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 the Data 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 constraints prevent 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 (e-mail, 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 (e-mail, 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 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/Student Data** ● Siena College ID number ● Race, ethnicity, nationality, gender ● Date and place of birth ● 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)	**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)

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