| Procedure Title: Data: Roles, Classification, & Access Requests | Number 138 |
|---|---|
| Related Policy: Information Security and Technology Resources – 6Hx20.1.033 | Page Page 1 of 6 |

## I. Summary

Pensacola State College has established standards for the protection and security of information and for the use of information and technology resources. Information is secure only when its integrity can be maintained, its availability ensured, and its confidentiality preserved. Security procedures protect information from unauthorized viewing, modification, dissemination, or destruction, and provide recovery mechanisms in the event of accidental loss. The security of information is the responsibility of all individuals authorized to access it. All workers and partners are expected to abide by these standards.

## II. Purpose

These procedures align with the College's Information Security and Technology Resources Standards. They define the responsibilities of information owners, custodians, and users, classify various types of information, and explain how users can request access to this information. The College is committed to safeguarding customer confidentiality and worker privacy, adhering to relevant laws and personnel policies. All individuals governed by this procedure must acknowledge their understanding and commitment to adhere to these guidelines. Acknowledging this statement is mandatory to access the organization's data systems and networks.

## III. Roles

A. Information Owners

College department administrators who serve as the primary source or originators of institutional data are designated as the Owners of the information their departments generate or manage through routine business activities. These administrators are responsible for making decisions about the use and classification of that information on behalf of the College. If ownership is unclear based on the organizational structure, the Executive Director, Technology Operations, will assign the appropriate designation. It is essential to note that Information Owners do not have legal ownership of the information. Instead, they are key figures within the College's administrative team, tasked with making decisions regarding the information on behalf of the organization.

Information Owners, or their delegates, are required to make the following decisions and perform the following activities:

1. Approve information-oriented access control privileges for specific job profiles.
2. Approve information-oriented access control requests that do not fall within the purview of existing job profiles.

3. Select a data retention period for their information, relying on legal advice and Florida record schedules relevant to the College..
4. Designate a system of records for information from which all management reports will be derived.
5. Select special controls to protect information (such as additional input validation checks or more frequent backup procedures).
6. Define acceptable limits on the quality of their information (accuracy, timeliness, time from capture to usage, etc.).
7. Approve all new and different uses of their information.
8. Approve all new or substantially enhanced application systems that use their information before these systems are moved into operational status.
9. Review reports on system intrusions and other events relevant to their information.
10. Review and correct reports that indicate the job profiles currently accessing their information.
11. Select a sensitivity classification category relevant to their information and review this classification periodically for possible modification.
12. Select a critical category relevant to their information so that appropriate contingency planning can be performed.
13. Define procedures to ensure information is stored and handled by all relevant laws, regulations, and professional standards.
14. Information Owners must designate a backup person to act on their behalf if they are absent or unavailable. Owners may not delegate ownership responsibilities to third-party organizations (such as outsourced firms or consultants) or any individual who is not a full-time employee of the College. When the Owner and the backup Owner are unavailable, the Executive Director of Technology Operations may make decisions on behalf of the Owner.

Technology Operations supports Information Owners in fulfilling these responsibilities by providing technical guidance, system support, and consultation on data classification, access control, and security measures. This collaboration ensures that Owners can make informed decisions and maintain compliance with College standards and applicable regulations. Owner responsibilities are also reviewed annually during formal information security risk assessments conducted jointly by Technology Operations and the Owner’s department, offering an opportunity to evaluate practices and identify areas for improvement.

B. Supervisors

Owners are not responsible for approving routine access control requests. The user's immediate supervisor approves system access requests based on established job profiles. If a specific job profile is not available, it is the manager's responsibility to create and request approval for this profile from the relevant Owners.

Additionally, when a worker leaves the College or moves to a different department, it is the direct responsibility of their immediate supervisor to process their departure or transfer in a timely manner. This ensures that integrations can promptly revoke the individual's access privileges.

C. Information Custodians

Custodians have physical or logical control over information and information systems. They are designated for specific types of information, much like Owners. Typically, the Enterprise Solutions Department serves as the Custodian. However, if a Custodian is not apparent based on the operational arrangements of existing information systems, the Executive Director, Technology Operations, will appoint one. Custodians are tasked with executing the instructions of Owners and managing systems on their behalf while also servicing users authorized by Owners.

In situations involving paper-based information, as opposed to electronic data, the role of the Information Custodian naturally falls to the department collecting the information. The Technology Operations Department can provide advice and recommendations for such systems, but does not assume custodial responsibilities.

Custodians are responsible for outlining technical options, such as information classification, allowing Owners to choose the best fit for their data. They also define the architecture of information systems and offer technical consulting to Owners, helping to create and maintain systems that align with business goals. Upon request, Custodians provide Owners with reports on information system operations, security issues, and similar matters. Their role is critical to protecting the information under their care. This includes implementing access control measures to prevent unauthorized disclosure and developing, documenting, and testing contingency plans for information systems.

D. Information Users

Users are defined as any worker with access to internal information or internal information systems, though they are not designated individually. They must comply with all security protocols established by the Owners, enforced by the Custodians, and set by the Technology Operations team. Users are responsible for being well-informed about and acting according to the College's information security policies. Additionally, they must take part in information security training and awareness initiatives.

