Information Security Roles and Responsibilities

Purpose

The purpose of this document is to clearly define roles and responsibilities that are essential to the implementation of the University's Information Security Policy. Article 9 - Information Technology - Part 1 Information Technology Security Plan.

Scope

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

Maintenance

These Roles and Responsibilities will be reviewed by the University's Office of Information Security every 5 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 University to provide a set of services and who stores, processes or

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

Roles and Responsibilities

The University'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 by the ESCC and maintained by the Information Security Office.” These roles and responsibilities are defined as follows.

The Senior IM&T Leadership

Are responsible for the following items:

a. Reviewing and recommending strategies to implement the Information Security Plan, Article 9.

b. Analyzing the business impact of proposed information security strategies on the University

c. Approving proposed information security strategies

Information Technology Committee

The Committee reports to both the Senior Vice President - CFO and the Senior Vice President for Academic Affairs - Provost. Faculty Senate and Student Senate representatives of the ITC enable a line of communication between the ITC, Faculty Senate, and the Student Senate. Specific oversight responsibilities related to implementation of the University of Northern Colorado Information Security Plan, Article 9 include the following:

a. Reviewing and recommending strategies to implement the Information Security Plan, Article 9.

b. Serving as a champion for accepted strategies within respective business units and/or colleges.

c.

Chief Information Security Officer

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

a. Developing and implementing a University-wide information security program.

b. Documenting and disseminating information security policies and procedures.

c. Coordinating the development and implementation of a University-wide information security training and awareness program.

d. 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 emploW nBTue approval processes may be appropriate based on the reporting relationship of the Data Custodian(s).

d. **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.

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

The Office of Information Security has published guidance on implementing reasonable and appropriate security controls based on three classifications of data: public, private and restricted. See the Policy for Data Classification and the Guidelines for Data Protection for more information. tthalaltlctedfio0.08.l 1ETEMC 4(ot TEMC 4(i)-6(e (ed)-1 (qC BTu)-2 (t)36(ed)1 (m 0 Tc 0.4

of Information Security and the Office of General Counsel can assist Data Stewards in understanding risks and weighing options related to data protection.

h. **Understanding how Institutional Data is governed by University policies, state and federal regulations, contracts and other legal binding agreements.**

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.

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

The Office of Information Security has published guidance on implementing reasonable and appropriate security controls for three classifications of data: public, private and restricted. See the Policy for Data Classification (ppu0) tmaisti (a) (ppu0) t (es)-5 (t)-6(h51(s)1 (igm0.00g

Users

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

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

   The Office of Information Security publishes various policies, guidelines and procedures related to the protection of Institutional Data and Information Systems. They can be found on the Office of Information Security website. 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 manager or system administrator.

b. **Reporting actual or suspected vulnerabilities in the confidentiality, integrity or availability of Institutional Data to a manager or the Office of Information Security.**

   During the course of 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 Office of Information Security. 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 Office of Information Security. Additional notifications may be appropriate based on procedures unique to a business unit or defined by a Data Steward. It may be appropriate to notify a local security point of contact that will in turn coordinate with the Office of Information Security.

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

   Reporting a security breach goes hand in hand with reporting vulnerabilities. Once again, it may be appropriate to notify a local security point of contact that will in turn coordinate with the Office of Information Security.

Additional Information

If you have any questions or concerns related to this Policy, please send email to the University's Office of Information Security at matthew.langford@unco.edu.

Additional information can also be found using the following resources:

- Information Security Plan, Article 9
- Policy for Data Classification
- Guidelines for Data Protection
- Procedure for Responding to a Compromised Computer

Revision History

Version	Published	Author	Description
1.0	2015/02/10	Matt Langford	Original publication.