Siena College

Data Classification Policy

COLLEGE POLICY

Policy Title:	**Data Classification Policy**
Type or category of Policy:	**COLLEGE Policy**
Approval Authority:	**President**
Responsible Executive:	**Associate VP, Academic Affairs for Institutional Effectiveness, and/or Provost and Senior VP, and Chief Information Officer**
Responsible Office:	**Information Technology Services**
Owner Contact:	**Information Security Administrator** **informationsecurity@siena.edu**
Reviewed By:	**Data Management Task Force**
Reviewed Date:	**9/30/2020**
Last Revised and Effective Date of Revision:	**Last Revised: 9/30/2020** **Effective Date of Revision: 10/13/2020**

Brief Overview of the Policy

Siena College has a large store of data, tracking everything we do. In order to better control that data this policy describes classification “buckets” which define the level of control neededfor each individual datum. Those buckets, or classifications are: Public, Sensitive, Restricted.

Reason for Policy

This policy is needed in order to determine how restrictions are put in place to control access to data. For example, the names of departments is public data, while students' Social Security Numbers are confidential and must not be shared except when absolutely necessary.

Scope of the Policy: Entities or Individuals affected by this policy

This Policy applies to all employees who work directly with College data. It affects anyone who wants or needs access to Siena data. Specifically, the policy applies to any person who uses, stores, or transmits data either within or outside Siena.

The Policy does NOT apply to data whose copyright is owned by individual members of the College community as defined by the Copyright Policy which can be found at:

https://www.siena.edu/files/resources/copyright-ownership.pdf

The Policy controls electronic data and does not apply to data which exists only on paper.

The Official Policy

Siena College data is generated by or otherwise owned by the College. College data may exist in various forms, from paper to electronic, but this policy applies only to data stored electronically, either on the College's central servers, or on computing devices (including smartphones) whether institutionally or privately owned, or removable media such as USB sticks or external hard drives.

In order to properly secure College data, we must have a lexicon which describes the data and the level of protection needed to protect that data according to either internal needs or external regulation. This policy defines three classifications which can be applied to any College data. Those classifications are:

- Public
    - Data that is classified as Public does not need to be restricted and may be placed, for example, on the pages of our College website with no restrictions. Public data is information whose disclosure would not impair the functioning of the College. Such information has no College, contractual, or regulatory restrictions on access or usage.
- Sensitive
    - Data classified as Sensitive is data that must be protected due to ethical, privacy, or business process considerations. Sensitive data may also include data that is covered by contractual obligations which require us to keep that information within the bounds of the College, or which has been defined as sensitive by the Data Steward responsible. Sensitive data must be protected from unauthorized access, modification, transmission, or storage. This classification is applied by the responsible Data Steward for business reasons that may not be legal or contractual. Most administrative data will fall into this classification. Data stored in Banner or third party software systems that contain data is considered sensitive and will not be provided for classroom projects.

- Restricted
    - Restricted data is College information that must receive the most stringent controls. Such data is protected by law, external regulations, contractual obligations, or specific College policies. Data Stewards may also classify data as restricted according to business process needs in their area of responsibility.

Restricted data must only be disclosed to individuals and business partners within and outside the College on a strict need-to-know basis. Disclosure to parties outside the College must be expressly authorized by the appropriate Data Steward and be protected as appropriate by written contract and with appropriate security controls.

Classification Inheritance:

Data Assets, logical or physical containers that hold data, will be classified according to the most restrictive classification of data contained in the data asset. Similarly a data asset may receive aclassification that would be inherited by all data contained within that data asset.

Data Protection Guidelines

Public Data:

While there are no restrictions on access to public data, such data should be properly secured to prevent unauthorized modification, unintended use, or inadvertent/improper distribution. It should be understood that any information that is widely disseminated within the campus community is potentially available to the public at large.

The following guidelines are for information systems which are used to store and share Siena's public data.

- When practical, public data should only be shared via systems over which the College maintains full administrative control, which includes the ability to remove or modify the data in question.
- Information systems such as web servers or cloud services which are used to share public data must be properly secured to prevent the unauthorized modification of published public data. Data in the cloud must be protected by contract with that contract reviewed in advance by the Chief Information Officer (CIO).
- Interactive access to databases containing public data such as online directories or library catalogs should be properly secured using query rate limiting, CAPTCHA's or similar technology to impede bulk downloads of entire collections of data.

Sensitive Data:

Sensitive data requires protection because its unauthorized disclosure, alteration, or destruction could cause damage to the College or members of the College community. The requirements for handling Sensitive data are as follows.

In addition to the requirements outlined for Public data, Sensitive data must be:

- If stored in the cloud, then only on cloud-based information systems managed or contracted by the College. All contracts for cloud-based services must be reviewed by the CIO.
- Protected through the use of an authentication and authorization system which conforms

to the Password Management Policy such as the College's Active Directory Federation Services (ADFS) system to prevent unauthorized access, loss, theft, disclosure, or modification.

