Data Classification Policy

Purpose/Statement
A data classification policy is necessary to provide a framework for securing data from risks including, but not limited to, unauthorized destruction, modification, disclosure, access, use, and removal. This policy outlines measures and responsibilities required for securing data resources. It shall be carried out in conformity with state and federal law.

Reason for the Policy
Olin must maintain and protect its institutional assets and comply with applicable state and federal regulations.

Entities Affected by this Policy
This policy applies to all centrally managed Olin enterprise-level administrative data and to all user-developed data sets and systems that may access these data, regardless of the environment where the data reside (including systems, servers, personal computers, laptops, portable/mobile devices, etc.). The policy applies regardless of the media on which data reside (including electronic, microfiche, printouts, CD, etc.) or the form they may take (text, graphics, video, voice, etc.).

Olin also expects all employees, partners, consultants and vendors to abide by Olin's information security policies. If non-public information is to be accessed or shared with these third parties, they should be bound by contract to abide by Olin's information security policies.

Who Should Read this Policy
All faculty, staff and student employees as well as third-party contractors should be aware of the policy.

Overview
Olin College takes seriously its commitment to respect and protect the privacy of its students, alumni, faculty, staff, parents and friends, as well as to protect the confidentiality of information important to the College's academic and research mission. The College recognizes that the value of its data resources lies in their appropriate and widespread use. It is not the purpose of this policy to create unnecessary restrictions to data access or use for those individuals who use the data in support of College business or academic pursuits.

Definitions

Data Ownership	Olin College is considered the data owner of all institutional data; individual units or departments may have stewardship responsibilities for portions of the data.
Data Administration	Responsibility for the activities of data administration is shared among the Data Managers, Data Custodians, The Information Security Officer and the Information Security Task Force.
Data Managers	College officials who have planning and policy-level responsibilities for data in their functional areas are considered Data Managers. The Data Managers, as a group, are responsible for recommending policies, establishing procedures and guidelines for college--wide data administration activities, and training of Data Users on the proper handling of data. Data Managers, as individuals, have operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data. Data managers are responsible for developing and applying standards for the management of institutional data, and for ensuring that Data Users are appropriately informed of

	security obligations associated with their data access. For historical reasons – because data and the responsibility for data have traditionally been organized along functional or subject-area boundaries – the Data Managers are established according to this same subject-area organizing principle. The ERP Steering group (a group of data managers) meets on a regular basis.
Data Custodian	Data Custodians are responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by Data Managers or their designees (usually the data managers), and implementing and administering controls over the information. In many cases at Olin the role of Data Custodian is a shared responsibility with the IT Department being responsible for physical security support (secure facility, backup and recovery) and the applicable Data Manager having responsibility for access and control over the information.
Data Users	Data Users have the ability to view, copy or download institutional data as part of their assigned duties or in fulfillment of their role within the Olin community. All Data Users are required to sign appropriate confidentiality statements. They also have an obligation to understand the security responsibilities associated with their level of data access. Data users are part of the larger ERP group and the IA ERP group, both of which meet on a regular basis.
Information Security Officer	College official who has oversight responsibility for the College's data security program as well as compliance with relevant regulations, security policies, standards and guidelines.
Protected Health Information	"Protected Health Information" or PHI is all individually identifiable information that relates to the health or health care of an individual and is protected under federal or state law.
Regulation Monitors	College officials who have oversight responsibility for one or more regulations. Regulation monitors stay abreast of updates to their respective regulations, ensure policies are up to date and notify the Information Security Officer and Data Managers about changes. The Compliance group meets on a regular basis.
Student Records	"Student Records" are those that are required to be maintained as non-public by the Family Educational Rights and Privacy Act (FERPA). Student Records include Olin-held student transcripts (official and unofficial), and Olin-held records related to (i) academic advising, (ii) health/disability, (iii) academic probation and/or suspension, (iv) conduct (including disciplinary actions), and (v) directory information maintained by the Registrar's Office and requested to be kept confidential by the student. Applications for student admission are not considered to be Student Records unless and until the student attends Olin College.
Qualified Machine	A "Qualified Machine" is a computing device located in a secure facility that is managed by IT or has access control protections that meet Olin's IT standards.
Computing Equipment	"Computing Equipment" is any Olin or non-Olin desktop, laptop, or portable device or system.

Procedures

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with data value, sensitivity, and risk. To implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data, data should be classified into one of the following categories:

1. Confidential - Data which is legally regulated and data that would provide access to confidential or restricted data.
2. Restricted - Data which the Data Managers have decided NOT to publish or make public and data protected by contractual obligations.
3. Public - Data which there is no expectation for privacy or confidentiality.

Confidential data and restricted data will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business or research functions of the College, result in financial loss, or violate law, policy or College contracts. Security measures for data are set by the Data Custodian, working in cooperation with the Information Security Officer, Information Technology Services and the respective Data Managers. The table below outlines the criteria used to determine which data classification is appropriate for a particular piece of data or information system.

