accordance with contractual and regulatory requirements. CUI data must be encrypted in transit and at rest.
g. Data shared with third parties requires a vetted contract, a security and data sharing agreement, and ongoing compliance and monitoring with applicable regulatory and institutional requirements.
h. CUI data is prohibited from being used with AI tools unless approved by the Chief Information Security Officer (CISO).
i. CUI data shall be retained and destroyed in accordance with institutional data retention and destruction policies and applicable federal requirements.
j. Access to and use of CUI data shall be logged and monitored in accordance with institutional logging and monitoring standards.
k. CUI data must reside within defined and approved security boundaries where access, processing, and storage are controlled and monitored in accordance with applicable federal requirements.

Restricted: Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the University or its affiliates, including reputational, financial, or security harm, and where no additional regulatory, contractual, or sponsor-imposed requirements dictate specific handling controls beyond institutional standards. Examples of Restricted data include proprietary information, data subject to contractual obligations, and security camera or surveillance footage. Where data meets criteria for multiple classifications, the classification with the most restrictive applicable requirements shall apply.

Restricted data includes the following:

- Social Security Number(s).
- Personally Identifiable Information (PII).
- Visa Number(s).
- Driver's license or state ID.
- Financial account number (bank, investment, 403B).
- Biometric data including fingerprints, voiceprints, retina image, iris image, or other unique physical representation, except for the fingerprints associated with individual fingerprint readers used for securing laptop or desktop computers.
- 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.), including data associated with the Family Education Rights and Privacy Act (FERPA)
- 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.).
- Academic Affairs information relating to non-public research and promotion and tenure files (i.e. notes relating to tenure decisions).
- Corporate records that include Board of Trustee minutes, Board of Trustee votes and other confidential information dispersed at Board meetings and/or shared with Board members.
- Information security data, including administrator passwords used by Information Technology staff and other data e.g., system, access and audit logs as required by federal, state and other regulations or related with security related incidents occurring at WPI.
- 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 Restricted Data

a. Restricted data shall be stored in institutionally supported applications residing in the WPI data center or an approved cloud provider such as Microsoft M365. Restricted data can also reside in approved third party hosted applications as approved by the Chief Information Security Officer (CISO) and/or Chief Information Officer (CIO).
b. Hard copy data shall be stored in locked receptacles and locked rooms. 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.

c. Access to Restricted data shall be limited to authorized users and performed through approved, authenticated access methods within defined security boundaries. Login credentials (including username, password, and multi-factor authentication information) must be used on these systems and be kept confidential. Users should not reuse their WPI passwords with non-WPI sites or services to avoid risks to WPI if those non-WPI sites are breached.
d. Restricted data shall only be stored or accessed on institutionally managed and approved systems within authorized security boundaries. Storage on endpoints or portable devices is permitted only when those devices are secured, encrypted, and used in accordance with institutional security requirements and approved services.
e. Restricted data shall only be transmitted using secure, encrypted transmission methods within approved systems or to authorized recipients in accordance with institutional requirements. When stored in the cloud, Restricted data will require multi-factor authentication.
f. Restricted data must be encrypted in transit and at rest.
g. Data shared with third parties requires a vetted contract, security and data sharing agreement in accordance with regulatory requirements.
h. Restricted data is prohibited from being used with unauthorized AI tools. ITS maintains a publicly-available list of authorized AI tools. To request the use of an AI tool not on this list, contact ITS for approval.
i. 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 ensure that data is being destroyed in a timely and effective manner.

Restricted-Specific: Data should be classified as Restricted-Specific when it meets the criteria for Restricted data and is also subject to specific protection, handling, or processing requirements defined by law, regulation, contractual terms, sponsor requirements, or data use agreements that impose controls beyond institutional standards. This includes, but is not limited to, data governed by regulatory frameworks such as HIPAA, GLBA, PCI-DSS, and Criminal Justice Information (CJIS). Where data meets criteria for multiple classifications, the classification with the most restrictive applicable requirements shall apply.

