WAGNER COLLEGE

POLICY:
DATA CLASSIFICATION

CONTENTS

DOCUMENT #: POL-0002
EFFECTIVE: 05/31/2023
OWNER: ISO

1.0 PURPOSE

The purpose of this policy is to define the data classification requirements for information assets and to ensure that data is secured and handled according to its sensitivity and the impact that theft, corruption, loss, or exposure would have on the institution. This policy has been developed to assist Wagner College and provide direction to the institution regarding the identification, classification, and handling of information assets.

2.0 SCOPE

The scope of this policy includes all information assets governed by Wagner College. All faculty, staff, student workers, and third parties who have access to or utilize the institution's information assets, including data at rest, in transit or in process shall be subject to these requirements.

3.0 POLICY

Wagner College has established the requirements enumerated below regarding the classification of data to protect the institution's information.

3.1 DATA OWNERSHIP AND ACCOUNTABILITY

Data owners are identified as the individuals, roles, or committees primarily responsible for information assets. These individuals are responsible for identifying the institution's information assets under their areas of supervision and maintaining an accurate and complete inventory for data classification and handling purposes.

Data owners are accountable for ensuring that their information assets receive an initial classification upon creation and a re-classification whenever reasonable. Re-classification of an information asset should be performed by the asset owners whenever the asset is significantly modified. Additionally, data owners are responsible for reporting deficiencies in security controls to management.

ROLE	STEWARDSHIP RESPONSIBILITIES
Asset Owner	Role Description: Asset Owner: An individual in the Institution that authorizes the type of access, care, and maintenance for a specific Information Asset. The organization must have business responsibility of the asset even if

ROLE	STEWARDSHIP RESPONSIBILITIES
	another organization or department may develop or another organization accesses or uses the Information Asset. Responsibilities: 1. Determine appropriate Data sensitivity classifications. Refer to the Business Continuity-Disaster Recovery Policy. 2. Approve access requests for authorized Users of the Information Asset. 3. Approve access of any role requiring access to the Information Asset. (Approval of roles implies approval of access by any individual assigned a role and therefore removes the need to approve every individual access request.) 4. Assist in adoption and compliance with security policies. 5. Coordinate the development, maintenance and adherence to processes and procedures necessary to comply with security policies, including conducting periodic access reviews for the Information Asset. 6. Coordinate the development, maintenance and adherence to processes and procedures necessary for testing of disaster recovery plans. 7. Properly protect Information Assets within the Asset Owner's access control in accordance with the asset's Data Sensitivity, and Data Criticality instructions. 8. Ensure maintenance of all relevant security documentation related to the Information Asset, including but not limited to: procedures, security assessments, risk analysis, related risk acceptance documentation, etc.
Custodian	Role Description: Custodian: An individual who is accountable for an Information Asset. Responsibilities:

ROLE	STEWARDSHIP RESPONSIBILITIES
	1. Properly protect Information Assets within the Asset Owner's access control, Data Sensitivity, and Data Criticality instructions. 2. Validate configuration and maintenance of security mechanisms under the control of the Systems Administration function are followed, such as the operating system configuration and maintenance. 3. Validate specific security control procedures, including system administration processes, are implemented. 4. Validate recovery capabilities consistent with the instructions of Asset Owners are followed. 5. Validate that a back-up process is followed so that critical information will not be lost. 6. Validate appropriate configuration management processes and procedures are executed to provide integrity and maintainability. 7. Validate disaster recovery plans exist.
Authorized User	Role Description: An authorized user is an employee, consultant, client or other individual with a legitimate business need and proper authorization to access Wagner College information in order to perform an activity on behalf of Wagner College or its customers. Responsibilities: 1. Understands and adheres to applicable Wagner College Information Security and acceptable use obligations as described in relevant policies and standards. 2. Reports security violations to the CISO, Security Manager or designee.

3.2 DATA CLASSIFICATION

Classification of data will be performed by the data asset owner based on the specific, finite criteria as identified in the Federal Information Processing Standard Publication 199 (FIPS-199) for confidentiality, integrity, and availability. Refer to the Data Classification and Handling Procedure to determine how data should be classified. Data classifications will be defined as follows:

