Data Classification and Protection Standard

1.0 Overview

Data assets are some of the most valuable assets owned by the Quincy College (QC). QC produces, collects, and uses many different types of data in fulfilling its mission. Laws and institutional policy mandate privacy and protection of certain types of data, and the University's need to manage the risks to its reputation and to its constituents requires the protection of other information. Classifying data is the first step in determining the data's need for protection.

2.0 Objective / Purpose

This standard is intended to help QC employees classify data for the purposes of determining its need for protection and determining applicable policies and laws.

3.0 Scope

This standard can be used to classify any data that are stored, processed, or transmitted by QC. The standard applies to all types of data: Electronic data, Data recorded on paper and Information shared orally, visually or by other means.

4.0 Standard

4.1 Classification

Data can be classified either in terms of its need for protection (e.g. Sensitive Data) or its need for availability (e.g. Critical Data). To classify data in terms of its need for protection, use section 4.1.1 of this standard. To classify data in terms or its availability needs, use section 4.1.2 of this standard.

4.1.1 Classifying Data According to Protection Needs

Match any data that need to be classified to the one of the four categories which best describes its need for confidentiality and its risk profile. The four categories are Public, Internal, Sensitive, and Restricted.

4.1.1.1 Public Data - Data can be disclosed without restriction. Examples - Directories, Maps, Syllabi and Course Materials, de-identified data sets, etc.

4.1.1.2 Internal Data - Confidentiality of data is preferred, but information contained in data may be subject to open records disclosure. Examples - email correspondence, budget plans, etc.

4.1.1.3 Sensitive Data - Data confidentiality required by law, policy, or contractual obligation.

Characteristics of Sensitive Data

- Compliance Risk: Protection of data is mandated by law (e.g. FERPA) or required by private contract (e.g. non-disclosure agreements).
- Reputation Risk: Loss of confidentiality or integrity will cause significant damage to QC's reputation. For example, loss of social security numbers or defacement of the QC website would likely be a news item that would appear in the media.
- Other Risks: Loss of confidentiality that could cause harm to individuals such as QC students, personnel, donors, and partners. Loss of confidentiality or integrity that would cause QC to incur significant costs in response.
- Treatment in Open Records Requests: Sensitive information is typically redacted from open records disclosures.

Examples of Sensitive Data

- Student records and prospective student records (w/o Social Security Numbers)
- Donor and alumni records
- Critical infrastructure information (physical plant detail, IT systems information, system passwords, information security plans, etc.)
- Research information related to sponsorship, funding, human subject, etc.
- Information protected by non-disclosure agreements (NDAs) or similar private contracts
- Law enforcement and investigative records
- QC ID Number (also known as the 81X Number)

4.1.1.4 Restricted Data - Restricted data requires privacy and security protections. Special authorization may be required for use and collection. Examples - data sets with individual Social Security Numbers (or last four of SSN), credit card transaction or cardholder data, patient health data, financial data, etc.

Characteristics of Restricted Data

Senior Vice President (SVP) Approval: QC SVPs or their designees must authorize all storing, processing, and transmitting of Restricted Information.

- Compliance Risk: Protection of information is mandated by law (HIPAA, GLBA) or required by private contract (PCI DSS).
- Reputation Risk: Loss of confidentiality or integrity will cause significant damage to QC's reputation.
- Other Risks: Loss of the confidentiality or integrity of the information that could cause harm to individuals and cause the University to incur significant costs in response.
- Treatment in Open Records Requests: Records with restricted information are typically not open for public inspection.

Examples of Restricted Data

- Social Security Numbers (or last four numbers of an individual's SSN)
- Credit/debit card data
- Healthcare data
- Financial account data

4.1.2 Classifying Data According to Availability Needs

Match any data that need to be classified according to availability needs to the one of the three categories which best describes its need for availability needs. The three categories are Supportive, High-Priority, and Critical.

4.1.2.1 Supportive Data - Supportive data is necessary for day-to-day operations, but is not critical to the University's or to a Department/Unit/College's mission or core functions. Examples - course materials, meeting minutes, workstation images, etc.

4.1.2.2 High-priority Data - Availability of data is necessary for departmental function. Destruction or temporary loss of data may have an adverse effect on college or departmental mission, but would not affect university-wide function.

4.1.2.3 Critical Data - Critical data has the highest need for availability. If the information is not available due to system downtime, modification, destruction, etc., the University's functions and mission would be impacted. Availability of this information must be rigorously protected.

Characteristics of Critical Data

- Mission Risk: Short-term or prolonged loss of availability could prevent QC from accomplishing its core functions or mission.

- Health and Safety Risk: Loss of availabity may create health or safety risk for individuals. (e.g. emergency notification data, health data, etc.).
- Compliance Risk: Availability of information is mandated by law (HIPAA, GLBA) or required by private contract.
- Reputation Risk: Loss of data will cause significant damage to QC's reputation.

Examples of Critical Data

- Emergency notification/contact data
- Health care data
- Student records

4.2 Protection

See the table below for minimum standard protection requirements for each category of data when being used or handled in a specific context (e.g. Sensitive Data sent in an email message). Please note that the below protection standards are not intended to supersede any regulatory or contractual requirements for handling data. Some specific data sets, such as student records data, credit/debit card data, healthcare data, and financial account data, may have stricter requirements in addition to the minimum standard requirements listed below.

	Public Data	Internal Data	Sensitive Data	Restricted Data
Collection and Use	No protection requirements	No protection requirements	Limited to authorized users. Departments that collect and/or use Sensitive data should report these records to the Information Technology Department.	Limited to authorized users. Departments that collect and/or use Restricted data should report these records to the Information Technology Department.

