Information Security Policy

Policy Number: **TRU - 926**

Date of Issuance: 12 Dec 22

Responsible Department: Office of the IT Director. Questions about this policy should be directed to the Information Security Team, infosec@indycc.edu

---

Purpose

Independence Community College ("College") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, integrity and availability of Institutional Data as well as any Information Systems that store, process, or transmit Institutional Data.

Scope

This Policy applies to all faculty, staff, and third-party Agents of the College as well as any other College affiliate, including student workers, who are authorized to access or manage Institutional Data.

Maintenance

This Policy will be reviewed by the College's Information Security Team every 3 years or as deemed appropriate based on changes in technology or regulatory requirements.

Enforcement

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and College owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the College. Civil, criminal and equitable remedies may apply.

Exceptions

Exceptions to this Policy must be approved by the Information Security Team and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Definitions

Agent, for the purpose of this Policy, is defined as any third-party that has been contracted by the College to provide a set of services and who stores, processes, or transmits Institutional Data as part of those services.

Information System, is defined as any electronic system that stores, processes, or transmits information.

Institutional Data is defined as any data that is owned or licensed by the College.

Sub-Policies

01	Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Information Security Team, given the level of sensitivity, value and criticality that the Institutional Data has to the College.
02	Any Information System that stores, processes, or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Information Security Team, given the level of sensitivity, value and criticality that the Institutional Data has to the College.
03	Individuals who are authorized to access Institutional Data shall adhere to the appropriate Roles and Responsibilities, as defined in documentation approved and maintained by the Information Security Team.

Information Security Roles and Responsibilities

Date of Issuance: 12 Dec 22

Responsible Department: Office of the IT Director. Questions about this policy should be directed to the Information Security Team,

infosec@indycc.edu

Purpose

The purpose of this document is to clearly define roles and responsibilities that are essential to the implementation of Independence Community College's ("College") Information Security Policy ("Policy").

Scope

These Roles and Responsibilities apply to all faculty, staff, and third-party Agents of the College as well as any other College affiliate who is authorized to access Institutional Data.

Maintenance

These Roles and Responsibilities will be reviewed by the College's Information Security Team every 3 years or as deemed appropriate based on changes in technology or regulatory requirements.

Definitions

Agent, for the purpose of these Roles and Responsibilities, is defined as any third party that has been contracted by the College to provide a set of services and who stores, processes or transmits Institutional Data as part of those services.

Information System is defined as any electronic system that stores, processes, or transmits information.

Institutional Account is defined as any account used to manage profiles or accounts on information systems not necessarily owned or licensed by the College, i.e., social media accounts.

Institutional Data is defined as any data that is owned or licensed by the College. See the Guidelines for Data Classification for more information.

Roles and Responsibilities

The College's Information Security Policy states that, "Individuals who are authorized to access Institutional Data shall adhere to the appropriate Roles and Responsibilities, as defined in documentation approved and maintained by the Information Security Team." These roles and responsibilities are defined as follows.

Chief Information Security Officer (CISO)

The Chief Information Security Officer is a senior-level role who oversees the College's information security program. Responsibilities of the Chief Information Security Officer include the following:

1. Developing and implementing a college-wide information security program.
2. Documenting and disseminating information security policies and procedures.

3. Coordinating the development and implementation of a college-wide information security training and awareness program.
4. Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of Institutional Data.

Data Steward

A Data Steward is a senior-level employee of the College who oversees the lifecycle of one or more sets of Institutional Data. Responsibilities of a Data Steward include the following:

Assigning an appropriate classification to Institutional Data.

All Institutional Data should be classified based on its sensitivity, value and criticality to the College. The College has adopted three primary classifications: public, private, and restricted. See the Guidelines for Data Classification for more information.

Assigning day-to-day administrative and operational responsibilities for Institutional Data to one or more Data Custodians.

Data Stewards may assign administrative and operational responsibility to specific employees or groups of employees. A Data Steward could also serve as a Data Custodian. In some situations, multiple groups will share Data Custodian responsibilities. If multiple groups share responsibilities, the Data Steward should understand what functions are performed by what group.

Approving standards and procedures related to day-to-day administrative and operational management of Institutional Data.

While it is the responsibility of the Data Custodian to develop and implement operational procedures, it is the Data Steward's responsibility to review and approve these standards and procedures. A Data Steward should consider the classification of the data and associated risk tolerance when reviewing and approving these standards and procedures. For example, high risk and/or highly sensitive data may warrant more comprehensive documentation and, similarly, a more formal review and approval process. A Data Steward should also consider his or her relationship with the Data Custodian(s). For example, different review and approval processes may be appropriate based on the reporting relationship of the Data Custodian(s).

Determining the appropriate criteria for obtaining access to Institutional Data.

A Data Steward is accountable for who has access to Institutional Data. This does not imply that a Data Steward is responsible for day-to-day provisioning of access. Provisioning access is the responsibility of a Data Custodian. A Data Steward may decide to review and authorize each access request individually or a Data Steward may define a set of rules that determine who is eligible for access based on business function, support role, etc. For example, a simple rule may be that all students are permitted access to their own transcripts or all staff members are permitted access to their own health benefits information. These rules should be documented in a manner that allows little or no room for interpretation by a Data Custodian.

Ensuring that Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity and availability of Institutional Data.

The Information Security Team has published guidance on implementing reasonable and appropriate security controls based on three classifications of data: public, private, and restricted. See the Guidelines for Data Classification and the Guidelines for Data Protection for more information. Data Steward will often have their own security requirements specified in contractual language and/or based on various industry standards. Data Stewards should be familiar with their own unique requirements and ensure Data Custodians are also aware of and can demonstrate compliance with these requirements. The Information Security Team can assist with mapping controls identified in the Guidelines for Data Protection to controls mandated by contract(s) or

industry standards. can assist with mapping controls identified in the Guidelines for Data Protection to controls mandated by contract(s) or industry standards.