- *Restricted* – Information assets whose loss, corruption, or unauthorized disclosure would cause financial loss or result in regulatory or government sanctions such as violations of federal or state laws or security breaches resulting in the compromise of customer or associate private information. Common examples include but are not limited to information covered by the Family Educational Rights and Privacy Act (FERPA), social security numbers, banking and health information, payment card information, personnel records, and information systems' authentication data.
    - *Jenzabar Data Base, and all info housed within the DATABASE.*
    - *Hardware housing Wagner College data.*
    - *Course Exams.*
    - *Wagner College computer hardware and mobile devices.*
    - *Personal Identifier Information.*
- *PRIVATE* – Information assets whose loss, corruption, or unauthorized disclosure would not seriously impair business functions but is otherwise private. Examples include but are not limited to final course grades, protected data related to research, financial statements, contracts, and legal information.
    - *Course Work.*
    - *Student Work.*
    - *Moodle.*
    - *Google Drive.*
    - *DFS.*
- *PUBLIC* – Information assets whose loss, corruption, or unauthorized disclosure would not impair business functions. Examples include but are not limited to sales and marketing strategies, website content, building plans, and promotional information.
    - Wagner College Website and information supplied on the site.
    - Information that may be released to anyone without a student's consent and that would not generally be considered harmful or an invasion of privacy if disclosed. Common examples include but are not limited to student name, address local, permanent, and e-mail), telephone number (local and permanent), photograph, dates of attendance at the institution, major, degrees and awards received, participation in officially recognized activities, and sports, and date and place of birth.

Data Classification Examples

	RESTRICTED	PRIVATE	PUBLIC
Description	Information whose unauthorized disclosure,	Information whose loss, corruption, or	Information whose loss, corruption, or

	RESTRICTED	PRIVATE	PUBLIC
	compromise, corruption, loss, or destruction would cause **severe** personal, financial or reputational harm to the organization, organization staff or the constituents/people we serve.	unauthorized disclosure would likely cause **limited** personal, financial, legal, or reputational harm to the organization, organization staff or the constituents/people we serve.	unauthorized disclosure would cause **minimal or no** personal, financial or reputational harm to the organization, organization staff or the constituents/people we serve.
Sensitivity	HIGH	MODERATE	LOW
Access Requirements	Individuals who have a relationship with Wagner College; a business need to know; approved access; and where appropriate, a signed non-disclosure agreement.	Wagner College personnel who have a business need to know.	Wagner College affiliates and general public

Examples	• Information regarding students, personnel, payroll, medical or Institution business that the Institution is obliged to protect; this includes production, development and testing environments.
	• Examples include:
	  ○ Credit Card Numbers
	  ○ Student Financial Aid Information
	  ○ Financial Account Numbers
	  ○ Healthcare/medical records
	  ○ Payroll information
	  ○ Full Social Security Numbers
	  ○ Full Date of Birth
	  ○ Driver's License Number
	  ○ National or State ID
	  ○ Passport ID
		• Information not classified as RESTRICTED containing information which, if improperly disclosed, could result in potential compromise or misuse of sensitive information; access must be limited to personnel with a business need to know.
		• Examples include:
		  ○ Student Academic Records
		  ○ FERPA Data
		• Commonly shared (internal) information, including operating procedures, policies and inter-office memoranda.
			• Marketing brochures
			• Published annual reports
			• Interviews with news media
			• Press releases
			• Business cards

	RESTRICTED	PRIVATE	PUBLIC
	○ Tax ID or Tax Return • Account passwords or voice mail codes • All personal data required solely for identification, including: ○ Racial or ethnic origin ○ Political opinions ○ Religious beliefs or other beliefs of a similar nature ○ Physical or mental health conditions ○ Sexual orientation ○ Criminal record • Attorney - client privileged information • IT security information (such as privileged credentials, incident information) • Information about customers, prospective customers, vendors and business partners • Data with the potential for providing competitive advantage • Information that would enable clients with numbered accounts to be identified, including: ○ Customer data, including contact details, specifications and preferences ○ Contracts and agreements, including terms, expiration dates, financials, etc.	• Internal telephone directories. • Information identifying a client, but excluding any financial data such as balances, safekeeping positions, credit data, etc. ○ ○ Subscription lists ○ Employee lists, with contact information ○ Software or computer programs ○ Partial dates of birth ○ Truncated numbers from Social Security, Driver Licenses or Credit Cards	

	RESTRICTED	PRIVATE	PUBLIC
	○ Data such as institution holdings, general ledger accounts, legal files and confidential reports ○ Trade secrets ○ Pricing policies and information • Any form of encryption key • Any of the following, prior to public disclosure: ○ Regulatory agency and internal or external audit reports ○ Strategic planning information ○ Information on mergers, acquisitions or divestitures Financial forecasts or results, balance sheets, closing data or analysis		

DATA CLASS	DATA ELEMENT EXAMPLES	Public	Private	Restricted
Product Data	General Product information	X		
	Product Design Data		X	
	Actuarial Data			X
	Market Research Data		X	
	Product R & D			X
	Product Cost			X
	Product Testing		X	
	New Product Launch		X	