Restricted Data:

Restricted data requires the highest level of protection due to the risk and magnitude of loss or harm that could result from unauthorized disclosure, alteration, or destruction of the data. Certain types of Restricted data such as Social Security or credit card numbers may have additional requirements for protection.

In addition to the requirements outlined for Sensitive data, Restricted data must be:

- Protected with strong, Information Technology Services (ITS) approved encryption whether at rest or in transit.
- Wherever possible, Restricted data should remain in the College's core administrative systems and not propagated via files, documents or spreadsheets saved onto a personal use device such as a desktop or laptop computer, phone, USB stick, etc. unless authorized by the appropriate Data Steward.
- If Restricted data must be moved to a personal use device, it must be an institutionally owned and configured device, and must be deleted as soon as possible after the purpose for the move has been accomplished. Also see the Siena laptop and portable device security policy.
- Protected by multi-factor authentication whenever that is possible.
- Accessed from an institutionally owned and configured personal use device, even if that access is only to view the data.
- Credit card transaction data is a special case and must never be stored on an institutionally owned or controlled device, or transmitted across institutionally managed networks. For more information, contact ITS or the Comptroller's Office.

Exceptions

Exceptions to this policy must be approved in writing by the Data Steward(s) responsible for the affected data.

Resources

https://www.siena.edu/files/resources/copyright-ownership.pdf
https://www.siena.edu/files/resources/laptop-portable-elec-devices-security-policy.pdf
https://www.siena.edu/files/resources/password-policy.pdf

Adopted: 10/13/2020

Reviewed: 9/30/2020

Revised: 9/30/2020

Addendum to Data Classification Policy

Addendum to Data Classification Policy

Data Classification Elements

	Restricted	Sensitive	Public
Description	Data which is legally regulated, and data that must receive the most restrictive controls.	Data must be protected due to ethical, privacy or business considerations.	Data for which there is no expectation for privacy or confidentiality and has no restrictions.
Requirements	Data protection is required by law, or determined by theData Steward.	Data protection is at the discretion of the Data Steward.	Data protection is at the discretion of the Data Steward.
Risk to the Institution	High	Medium	Low
Data Access and Control	Data is accessible only to those individuals who have been approved access; legal,ethical and other constraintsprevent access without specific authorization.	May be accessed by Siena College employees who have a business need.	There are no access restrictions as the data is available publicly.
Transmission	Unauthorized transmission of Restricted data through any non-Siena network (Internet) or through any electronic messaging system (email, instant messaging, text messaging) is prohibited. Legal or regulatory requirements may supersede.	Transmission of Sensitive data through any non-Siena network (Internet) or through any electronic messaging system (email, instant messaging, text messaging) is strongly discouraged.	No additional protection is required, although care should be taken to use all College related information appropriately.
Storage	Data designated as Restricted cannot be stored on unauthorized machines that do not belong to the College.	Data cannot be stored on unauthorized machines that do not belong to the College.	No additional protection is required, although care should be taken to use all College related 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.
Controls	Data Stewards must ensure that appropriate controls for their systems and procedures are in place for potential misuse and/or unauthorized access.	Data Stewards periodically review systems and procedures for potential misuse and/or unauthorized access	No audit controls are required.

Examples (not all-inclusive)	**Personally Identifiable Information:** Last name, first name, with any one of the following: ● Social Security Number (SSN) ● Driver's license ● State ID card ● Passport number ● Financial account (checking, savings, brokerage, CD, etc .), credit card, or debit card numbers) ● Protected Health Information (PHI) ● Health status ● Healthcare treatment ● Healthcare payment **Personal/Employee Data:** ● Worker's compensation or disability claims ● Income and payroll information ● Personnel records, performance reviews **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	● Directory/contact information designated by the owner as private ● ID card photographs ● Financial transactions which do not include confidential data ● Information covered by non-disclosure agreements ● Dates of current employment, position(s) **Academic / Research Information:** ● Library transactions ● Unpublished research or research detail / results that are not confidential data ● Course evaluations **Donor Information:** ● Last name, first name or initial (and/or name of organization if applicable) with any type of gift information (e.g., amount and purpose of commitment) **Management Data:** ● Detailed annual budget information ● Conflict of Interest Disclosures	**Information not designated by the owner as private, such as:** ● Name ● Email address ● Listed telephone number(s) ● Degrees, honors and awards ● Most recent previous educational institution attended ● Major field of study **Business Data:** ● Campus maps ● Job postings ● List of publications (published research)

	● Athletics or department recruiting information **Business/Financial Data:** ● Credit card numbers with/without expiration dates		