Data Access Policy

1.0 Overview

Quincy College (QC) shall approve access to Sensitive Institutional Data in order to ensure that access to sensitive data is authorized, that sensitive data with a need for protection are used appropriately and that authorized access complies with the QC Privacy Policy and relevant state and federal laws.

2.0 Objective / Purpose

This policy outlines requirements for granting and revoking access to Sensitive Institutional Data.

3.0 Scope

This policy applies to access to Sensitive or Restricted data maintained by the College or a party acting on the behalf of the College. This policy does not apply to data or records that are personal property of a member of the College community, research data, or data created and/or kept by individual employees or affiliates for their own use. Requests for records by the public are outside of the scope of this policy and shall be handled by the Registrar's Office. This policy also does not apply to situations in which the College is legally compelled to provide access to information.

4.0 Policy

4.1 Institutional Data shall be Classified

Institutional Data shall be classified in accordance with the Data Classification and Protection Standard to identify the level of confidentiality needs, legal requirements, and minimum standard protections for the data before access is granted.

4.2 Data Stewards Approve Access to Sensitive Institutional Data

Access to Sensitive Institutional Data is approved by QC designated Data Stewards. Data Stewards shall grant access in compliance with the QC Privacy Policy and all relevant regulations (e.g. FERPA, HIPAA and GLBA). Data Stewards shall grant access only to those employees, affiliates, and systems that need the access to perform their job duties or mission. Data Stewards are designated in Appendix A - Data Stewards and Trusted Designees (below). In the case that a Data Steward is not designated, the data in question are owned by the dean, vice president, or department head of the unit that originates the data.

4.3 Senior Vice Presidents Retain the Right to Approve All Access to SSN Data

Access to Social Security Number (SSN) data shall not be granted to an employee unless approval has been granted by a College Vice President or a Vice President's designee.

4.4 Data Stewards are Responsible for Procedures for Requesting, Approving, and Revoking Access

Data Stewards shall ensure that procedures for requesting and approving access to Sensitive Institutional Data exist and are followed. Data Stewards shall also implement procedures for regularly auditing access to Sensitive Institutional Data and revoking access when it is no longer needed or authorized. Procedures may vary from Data Steward to Data Steward as necessary to accommodate different Data Steward mission/resources/etc. and different groups of Data Users. However, all procedures shall include sufficient tracking for requests, approvals, and revocations such that authorized access to Sensitive Institutional Data is auditable.

4.5 Only Authorized Users Shall Access Sensitive Institutional Data

All access by individuals to Sensitive Institutional Data shall be controlled by reasonable measures to prevent access by unauthorized users.

4.6 Data Users Shall Use Sensitive Institutional Data Responsibly

Data Users must responsibly use data for which they have access including only using the data for its intended purpose and respecting the privacy of members of the College community. Data Users must maintain the confidentiality data in accordance with the all applicable laws, the QC Privacy Policy and the Data Classification and Protection Standard. Authorized access to Sensitive Institutional Data does not imply authorization for copying, further dissemination of data, or any use other than the use for which the employee was authorized. The Data Steward retains the right to approve and grant access to Sensitive Institutional Data.

4.7 Data Stewards May Delegate Approval Responsibilities to a Trusted Designee

A Data Steward may delegate the ability to approve access to Sensitive Institutional Data to trusted individuals in designated roles. A Data Steward may delegate by creating procedures through which the designee may approve access by employees that have certain pre-approved roles and responsibilities. Data Stewards retain the responsibility for ensuring that all access to Sensitive Institutional Data is authorized, appropriate, and complies with relevant legal requirements; the responsibility does not transfer to designees.

4.8 External Third-Party Access to Sensitive Institutional Data Shall be Governed by Contractual Agreement

Access to Sensitive Institutional Data by external parties shall be governed by individual contractual agreement or memoranda of understanding if the third party is a governmental organization. Such contractual agreements shall be approved by the Information Technology department and by the appropriate QC designated Data Steward.

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 policy.

The Information Technology department is responsible for enforcing this policy.

5.2 Consequences and Sanctions

Violation of this policy may incur the same types of disciplinary measures and consequences as violations of other 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.

Violation of this policy may also result in termination of contracts or commitments to vendors and other affiliates. Legal action may be pursued where appropriate.

6.0 Definitions

Access - Flow of information between a store of data and a user, system, or process. A user, system, or process is considered to have access to data if it has one or more of the following privileges: the ability to read or view the data, update the existing data, create new data, delete data or the ability to make a copy of the data. Access can be provided either on a continual basis or, alternatively, on a one-time or ad hoc basis. Transferring any data from one party to another in any medium is tantamount to permitting access to those data.

Institutional Data - Those data, regardless of format, maintained by the Quincy College (QC) or a party acting on behalf of QC for reference or use by multiple College units. Institutional Data does not include data that is personal property of a member of the College community, research data, or data created and/or kept by individual

employees or affiliates for their own use. Examples of Institutional Data include student education records, payroll records, human resources records, and enterprise directory records.

Sensitive Institutional Data - Those Institutional Data that contain information that can be classified as either "sensitive" or "restricted" using the QC Data Classification and Protection Standard. Some examples of Sensitive Institutional Data include Institutional Data that are personally identifiable in nature and contain Social Security Numbers, Credit Card Numbers or other financial account numbers, HIPAA protected health information, or FERPA protected student education records.

Data Steward - The individual responsible for the data. The Data Steward is usually the dean, vice president, or unit head of the College unit that creates or originates the Institutional Data.

Data User - An individual that has been authorized to access data for the performance of his/her job duties.