To access information systems, users must obtain permission from their immediate supervisor. They also must report any suspicious activities or security issues they encounter. Detailed procedures and guidelines for reporting such issues can be found in the section titled "Reporting Problems."

E. Information Security

The Technology Operations Department, specifically the Executive Director of Technology Operations or the Information Security Analyst, serves as the primary point of contact for all information security issues at the College. This department, acting as an internal technical consultant, is tasked with creating practical information security solutions that balance the needs of Users, Custodians, and Owners. They are responsible for drafting information security plans and standards, as well as related procedures and other requirements, for the entire organization. The plans and standards formulated by the department are subject to approval by the President.

Technology Operations oversees all access control management activities, monitors the security of the College's information systems, and coordinates information security training and awareness programs for College employees. They also provide management with reports on the status of information security.

The Technology Operations Department also offers technical support regarding emergency response and disaster recovery procedures. They organize the Information Security Advisory Team (ISAT) to rapidly address security incidents, such as virus infections, hacker intrusions, system failures, and other related issues.

The department plays a critical role in guiding and providing technical expertise to ensure the College's information is appropriately secured, considering the confidentiality, integrity, and availability of the information and its systems. As a liaison for information security matters among all College departments, Technology Operations is central to all information security endeavors within the organization. Their responsibilities include conducting risk assessments, developing action plans, evaluating supplier products, assisting in implementing controls, investigating security breaches, and undertaking various activities essential to maintaining a secure information handling environment. The risk assessments are conducted in collaboration with each Information Owner’s department. These assessments provide an opportunity to review the Owner’s assigned tasks, evaluate current practices, and identify areas for improvement in data classification, access control, contingency planning, and compliance with College standards and applicable laws. This process strengthens accountability and ensures that Owners have the support and insight needed to fulfill their responsibilities effectively.t.

## IV. Information Classification

College information is categorized based on its sensitivity, value, and potential impact on the College if it were to be unauthorizedly disclosed, altered, or destroyed. All College faculty, staff, and associated entities are responsible for safeguarding this information in accordance with its classification.

A. Public Data

This category includes information whose unauthorized disclosure, alteration, or destruction poses little or no risk to the College or its affiliates. Public data include course information, the College Catalog, press releases, and other materials intended for public dissemination. Basic security measures are necessary to maintain the integrity of Public Data. Generally, access to Public Data is unrestricted.

B. Sensitive Data

This classification pertains to information whose unauthorized disclosure, alteration, or destruction could result in moderate risk to the College or its affiliates. Sensitive Data encompasses information related to the College's routine business and administrative activities, which is not intended for public access. Reasonable security controls are required to safeguard the integrity and availability of Sensitive information. Access to Sensitive Data is limited to College faculty, staff, and affiliates.

C. Confidential Data

This category is for information whose unauthorized disclosure, alteration, or destruction would pose a high risk to the College or its affiliates. Any information not explicitly classified as Public or Sensitive is deemed Confidential by default. Examples of Confidential Data include, but are not limited to, student records, certain personnel records, and College donor information. Security measures for Confidential information, often mandated by law, are necessary to ensure its confidentiality, integrity, and availability. Access to Confidential Data is restricted to College faculty, staff, and affiliates who have received approval and signed confidentiality agreements.

## V. Procedures

A. Requesting Access to Reports and Data

Gaining access to Reports and Data begins through Workday's Request Framework. Typically, this procedure starts when a user's supervisor initiates the 'Create Request' task in Workday and chooses the appropriate Request Type, either 'Security Request' or 'Report Request'. Following the input and review of necessary details, the Request will proceed through the required approval channels. Upon final approval, the user will receive a notification. Detailed, step-by-step guidance for this process can be found in the Workday training section on our Technology Support Portal (https://techhelp.pensacolastate.edu) or through the Workday Help app on MyPSC.

B. Virtual Private Network (VPN)

For users requiring off-campus access to local data storage (commonly referred to as Datastore, "S" drive, or "U" drive), it is necessary to obtain access through our Virtual Private Network (VPN). Gaining VPN access mandates approval from a Vice President or the President. This process can be initiated by submitting a service request on our Technology Support Portal at https://techhelp.pensacolastate.edu.

C. Network & Cloud Storage Access (Datastore & Email/Teams Groups

To initiate the creation of new data storage locations, you can start the process by submitting a service request on our Technology Support Portal, accessible at https://techhelp.pensacolastate.edu. Upon receiving the request, Systems Support will contact the requester to analyze the needs presented. They will provide recommendations and assist in effectively addressing data storage requirements, documenting data Owners, and classifying data.

D. Modifications to Network & Cloud Storage (Datastore & Email/Teams Groups)

The data Owners approve requests for access to data. To initiate the modification of users to existing data storage locations, you can start the process by submitting a service request on our Technology Support Portal, accessible at https://techhelp.pensacolastate.edu. Upon final approval, the user will receive notification and instructions on how to access the data.

E. Reporting Problems

All workers are responsible for reporting suspicious activity and security issues regarding College information. All workers are expected to assist in maintaining the confidentiality, integrity, and availability of the data. Workers of the College should report information security-related issues by contacting the Executive Director, Technology Operations, directly or via the Technology Support Desk at 850.484.1702

| | |
|---|---|
| Responsible Official | Executive Director, Technology Operations |
| President's Signature: | Date: 10/14/2025 |