DATA CLASS	DATA ELEMENT EXAMPLES	Public	Private	Restricted
Compliance & Legal Data	Policies		X	
	Regulatory Compliance Data			X
	Policy & Training Attestations		X	
	Subpoena			X
	Attorney Client Privilege Information			X
	Titles			X
	Contracts			X
	Regulatory and Legal Filings			X
	Pending Litigation			X
	Investigation Reports			X
	Security Incident Reports			X
	Safety Incident Reports			X
	Investigation Reports			X
	Sexual Assault Reports			X
DATA CLASS	DATA ELEMENT EXAMPLES	Public	Private	Restricted
Financial Data	Electronic Payment Information (Wire Payment / ACH)			X
	Paychecks			X
	Incentives or Bonuses (amounts or percentages)			X
	Bank Account Information			X
	Investment-Related Activity			X
	Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)			X
	Debt Amount Information			X
	SEC Disclosure Information		X	
	Corporate Tax Return Information			X
	Legal Billings			X
	Budget-Related Data		X	
	Unannounced Merger and Acquisition Information			X
	Donation Information			X
	Financial Data Related to Revenue Generation			X

DATA CLASS	DATA ELEMENT EXAMPLES	Public	Private	Restricted
	Annual Reports		X	
DATA CLASS	DATA ELEMENT EXAMPLES	Public	Private	Restricted
Sales and Marketing Data	Business Plan (including marketing strategy)			X
	Marketing Promotions Development			X
	Internet-Facing Websites (e.g., institution website, social networks, blogs, promotions, etc.)	X		
	News Releases	X		
	Sales Forecasts		X	
	Client lists		X	
DATA CLASS	DATA ELEMENT EXAMPLES	Public	Private	Restricted
Physical Environment	Non-Public Building Plans		X	
	Emergency response plans		X	
	Alarm & Emergency system information			X
	Environmental control system information		X	
	Utilities related information		X	
	Surveillance and monitoring system information			X
DATA CLASS	DATA ELEMENT EXAMPLES	Public	Private	Restricted
Network and Infrastructure	Username & Password Pairs			X
	Public Key Infrastructure (PKI) Cryptographic Keys (Public and Private)			X
	Hardware or Software Tokens (multifactor authentication)			X
	System Configuration Settings		X	

DATA CLASS	DATA ELEMENT EXAMPLES	Public	Private	Restricted
	Internal IP Addresses			X
	Privileged Account Usernames			X
	Service Provider Account Numbers		X	
	Enterprise, Security, Network Architecture			X
	Security monitoring technologies			X
	Vulnerability related information			X

3.3 DATA HANDLING

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies, and destruction methods. The specific methods must be described in the Data Classification Procedure.

The Wagner College IT Department has implemented multiple layers of security to protect against unauthorized access of data.

First, the use of Active Directory and Last Pass provides a way to manage and enforce strong password policies for user accounts. This can help prevent brute force attacks and other methods of password guessing.

Second, folder permissions are assigned on a least-privilege basis, meaning that users are only given access to the files and folders they need to do their jobs. This can help prevent accidental or intentional access to sensitive data.

Third, the use of complex passwords and multifactor authentication adds additional layers of protection to prevent unauthorized access. Multifactor authentication requires users to provide a second form of identification, such as a fingerprint or a code sent to their phone, before they can access the system. This can help prevent attacks that rely on stolen or guessed passwords.

Finally, the process of encrypting data at rest and in motion adds an additional layer of protection to prevent unauthorized access to sensitive data. Encrypting data makes it more difficult for attackers to read or modify the data, even if they are able to gain access to it. Overall, it seems like

the system you described has a strong set of security controls in place to protect against unauthorized access to sensitive data.

HANDLING CONTROLS	RESTRICTED	PRIVATE	PUBLIC
Internal distribution of printed documents and media	Carry the document or media personally; if the receiver is not present then wait for him/her or come back later when he/she is present. Never leave paper or media unattended.	No special requirements	No special requirements
External distribution of printed documents and media	Transmit only minimum necessary RESTRICTED information to authorized person(s). Double envelope with tampering detection and the word CONFIDENTIAL in a visible place. Use a contracted service provider for transport.	Transmit only minimum necessary CONFIDENTIAL information to authorized person(s).	No special requirements
Fax	Normal fax machine. Call the receiver before sending the fax to make sure that he/she is near the fax machine to get the document. Dial the number manually to avoid wrong, corrupted or altered numbers. Remain near the fax and call the receiver in the end to confirm the good reception and the number of pages received. Stamp the fax with the word CONFIDENTIAL.	Normal fax machine with coversheet addressed to the recipient.	Normal fax machine
Inter-departmental Communications (e.g., e-mail, IM)	Transmit only minimum necessary RESTRICTED information to authorized person(s).	No special requirements	No special requirements