Restricted-Specific data includes:

- Health care data protected under the Health Insurance Portability and Accountability Act (HIPAA), including patient billing or medical records, information about physical or psychological state of health, counseling record, disease, medical history, medical treatment, drugs, therapies, genetic test results, family health, or morbidity history. 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.).
- Credit / Debit Card information to meet PCI-DSS.
- Financial and/or financial aid data as related to Gramm Leach Bliley Act (GLBA).

Rules for Usage of Restricted-Specific Data

a. Restricted-Specific data shall only be stored in approved environments that meet applicable regulatory, contractual, or sponsor-imposed security requirements, as determined by the type of data and associated obligations.
b. Hard copy data shall be stored in locked receptacles and locked rooms. 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.
c. Access to Restricted-Specific data shall be limited to authorized users and performed through approved, authenticated access methods within defined security boundaries.
d. Login credentials (including username, password, and multi-factor authentication information) must be used on these systems and be kept confidential. Users should not reuse their WPI passwords with non-WPI sites or services to avoid risks to WPI if those non-WPI sites are breached. Where multi-factor authentication is not explicitly required by applicable regulatory or contractual obligations, its use is strongly recommended in accordance with institutional identity and access management standards.
e. Restricted-Specific data shall only be stored or accessed on institutionally managed and approved systems within authorized security boundaries. Storage on endpoints or portable devices is prohibited unless explicitly authorized, managed, encrypted, and compliant with applicable regulatory and institutional requirements.
f. Restricted-Specific data shall only be transmitted using secure, encrypted transmission methods in accordance with applicable regulatory, contractual, or sponsor requirements. Data must be encrypted in transit and at rest where required by those obligations.
g. Data shared with third parties requires a vetted contract, a security and data sharing agreement, and ongoing compliance and monitoring in accordance with applicable regulatory and institutional requirements.

h. Restricted-Specific data may be used with AI tools only when formally approved through the institutional AI governance process and aligned with applicable regulatory and contractual requirements. To request approval for the use of AI tools not explicitly authorized by the institution, users must follow the ITS-defined approval process.
i. Restricted-Specific data shall be retained and destroyed in accordance with institutional data retention policies and any applicable regulatory, contractual, or sponsor-imposed requirements.
j. Access to and use of Restricted-Specific data shall be logged and monitored in accordance with institutional logging and monitoring standards and any applicable regulatory requirements.
k. Restricted-Specific data must reside within defined and approved security boundaries where access, processing, and storage are controlled and monitored in accordance with applicable regulatory, contractual, or sponsor-imposed requirements.

Private: Data should be classified as Private when the unauthorized disclosure, alteration and/or destruction of that data could result in a moderate risk to the University or its affiliates including reputational, financial or security harm. By default, all institutional data that is not explicitly classified as CUI, Restricted, Restricted-Specific or Public should be treated as private.

Private Data Includes:

- Student ID Number.
- Data related to WPI operations, audits, legal matters, or other activities that are not public in nature.
- Faculty grade worksheets (i.e. Excel files used to track students' grading prior to submitting to the Registrar's Office).
- Personal white page, business white page or professional employment information for students, alumni or donors. This includes name, business name, business address, home address, email address, cell phone numbers, business phone numbers, home phone numbers, occupations, titles.
- Personal white page information for faculty and staff. This includes home address, cell phone number, home phone number, home fax number, personal email address.
- Personal characteristics such as gender, height, weight, marital status, nationality, personal interests, photographs and names of children or other demographic information.
- Internal WPI data, the distribution of which is limited by intention of the author, owner, or administrator.

