Information Security Awareness Program

This document is part of a collection of documents that make up the Information Security Awareness Program. The following is a link to the main Information Security Awareness Program document.

Sensitive Data

First, we will define *sensitive data*. Although there are varied definitions of this, we will focus on two here. **Sensitive data**: 1) Any data that, if compromised from confidentiality, integrity, and/or availability perspectives, could have a material adverse effect on College interests; 2) Information that is protected against unwarranted disclosure.

Sensitive Information includes all data, in its original and duplicate form, which contains:

- Personally Identifiable Information – Ohio Identity Theft (PII)
- Student Education Information – Family Education Rights and Privacy Act (FERPA)
- Health Information – Health Insurance Portability and Accountability Act (HIPAA)
- Credit Card Information – Payment Card Industry (PCI)
- Public Records Information – Ohio Public Records Act

Other forms of sensitive data include: some types of research data (such as research data that is personally identifiable or proprietary), public safety information, financial donor information, information concerning select agents, system access passwords, information security records, and information file encryption keys.

Personally Identifiable Information

Personally Identifiable Information (PII) is data that can be used to uniquely identify or locate a single individual or data used with other sources to uniquely identify or locate a single individual. PII comes in many forms.

- Full Name (if not common)
- National Identification Number (including SSN)
- IP Address (in some cases)
- Vehicle License Plate Number
- Driver's License Number
- Face, Fingerprints, or Handwriting
- Credit Card Numbers
- Digital Identity
- Date of Birth
- Birthplace
- Genetic information

The following are less often used to uniquely identify or locate a single individual, because they are characteristics shared by many. However, they become PII because they may be combined with other personal information to uniquely identify or locate a single individual.

- First or Last Name (if common)
- Country, State, or City of Resident
- Age (especially if non-specific)
- Gender or Race
- School Name or Workplace
- Grades, Salary, or Job position
- Criminal Record

Read more on Ohio Identity Theft.

Student Education Information

The College has significant student education data. This data is protected by the Federal Government via the Family Educational Rights and Privacy Act of 1974 (FERPA). In general, schools are required to have written permission from students in order to release any information from a student's education record. This includes releasing information to parents. FERPA does, however, allow schools to disclose student records, without consent, to the following groups or under the following conditions:

- School officials with legitimate educational interest
- Other schools to which a student is transferring
- Specified officials for audit or evaluation purposes
- Appropriate parties in connection with financial aid to a student
- Organizations conducting certain studies for or on behalf of the school
- Accrediting organizations
- To comply with a judicial order or lawfully issued subpoena
- Appropriate officials in cases of health and safety emergencies
- State and local authorities, within a juvenile justice system, pursuant to specific State law

Schools may disclose, without consent, "directory" information such as students':

- Name
- Address
- Telephone number
- Date/place of birth
- Honors and awards and dates of attendance

However, schools must tell students about directory information and give them a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify students annually of their rights under FERPA. The actual means of notification (special letter, student handbook, or newspaper article) is left to the discretion of each school.

Health Information

Similar to student education data and FERPA, health information is protected by the Federal Government via the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA regulations define health information as "any information, whether oral or recorded in any form or medium" that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse

  And

- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual

Payment Card Information

Payment Card Industry (PCI) compliance applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If a business accepts or processes payment cards, it must comply with the PCI Data Security Standards (DSS).

PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit this data, and include specific requirements for software developers and manufacturers of applications and devices used in the transaction process. Compliance with the PCI security standards is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

Public Records Information

The Ohio Public Records Law generally requires every public office, when requested, to promptly prepare public records and make them available for inspection at all reasonable times during regular business hours. Upon request and within a reasonable period of time, a public office or person responsible for public records generally must make copies available at cost. Public records must be maintained in such a manner that they can be made available for inspection and copying.