Stewardship of Information Policy

Effective Date	Responsible Officer	Responsible Office	This Policy Applies to:
07/01/2020	General Counsel	Compliance and Risk Management	All Institute departments and all faculty, staff, contractors, student employees, and anyone with access to institutional information.

1. POLICY STATEMENT

All information owned, managed, or in the custody of WIT ("information") shall be consistently and appropriately protected from its time of origin or receipt until the time of its destruction according to its classification. Information is classified into three categories, based on its sensitivity, criticality, and applicable regulations and statutes: **Restricted**, **Private**, and **Public**.

Individuals with access to institutional information are obligated to know the classification of information they access and create and to follow the corresponding standard for protecting, handling, disseminating, and destroying information as required and specified by this policy and related WIT procedures and standards.

2. DEFINITIONS

Data Classifications	
Data Classification	Description
Restricted	Data should be classified as Restricted when: 1) unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates 2) protected by state or federal privacy regulations, or 3) protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data. Examples: *Personally identifiable information (PII)[1] as defined by any state, federal, or other applicable privacy law. Non-personally identifiable information covered by FERPA (such as application/admissions information, grades, transcripts, disciplinary actions, financial application/award information, directory information that a student has elected to not have disclosed); non-personally identifiable information covered by GLBA (such as financial transaction information); employment information (such as salary, benefits, and performance evaluations); and sensitive non-personally identifiable information regarding applicants, alumni, donors, parents, or business associates of the Institute; information that is subject to a confidentiality agreement; sensitive infrastructure data; legally privileged information, trade secrets and intellectual property; details about WIT's security (cyber or physical) controls, plans, or vulnerabilities.*
Private	Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data. Examples: *Course materials, internal-use only policies and procedures, research and assessment data, inventory data (library, technical, infrastructure entities), marketing plans, meeting minutes or agendas with potentially non-public information, non-public strategic plan information, departmental budgets, and unpublished writing or research.*
Public	Data should be 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

[1] Broadly, PII is the combination of the full personal name of an individual plus one or more other elements of uniquely identifying information, such as, but not limited to, date of birth, home address, student or employee ID number, financial account number, bank account number, credit card number, social security number, credit history, CORI record, medical record number, personal email address, or driver's license number. Privacy laws may differ in what is in scope for PII. The Mass. Privacy Law (MGL c. 93H and 201 CMR) defines PII as a Massachusetts resident's full personal name plus one or more of the following: SSN, financial account number, driver's license number.

	affiliates. While enhanced controls are not required, careful forethought should be given to the release of data deemed Public. Examples: *Campus maps and directory information, IPEDS, Common Data Set, Institute of International Education, Open Doors, promotional material, redacted departmental meeting minutes, program and course descriptions, student/campus activities, athletics information, hosted conference information, event schedules, public-facing Internet content, approved press releases, publication-oriented personnel biographies and photos, publication archives, and published materials.*
Risk Classifications	
Low Risk	Data is classified as **Low Risk** if either of the following conditions apply: 1. The data is generally available to the public, or 2. The unauthorized use, access, or alteration of the data would not have an adverse impact on Institute or an individual community member.
Moderate Risk	Data is classified as **Moderate Risk** if any of the following conditions apply: 1. The data is governed by laws or regulations that restrict the use or disclosure of such data, or 2. The data is subject to contractual restrictions that restrict the use or disclosure of such data, or 3. The unauthorized use, access, or alteration of the data could have an adverse impact on Institute or an individual community member.
High Risk	Data is classified as **High Risk** if either of the following conditions apply: 1. The data is governed by laws or regulations that require Institute to report to the government and/or provide notice to individuals if the data is breached, or

	2. The unauthorized use, access, or alteration of the data could have a significant adverse impact on Institute or an individual community member.
Roles and Responsibilities	
Data Trustee	Vice Presidents who have overall responsibility for all the data sets maintained by units reporting to them. Data Trustees are responsible for ensuring that campus institutional data resources are used in ways consistent with the mission of the Institute. The Data Trustees have the responsibility for the appointment and accountability of Data Owners. Data Trustees are also responsible for ensuring that institutional data and information systems used with such data are adequate to meet the business and regulatory compliance requirements[1] set for these data.
Data Steward	Generally, those authorized, by Data Trustees and/or Data Owners, with operational responsibilities over the systems that are used to collect, access, store, transmit, and destroy data. Data Stewards are responsible for effectuate the policies, procedures, and guidelines concerning the accuracy, privacy, security, and integrity of the data subsets for which they are responsible. Data Stewards are also responsible for enacting and maintaining the technical, administrative, and physical controls used to ensure the confidentiality, integrity, and availability of data. In addition, Data Stewards may be responsible for providing the mechanism(s) to also ensure the resiliency of the data and information systems used with these data. Requirements, including policies and standards, are set by Data Trustees and Data Owners. Data Stewards ensure that mechanisms and functions are in place to enable and enforce those requirements. Examples of Data Stewards could include coordinators, managers, assistant/associate directors, database and application administrators, etc. who meet the above definition.
Data User	Employees, independent contractors, or students (e.g., interns, work study, co-op) who have been granted authorization by a Data Steward to access institutional data. Authorization is granted for a specific level of access to a specific set of data, as defined by the data management policies, solely for the conduct of institutional business. Data Users are responsible for adhering to all policies, standards, and best practices as established by Data Trustees and Data Owners.
Terminology	
Personally Identifiable Information (PII)	PII is the combination of the full name (first and last) of an individual person plus one or more other elements of uniquely identifying information, such as, but not limited to, date of birth, home address, student or employee ID number, financial account number, bank account number, credit card number, social security number (SSN), credit history, CORI record, medical record number, personal email address, and driver's license number. Various domestic and foreign laws stipulate special handling and protection of various PII, particularly SSNs, financial account numbers, driver's license number, and date of birth.