Rules for Usage of Private Data

a. Private data can be stored on institutionally supported applications residing in the WPI data center, or on an approved Cloud provider such as Microsoft 365 institutionally supported shared drives, third party hosted applications, WPI authorized devices, and personal devices. This data can be copied to smartphones, USB devices or other portable media.
b. Only authorized users may access Private data.
c. Login credentials (including username, password, and multi-factor authentication information) must be used on these systems and be kept confidential. Users should not reuse their WPI passwords with non-WPI sites or services to avoid risks to WPI if those non-WPI sites are breached.
d. When stored in the cloud Private data will require multi-factor authentication.
e. Users are permitted to transmit this data via unencrypted e-mail. It is strongly recommended that Private data be encrypted in transit, Private data must be encrypted at rest.
f. Data shared with third parties requires a vetted contract, security and data sharing agreement in accordance with regulatory requirements.
g. AI tools may be used with Private data only when institutionally approved. ITS maintains a publicly-available list of authorized AI tools. To request the use of an AI tool not on this list, contact ITS for approval.
h. 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 ensure that data is being destroyed in a timely and effective manner.
i. The use of Private data must not violate any University policy or any applicable laws and regulations.

Public: Data should be classified as Public when the unauthorized disclosure, alteration, and/or destruction would result in little or no risk to the University and its affiliates. 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. While little or no controls are required to protect the confidentiality of Public data, some control is required to prevent unauthorized modification and/or destruction of Public data.

Public data includes:

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

Rules for Usage of Public Data

a. All Public data, whether in paper or electronic form, can reside in the public domain and is available to all students, faculty and staff; but is subject to WPI's Acceptable Usage Policy and federal copyright laws. Only authorized users may change Public data.
b. Access to Public data does not require login credentials.
c. Public data does not require encryption in transit or at rest.
d. Use of generally available AI tools is acceptable.

5.0 Policy Enforcement

Any person(s) 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. To view the Confidentiality Agreement or any other WPI Policies, they can be found on the WPI.edu website at, Policies | Worcester Polytechnic Institute (wpi.edu).

6.0 Policy Review

This policy should be reviewed annually by WPI Information Technology Services (ITS) and the Information Security Office.

Questions: For immediate reporting of a possible information security incident, contact the WPI ITS Helpdesk at its@wpi.edu and for information security questions please contact infosec@wpi.edu.

Policy Sponsor: WPI Chief Information Officer (CIO) and WPI Chief Information Security & Technology Officer (CISTO)

Responsible Department: WPI Information Technology Services (ITS)

Effective Date (i.e., date of Presidential Approval): May 19, 2026

Revision Date: May 12, 2026

Appendix

Minimum Protection Requirements	Restricted Restricted (CUI, Restricted-Specific, Restricted)	Private Private	Public Public
Examples	**SSN, Finance, HIPAA, FERPA, FCI**	**WPI ID number, addresses, demographic data**	**wpi.edu content, course catalogue, white page information**
Use of this data must not violate University policy or any applicable laws and regulations.	Required	Private Required	Public Required
Only authorized users may access data	Restricted Required	Private Required	Public Not Required
Only authorized users may change the data.	Restricted Required	Private Required	Public Required
Login credentials (username/password) are required, unique, and kept confidential.	Restricted Required	Private Required	Public Not Required
Two-factor authentication	Restricted Required	Private Required	Public Not Required
Data must be encrypted during transmission. Unencrypted transmission is prohibited.	Restricted Required	Private Encryption is strongly recommended; unencrypted transmission is permitted where appropriate.	Public Not Required
Encrypt data at rest.	Restricted Required	Private Required	Public Not Required
Only store data on institutionally managed and approved systems and in approved secure locations*	Restricted Required	Private Strongly Recommended	Public Not Required
Data sharing with vendors and 3rd-parties requires a vetted contract and a security review.	Restricted Required	Private Required	Public Not Required
Store printed materials securely.	Restricted Required	Private Required	Public Not Required
Destroy data according to University policies and procedures.	Restricted Required	Private Required	Public Not Required
Make data available to the public.	Restricted Prohibited	Private Prohibited	Public Acceptable
AI Tool Use	Restricted Allowed only when formally approved through the institutional AI governance process and aligned with applicable regulatory, contractual, and institutional requirements	Private Allowed only with institutionally approved AI tools and in accordance with institutional AI governance requirements	Public Acceptable

***Authorized locations include WPI M365 - Email, OneDrive, SharePoint, Teams, WPI provided laptops, WPI's Azure environment, WPI's AWS Redshift environment* or other ITS-approved environments.**