Understanding and approving how Institutional Data is stored, processed and transmitted by the College and by third-party Agents of the College.

In order to ensure reasonable and appropriate security controls are implemented, a Data Steward must understand how data is stored, processed and transmitted. This can be accomplished through review of data flow documentation maintained by a Data Custodian. In situations where Institutional Data is being managed by a third-party, the contract or service level agreement should require documentation of how data is or will be stored, processed and transmitted.

Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity and availability of Institutional Data.

Information security requires a balance between security, usability, and available resources. Risk management plays an important role in establishing this balance. Understanding what classifications of data are being stored, processed and transmitted will allow Data Stewards to better assess risks. Understanding legal obligations and the cost of non-compliance will also play a role in this decision making. Both the Information Security Team and the College's General Counsel can assist Data Stewards in understanding risks and weighing options related to data protection.

Understanding how Institutional Data is governed by College's policies, state, and federal regulations, contracts and other legal binding agreements.

Data Stewards should understand whether or not any College policies govern their Institutional Data. Data Stewards are responsible for having a general understanding of legal and contractual obligations surrounding Institutional Data. For example, the Family Educational Rights and Privacy Act ("FERPA") dictates requirements related to the handling of student information. The Information Security Team and the College's General Counsel can assist Data Stewards in gaining a better understanding of legal obligations.

Data Custodian

A Data Custodian is an employee of the College who has administrative and/or operational responsibility over Institutional Data. In many cases, there will be multiple Data Custodians. An enterprise application may have teams of Data Custodians, each responsible for varying functions. A Data Custodian is responsible for the following:

1. **Understanding and reporting on how Institutional Data is stored, processed and transmitted by the College and by third-party Agents of the College.**

Understanding and documenting how Institutional Data is being stored, processed and transmitted is the first step toward safeguarding that data. Without this knowledge, it is difficult to implement or validate safeguards in an effective manner. One method of performing this assessment is to create a data flow diagram for a subset of data that illustrates the system(s) storing the data, how the data is being processed and how the data traverses the network. Data flow diagrams can also illustrate security controls as they are implemented. Regardless of approach, documentation should exist and be made available to the appropriate Data Steward.

2. **Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of Institutional Data.**

The Information Security Team has published guidance on implementing reasonable and appropriate security controls for three classifications of data: public, private, and restricted. See the Guidelines for Data Classification and the Guidelines for Data Protection for more information. Contractual obligations, regulatory requirements and industry standards also play in important role in implementing appropriate safeguards. Data Custodians should work with Data Stewards to gain a better understanding of these requirements. Data Custodians should also document what security controls have been implemented and where gaps exist in current controls. This documentation should be made available to the appropriate Data Steward.

3. **Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of Institutional Data.**

Documenting administrative and operational procedures goes hand in hand with understanding how data is stored, processed and transmitted. Data Custodians should document as many repeatable processes as possible. This will help ensure that Institutional Data is handled in a consistent manner. This will also help ensure that safeguards are being effectively leveraged.

4. **Provisioning and deprovisioning access to Institutional Data as authorized by the Data Steward.**

Data Custodians are responsible for provisioning and deprovisioning access based on criteria established by the appropriate Data Steward. As specified above, standard procedures for provisioning and deprovisioning access should be documented and made available to the appropriate Data Steward.

5. **Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of Institutional Data.**

Data Custodians should have a thorough understanding of security risks impacting their Institutional Data. For example, storing or transmitting sensitive data in an unencrypted form is a security risk. Protecting access to data using a weak password and/or not patching a vulnerability in a system or application are both examples of security risks. Security risks should be documented and reviewed with the appropriate Data Steward so that he or she can determine whether greater resources need to be devoted to mitigating these risks. This Information Security Team can assist Data Custodians with gaining a better understanding of their security risks.

User

For the purpose of information security, a User is any employee, contractor, or third-party Agent of the College who is authorized to access College Information Systems and/or Institutional Data and Accounts. A User is responsible for the following:

1. **Adhering to policies, guidelines and procedures pertaining to the protection of Institutional Data.**

   The Information Security Team publishes various policies, guidelines and procedures related to the protection of Institutional Data and Information Systems. Business units and/or Data Stewards may also publish their own unique guidelines and procedures. Information on requirements unique to your business unit or a system you have access to can be found by talking to your supervisor or Technology Services.

2. **Reporting actual or suspected vulnerabilities in the confidentiality, integrity, or availability of Institutional Data to a supervisor or the Information Security Team.**

   During day-to-day operations, if a User comes across a situation where he or she feels the security of Institutional Data might be at risk, it should be reported to the Information Security Team. For example, if a User comes across sensitive information on a website that he or she feels shouldn't be accessible, that situation should be reported to the Information Security Team. Additional notifications may be appropriate based on procedures unique to a business unit or defined by a Data Steward.

3. **Reporting actual or suspected breaches in the confidentiality, integrity, or availability of Institutional Data to the Information Security Team.**

   Reporting a security breach goes hand in hand with reporting vulnerabilities. See the Procedure for Responding to a Compromised Computer for more information on what constitutes a security breach and for what steps to take if you suspect a security breach. Once again, it may be appropriate to notify a local security point of contact that will in turn coordinate with the Information Security Team.

Revision History

Status:	Published
Issuance:	12 Dec 22
Last Reviewed:	12 Dec 22
Last Updated:	