3. APPENDIX: STANDARDS FOR HANDLING INSTITUTIONAL INFORMATION

Rule #	Rule Statement	Applicable Role	Digital	Paper
3.1	Always Transmit Restricted Information Securely	All employees	Restricted information must be transmitted using industry-standard encryption protocols, such as HTTPS or SSL[2]	Require a recipient signature and use a trusted shipper or courier who provides tracking numbers.
3.2	Always Destroy Private and Restricted Information Using an Approved Method.	IT Administrators	Storage devices that may have contained Restricted or Private at any time must be sanitized using a method approved by the ISO[3] before disposal, reassignment, or re-use.	[redacted]
		All employees	[redacted]	Shred paper documents containing Restricted or Private information using a crosscut shredder[3]. If shredding cannot be done immediately, store the document in a locked drawer, cabinet, or container within a locked office when unattended until it can be shredded.
3.3	Never Disclose Private or Restricted Information to Unauthorized Parties	All employees	Restricted and Private information must only be disclosed to individuals who have previously been approved to see that information and have a valid business justification for any particular instance. Records, files, documents, or databases unnecessarily containing Restricted or Private must have the personally identifiable elements de-identified before being disseminated or shared.	
3.4	Never Leave Private or Restricted Information Openly Accessible and Unattended	All employees	If viewing Private or Restricted information on a computer screen, lock the screen before leaving. Consider using a privacy screen if regularly viewing Restricted or Private.	Observe the 'Clean Desk' security principle and never leave documents with Private or Restricted information unattended in unsecured areas (e.g. shared printers, workstations in open spaces, meeting rooms, etc.); store documents in a locked drawer, cabinet, or container within a locked office.
3.5	Never Retain Restricted or Private Information Longer than Required	All employees	Delete files containing Restricted or Private using a secure file deletion method as soon as the information is no longer needed.	Securely shred all paper documents containing Restricted or Private using a cross-cut shredder once the document is no longer needed.[3]
3.6	Never Store or Capture more Restricted or Private Information than Required	All employees	When receiving Restricted or Private, only record the minimal information needed to perform the business function. For example, for credit card transactions, do not store the	

[2] Consult the ISO if you are unsure about the security of the electronic transfer method you intend to use.
[3] Sanitization methods, including disk wiping tools and document shredders, must meet or exceed the standard specified in NIST SP 800-88.

Rule #	Rule Statement	Applicable Role	Digital	Paper
			full contents of any track, the card verification code or value, personal identification number (PIN) or the encrypted PIN block after authorization. If Restricted or Private within the data set or document is not required, then de-identify the personally identifiable elements.	
3.7	Never Display more Restricted or Private Information than Required:	All employees	When designing screens, dashboards, or reports which show Restricted or Private, only display the minimum amount of information necessary to accomplish the business purpose. For example, if a credit card or SSN must be shown, only reveal the last four digits.	
3.8	Never Create Unsecured Copies of Restricted or Private Information.	All employees	Only copy a file containing Restricted or Private to an approved and encrypted storage location.	Never write down or print Restricted or Private in a document that could be easily seen by an unauthorized party, such as writing it down in a shared notebook or on a sticky note.
3.9	Always Retain Information According to Legal Requirements	Administrators	Be informed about how information in your stewardship is classified and your responsibilities for retaining under applicable Federal, State, and other laws and regulations.	
3.10	Always Grant Access to Private and Restricted Information on a Need-to-know Basis	Administrators	Before granting any type of access to Private or Restricted information, establish that the employee has a valid business justification for that access.	

4. RELATED DOCUMENTS

Document Name	Publisher[4]
Information Technology Resource Acceptable Use Policy	WIT

5. ENFORCEMENT OF POLICY VIOLATIONS

Failure to comply with this policy, intentionally or unintentionally, may result in one or more of the following:

- Termination, without notice, of access privileges to information and technology resources.
- Disciplinary action, up to and/or termination of employment.
- Civil or criminal penalties as provided by law.

6. REVIEW AND REVISION HISTORY

Policies must be reviewed annually by the policy owner. If a policy has been revised, then it must have all necessary approvals before being published. In the last column, indicate whether the activity was a review or a revision; if a revision, summarize the changes.

Date	Name and Title	Annual Review or Revision Summary

[4] For documents originating within WIT, such as policies or procedures, specify "WIT". For other relevant third-party documents, such as external standards to which WIT subscribes, list the name of the organization that publishes the document.