Classification of Data

An integral part of our data security practices at Ursinus involves classifying our college data based on levels of sensitivity and value. The four classification of data classes provides the foundation to allow us to protect sensitive data while simultaneously providing broad, open access to data in all of its forms. Our classification policy defines 4 classes of data from critical (Class I) to public (Class IV). Decisions about data types not explicitly defined in this policy should be made by the Data Stewards overseeing the data.

	Class 1: Critical Information	**Class II: Restricted Information**	**Class III: Institutional Data**	**Class IV: Public /Unrestricted Information**
Description	Information legally classified as breach notifiable and where Ursinus College is required to self-report to the government and /or provide notice to the individual if the information is inappropriately accessed. Data of this type includes, but is not limited to, all data identified by law, specifically, Pennsylvania Statute 73 Pa. Stat. § 2301 et seq. as well as other applicable state statutes*, Payment Card Industry Data Security Standard (PCI DSS), and specific combinations of individual financial records (Gramm-Leach_Bliley Act), health care records (Health Insurance Portability and Accountability Act of 1996 (HIPAA)).	Information regulated or restricted by federal and/or state regulatory or legal requirements, contractual requirements, or College policy. Data of this type includes, but is not limited to, student records (Family Educational Rights and Privacy Act (FERPA)), financial records (Gramm-Leach_Bliley Act), health care records (Health Insurance Portability and Accountability Act of 1996 (HIPAA)), International Traffic in Arms Regulations (ITAR)***, Export Administration Regulations (EAR)***, Red Flags Rule, Children's Online Privacy Protection Act (COPPA), employment records, legal records, and certain business records.	Information at the Institutional /Proprietary level must be protected due to privacy, ethical, or proprietary constraints. Data of this type includes, but is not limited to, intellectual property and any data or documents that are not intended for public access or distribution.	Data at the Public/Unrestricted level is protected at the discretion of the department or the data owner. Data of this type includes, but is not limited to, all documents slated for public distribution, directory information as per FERPA, and any departmental data not deemed to be at a higher level of sensitivity.
Examples of Data Elements within Specific Classification Levels	• Social Security Numbers • Credit Card Numbers • Driver's license number or state identification card number issued in lieu of a driver's license • Account number or credit card number or debit card number in combination with any required security verification code**, access code, or password that would permit access to an individual's financial account. • Passport ID Numbers or Other forms of Official Government Issued Identification • Health Care Information, including Protected Health Information (PHI) • A username or email address, in combination with an unencrypted password, biometric identifier, or security question and answer that would allow unauthorized access to an online account.	• Human Subjects Information • Information gathered of children under the age of 13 • Employment applications • Employee information, including personnel files, benefits information, salary, conflict of interest filings, birth date, and personal contact information • Privileged attorney-client communications • Internal policy records • Export controlled information under U.S. laws*** • Emergency and disaster recovery/incident response plans	• Student grades, attendance, and performance records **** • Ursinus Colleague ID • Departmental data • Unpublished research data • Ursinus internal memos • Internal reports • Class rosters • Marketing and forecasting reports • Email distribution lists • Source code • Building diagrams and blueprints • Donor information • Vendor non-disclosure agreements • Business transactional data and documents • Personal information that can be used to verify identity such as birth dates, mother's maiden name, photographs	• Published articles and newsletters • Student achievements and accolades • Published research data • Campus maps • Job postings • Student enrollment numbers • Directory Information (Ursinus definition)
Access	Access limited to those permitted under law, regulation and Ursinus College policies, and with a job-specific need and required training. External release of this type of information is only through executive management or through subpoena or warrant. Unauthorized release of this type of data could result in termination from College employment.	Access limited to those permitted under law, regulation and Ursinus College policies, and with a specific need to know. External release of this type of information is only through executive management or through subpoena or warrant. Unauthorized release of this type of data could result in termination from College employment.	Access is limited to only those individuals who have been approved for access by the Data Steward based on need to know. Public or external requests to release this type of information is only through management or through subpoena or warrant. Unauthorized release of this type of data could result in disciplinary action.	Access to all data not meant for public consumption is at the discretion of the department or data owner.
Transmission	NIST-approved encryption methods are required when transmitting information through a network. Prohibited data shall not be sent by email unless it is sent using an institution-approved method.	NIST-approved encryption methods are required when transmitting information through a network. Restricted data shall not be sent by email unless it is sent using an institution-approved method.	NIST-approved encryption is strongly recommended when transmitting information through a network. Institutional Confidential /Proprietary information sent by email should follow the institution guidelines.	No encryption is required for public/unrestricted information.