			Quincy College web pages that are used to collect sensitive data must include a link to the Privacy Policy.	Quincy College web pages that are used to collect restricted data must include a link to the Privacy Policy. SSNs may not be used to identify members of Quincy College if there is a reasonable alternative. SSNs shall not be used as a username or password. SSNs shall not collected on unauthenticated individuals.
Granting Access or Sharing	No protection requirements	Reasonable methods shall be used to ensure internal data is accessed by or shared with authorized individuals or individuals with a legitimate need to know.	Access shall be limited to authorized college officials or agents with a legitimate academic or business interest. All access shall be approved by an appropriate data owner and documented in a manner sufficient to auditable. Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data must be approved.	Access shall be limited to authorized college officials or agents with a legitimate academic or business interest and a need to know security leve. All access shall be approved by an appropriate data owner and documented in a manner sufficient to auditable. Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved..
Disclosure, Public Posting, etc.	No protection requirements	Reasonable methods shall be used to	Sensitive data shall not be disclosed without consent.	Not permitted unless required by law.

		ensure internal data is only disclosed to authorized individuals or individuals with a legitimate need to know.	Sensitive data may not be posted publicly. Directory information can be disclosed without consent. However, per FERPA, individual students can opt out of directory information disclosure.	
Electronic Display	No protection requirements	Reasonable methods shall be used to ensure internal data is only displayed to authorized individuals or individuals with a legitimate need to know.	Only to authorized and authenticated users of a system.	Restricted data shall be displayed only to authorized and authenticated users of a system. Identifying numbers or account number shall be, at least partially, masked or redacted.
Open Records Requests	Data can be readily provided upon request. However, individuals who receive a request must coordinate the Quincy College Registrars office before providing data.	Individuals who receive a request must coordinate with the Quincy College Registrars office.	Sensitive data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with the Quincy College Registrars office.	Restricted data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with the Quincy College Registrars office.

Exchanging with Third Parties, Service Providers, Cloud Services, etc.	No protection requirements	Reasonable methods shall be used to ensure that the third party's responsibilities for confidentiality / privacy of the data are defined and documented.	An contractual agreement outlining security responsibilities shall be in place and approved by the Information Technology department before exchanging data with the third party / service provider.	An contractual agreement outlining security responsibilities shall be in place and approved by the Information Technology department before exchanging data with the third party / service provider.
Storing or Processing: Server Environment	Servers that connect to the QC Network shall comply with Antivirus Security Policy.	Servers that connect to the QC Network shall comply with Antivirus Security Policy.	Servers shall comply with security requirements as outlined in the Antivirus Security Policys.	Servers shall comply with security requirements as outlined in the Antivirus Security Policy. Storing Credit/Debit card data is not permitted.
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop,tablet, etc.)	Systems that connect to the QC Network shall comply with Antivirus Security Policy.	Systems that connect to the QC Network shall comply with Antivirus Security Policy.	Systems shall comply with security requirements as outlined in the Antivirus Security Policy.	Systems shall comply with security requirements as outlined in the Antivirus Security Policy. Storing Credit/Debit card PAN data is not permitted. Storing restricted data on personally-owned devices is not permitted.
Storing on Removable	No protection requirements	No protection requirements	Sensitive data shall only be stored on	Not permitted unless required by law.

Media (e.g. thumbdrives, CDs, tape, etc.)			removable media in an encrypted file format or within an encrypted volume.	If required by law, data stored on removable media shall be encrypted and the media shall be stored in a physically secured environment. Storing restricted data on personally-owned media is not permitted.
Electronic Transmission	No protection requirements	No protection requirements	Data shall be transmitted in either an encrypted file format or over a secure protocol or connection.	Secure, authenticated connections or secure protocols shall be used for transmission of restricted data.
Email and other electronic messaging	No protection requirements	Reasonable methods shall be used to ensure internal data is only included in messages to authorized individuals or individuals with a legitimate need to know.	Sensitive data shall only be included in messages within an encrypted file attachment. Messages shall only be sent to authorized individuals or other individuals with a legitimate need to know.	Not permitted unless required by law. If required by law, data shall included in an encrypted file that attached to the message.
Printing, mailing, fax, etc.	No protection requirements	Reasonable methods shall be used to ensure that printed materials are only distributed or available to authorized	Printed materials that include sensitive data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know.	Printed materials that include restricted data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know.

		individuals or individuals with a legitimate need to know.	Access to any area where printed records with sensitive data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.	Access to any area where printed records with restricted data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry. Social Security Numbers shall not be printed on any card required to access services. New processes requiring the printing of SSN on mailed materials shall not be established unless required by another state agency or a federal agency.
Disposal	No protection requirements	No protection requirements.	Data shall be deleted and unrecoverable (e.g. eraser, zero-fiil, DoD multipass, etc.). Physical media (e.g. paper, CD, tape, etc.) should be destroyed so that data on the media cannot be recovered or reconstructed.	Data shall be deleted and unrecoverable (e.g. eraser, zero-fiil, DoD multipass, etc.). Physical media (e.g. paper, CD, tape, etc.) should be destroyed so that data on the media cannot be recovered or reconstructed.

5.0 Enforcement

5.0 Enforcement and Implementation

5.1 Roles and Responsibilities

Each college department/unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this standard.

The department of Information Technology is responsible for enforcing this standard.

5.2 Consequences and Sanctions

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other Quincy College policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation.

Any device that does not meet the minimum security requirements outlined in this standard may be removed from the QC network, disabled, etc. as appropriate until the device can comply with this standard.

6.0 Exceptions

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, contact the Information Technology Department.