	Confidential (highest, most sensitive)	**Restricted (moderate level of sensitivity)**	**Public (low level of sensitivity)**
Description	Data which is legally regulated; and data that would provide access to confidential or restricted data.	Data which the data managers have not decided to publish or make public; and data protected by contractual obligations.	Data for which there is no expectation for privacy or confidentiality.
Legal requirements	Protection of data is required by law.	Protection of data is at the discretion of the owner or custodian.	Protection of data is at the discretion of the owner or custodian
Reputation risk	High	Medium	Low
Data Access and Control	Legal, ethical, or other constraints prevent access without specific authorization. Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements.	May be accessed by Olin College employees and non-employees who have a business "need to know."	No access restrictions. Data is available for public access.
Transmission	Transmission of Confidential data through any non-Olin network or Olin guest network is prohibited (e.g. Internet). Transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is also prohibited.	Transmission of Restricted data through any non-Olin network or Olin guest network is strongly discouraged. Third party email services are not appropriate for transmitting Restricted data.	No encryption or other protection is required for public data; however, care should always be taken to use all College information appropriately.
Storage	Storage of Confidential data is prohibited on Non-qualified Machines and Computing Equipment unless approved by the Information Security Officer. If approved, IT approved encryption may be required.	Level of required protection of Restricted data is either pursuant to Olin policy or at the discretion of the owner or custodian of the information. If appropriate level of protection is not known, check with Information Security Officer before storing Restricted information unencrypted.	No encryption or other protection is required for public data; however, care should always be taken to use all College information appropriately.
Documented Backup and Recovery Procedures	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are not necessary, but strongly encouraged.	Documented Backup and Recovery Procedures are not necessary, but strongly encouraged.
Documented Data Retention Policy	Documented data retention policy is required.	Documented data retention policy is required.	Documented data retention policy is not required, but strongly encouraged.
Audit Controls	Data Managers and Data Custodians with responsibility for	Data Managers and Data Custodians with responsibility	No audit controls are required.

	Confidential data must actively monitor and review their systems and procedures for potential misuse and/or unauthorized access. They are also required to submit an annual report to the Information Security Officer outlining departmental security practices and training participation.	for Restricted data must periodically monitor and review their systems and procedures for potential misuse and/or unauthorized access.	
Examples	**Information resources with access to Confidential data (username and password).** **Student Data not included in directory information. This includes:** - Loan or scholarship information - Payment history - Student tuition bills - Student financial services information - Class lists or enrollment information - Transcripts; grade reports - Notes on class work - Disciplinary action - Athletics or department recruiting information **Personally Identifiable Information (PII):** Last name, and first name or initial, with any one of following: - Social Security Number - Driver's license - State ID card - Passport number - Financial account (checking, savings, brokerage, CD. . .), credit card, or debit card numbers - Date of birth **Protected Health Information (PHI) *** - Health Status - Healthcare treatment - Healthcare payment **Personal/Employee Data** - Worker's compensation or disability claims **Business/Financial Data** - Credit card numbers with/without expiration	**Personal/Employee Data** - Olin ID number - Income information * - Payroll information * - Personnel records, performance Reviews, benefit information - Race, ethnicity, and/or nationality - Gender **Business/Financial Data** - Financial transactions which do not include regulated/confidential data - Information covered by non-disclosure agreements - Contracts – that don't contain PII - Credit reports - Assets/Net Worth - Records on spending and borrowing **Academic / Research Information** - Library transactions (e.g., catalog, circulation, acquisitions) - Unpublished research or research detail / results that are not regulated/confidential data - Non-anonymous faculty course evaluations - Private funding information - Human subject information **Anonymous Donor Information** Last name, first name or initial (and/or name of organization	**Certain directory/contact information not designated by the owner as private**. - Name - Addresses (campus and home) - Email address - Listed telephone number(s) - Degrees, honors and awards - Most recent previous educational institution attended - Major field of study - Dates of current employment, position(s) - ID card photographs for institutional use Specific for students: - Class year - Participation in campus activities and sports - Weight and height (athletics) - Dates of attendance - Status **Business Data** - Campus maps - Job postings - List of publications (published research)

	dates - Bank or brokerage account numbers - Purchasing card (P-card) numbers - Social Security or other Taxpayer ID numbers - Loan information - Wire Transfer Information	if applicable) with any of the following: - Gift information, including amount and purpose of commitment **Other Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any of the following: - Telephone/fax numbers - E-Mail, URLs - Employment information - Family information (spouse(s)/partner/ guardian/children/ grandchildren, etc.) - Medical information **Management Data** - Detailed annual budget information - Conflict of Interest Disclosures - College's investment information **Systems/Log Data** - Server Event Logs * Exceptions apply	

Responsible Organization/Party

This policy will be re-evaluated on or about the first day of each calendar year to determine whether all aspects of the program are up to date and applicable in the current business environments, and revised as necessary. Operational responsibility of the program, including appropriate training of College staff, is delegated to the Information Security Officer.

Enforcement

The Information Security Officer will investigate suspected violations, and may recommend disciplinary action in accordance with Olin College's codes of conduct, policies, or applicable laws. Sanctions may include one or more of the following:

- Suspension or termination of access
- Disciplinary action up to and including termination of employment
- Student discipline in accordance with applicable College policy
- Civil or criminal penalties
- Or any combination of the above

Reporting Violations

Report suspected violations of this policy to the Information Security Officer, the appropriate Data Steward or the Responsible Organization/Party. Reports of violations are considered restricted information until otherwise classified.

Related Policies and Resources

- Appropriate Use of Olin's Information Technology system
- Olin's Information Security Plan
- Olin's Data Classification Policy
- FERPA Policy
- Olin's HIPAA Policy
- Olin's Red flags Policy
- Council for the Aid and Support of Education (CASE) for management and reporting standards (for gift-related information).