Storage	Prohibited information shall not be stored on any of the following media or devices: • non-Ursinus owned or personal devices • external media, including flash drives, cell phones, or other external forms of storage (excluding College Data Center disaster recovery backups) Prohibited data shall be encrypted if utilized or stored on any end point device or local system and that data should strictly be used for short-term processing and not for long-term storage. Prohibited data should be stored only on NIST-encrypted or other qualified College-owned hosts, and in accordance with the Ursinus College Records Management and Retention Policy (needs to be developed)	Restricted/Regulated information shall be stored in accordance with the following: • Any computers containing this type of data is stored utilizing strong password encryption and can not be accessed without first authenticating (de-crypting) the data. Whole disk encryption is a preferable solution in place of manually encrypting data. • Any storage of this type of information in a cloud environment must be in an approved Ursinus College approved Cloud storage solution. Any of this type of data stored on flash drives, cell phones, or any other external form of storage (including backups), must be in an encrypted form. Please note that while some services are approved for storage of Type II data, they cannot be used for ITAR and export controlled data unless they guarantee US-only storage and confirm that the data is not accessible by foreign nationals of restricted countries. In addition to storage restrictions on this type of data there are also restrictions on sharing such data with those located in other countries. It is up to the data owner to determine whether any export controlled data may be shared with someone or transported to a particular country. Guidance can be found at the US Department of Commerce Control List site at http://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl Long-term or archival storage of restricted/regulated data should be on NIST-encrypted or other qualified College-owned hosts, and in accordance with the Ursinus College Records Management and Retention Policy (needs to be developed)	Institutional Confidential /Proprietary information shall be stored in accordance with the following: • It is strongly recommended that this type of data is stored utilizing strong password encryption and can not be accessed without first authenticating (de-crypting) the data. Whole disk encryption is a preferable solution in place of manually encrypting data. • Any storage of this type of information in a cloud environment must be in an approved Ursinus College Cloud storage solution. It is strongly recommended that this type of data stored on flash drives, cell phones, or any other external form of storage (including backups), be in an encrypted form. Long-term or archival storage of institutional confidential/proprietary data should be on qualified College-owned or Cloud services hosts, and in accordance with the Ursinus College Records Management and Retention Policy (needs to be developed)	Long-term or archival storage of Ursinus College public /unrestricted data should be on qualified College-owned or Cloud services hosts, and in accordance with the Ursinus College Records Management and Retention Policy (needs to be developed)

*NCSL Security Breach Notification Laws by State

Pennsylvania Office of Administration Information Technology IT Security Incident Reporting Policy (PDF)

**Per PCI-DSS, card verification code or value, aka CVV, CAV, CID, CVC, should never be stored.

***Additional restrictions apply to this type of data. It must be stored within the United States and cannot be shared with those located in other countries. It is up to the data owner to determine whether any export controlled data may be shared with someone or transported to a particular country. Guidance can be found at the US Department of Commerce List site at: http://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl

**** Current processes on campus provide grade related information via email. The Data Standards in Governance committee is committed to improving these processes to eventually provide all grade related information through more secure methods. Once this is accomplished, grade related information would then be reclassified to Class II.