HANDLING CONTROLS	RESTRICTED	PRIVATE	PUBLIC
External Communications (e.g., e-mail, IM)	Transmit only minimum necessary RESTRICTED information to authorized person(s). Always use secure/encrypted channels to transmit CONFIDENTIAL data and/or information.	Approval to send external and preferably protect the attachment with a password.	No special requirements
External transmission of data and/or information	Transmit only the minimum necessary RESTRICTED information to the authorized person(s). Always use secure/encrypted channels to transmit CONFIDENTIAL data and/or information.	Approval to send external and preferably whenever possible, use safe channels.	No special requirements
Copying to Removable Media	Wagner College restricts the use of removable media to store/transmit RESTRICTED information to authorized individuals. Erase or reformat when no longer needed.	Erase or reformat	No special requirements
Storage/Archive: printed paper and media	Never leave the document or media unattended, store in a locked room, cabinet or case whenever not in use.	No special requirements	No special requirements
Storage/Archive: data and digital files	Storage only allowed in repositories authorized for RESTRICTED data, ex. file share with access profiles defined. On laptops always encrypt confidential information, ex. Windows 10 BitLocker. All information stored in tapes or any other optical format must be encrypted.	No special requirements	No special requirements

HANDLING CONTROLS	RESTRICTED	PRIVATE	PUBLIC
Destruction: printed documents	Destroy papers personally using a shredder, this task must not be delegated. When out of the office, keep the documents in a safe place until you can return to the office and follow the above procedure.	Recycle whenever possible using shredders.	No special requirements. Recycle whenever possible.
Destruction: data and media (HDD)	Since the recovery of data is always possible, the media must be physically destroyed or follow the procedure for secure media disposal.	Erase or reformat	No special requirements
(Data Duplication and Displaying e.g., Teams)	Restrict copying and displaying only minimum necessary RESTRICTED information to those authorized.	Approval to display externally	No special requirements
Information communicated by phone	Do not discuss RESTRICTED information on the phone in public places. Do not leave RESTRICTED information in voice mails.	Do not discuss this on the phone in public.	No special requirements
Public conversations	Do not discuss in public, only in private.	Avoid discussing in public.	No special requirements

3.4 DATA RETENTION

Guidelines and procedures are put in place to ensure that the institution's data is managed, stored, and deleted properly. The policy is usually developed to comply with legal requirements, industry standards, and best practices to protect sensitive data from unauthorized access, misuse, or loss.

The retention period for data varies depending on its type and purpose. For instance, student academic records may be retained for a certain number of years after graduation, while employee files may be kept for several years after the individual leaves the institution. Research data may be retained for several years or permanently, depending on the discipline and funding source.

The Data Owner is both responsible and accountable for determining the retention requirements for all data and data records in their charge and any specific destruction requirements for the data based on its classification. Data retention requirements must address both legitimate business needs and all regulatory and legal requirements or restrictions. The

Data Owner must communicate all requirements to the Data Custodian and work with the Data Custodian to ensure data retention, recovery, and destruction strategies are appropriate and efficient.

Wagner College IT Department is responsible for data management and security, and the protocols for accessing and sharing the data. It outlines the procedures for data backup and disaster recovery, and the steps to be taken in case of a data breach or loss.

By adhering to this policy, the institution can safeguard its reputation, comply with legal and regulatory requirements, and maintain the privacy and confidentiality of its stakeholders' data.

3.4 RE-CLASSIFICATION

A re-evaluation of classified data assets will be performed at least once per year by the responsible data owners. Re-classification of data assets should be considered whenever the data asset is modified, retired, or destroyed.

3.5 CLASSIFICATION INHERITANCE

Logical or physical assets that "contain" a data asset may inherit classification from the data asset(s) contained therein. In these cases, the inherited classification shall be the highest classification of all contained data assets.

4.0 ENFORCEMENT

Users who violate this policy may be denied access to the institution's resources and may be subject to penalties and disciplinary action both within and outside of the institution. The institution may temporarily suspend or block access to an account prior to the initiation or completion of such procedures when it appears reasonably necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect the institution from liability.

5.0 EXCEPTIONS

Exceptions to this policy must be approved in advance by the Chief Information Officer, at the request of the responsible data asset owner. Approved exceptions must be reviewed and re-approved by the asset owner annually.

6.0 REFERENCES

- Federal Information Processing Standard Publication 199 (FIPS-199)
- NIST Special Publication 800-53 r4

7.0 RELATED POLICIES

- Acceptable Use Policy
- Information Security Policy
- Data Classification and Handling Procedure

8.0 RESPONSIBLE DEPARTMENT

Wagner College IT Department.

9.0 POLICY AUTHORITY

This policy is issued by the Chief Information Officer for Wagner College.