4-5011 Information Security

This Regulation provides an overview of various College policies and procedures that pertain to access of College data and information, and aims to define the overall information security structure which will insure the confidentiality, availability, and integrity of all College data and information systems. This Regulation establishes the structure and processes applicable to the College to ensure compliance with any applicable federal and state laws regarding information that is transmitted, stored, and managed by the College's Office of Information Technology (IT).

This regulation applies to all members of the College that require or request access to College information, including but not limited to staff, faculty, students, contractors, alumni, and volunteers. College data are classified into three (3) categories according to sensitivity of the data.

(1) Definitions

(a) Confidential/PII (Personally Identifiable Information). Confidential/PII is data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or College contracts (i.e., protected data); personally identifiable data; data that involves issues of personal privacy; or data whose loss, corruption or unauthorized disclosure may impair the academic, research or business functions of the College, or result in any business, financial, or legal loss. Examples of data classified as confidential include but are not limited to: social security numbers, bank account numbers, driver license numbers, student records protected by FERPA, or health records as protected by HIPAA. This information is held with the highest level of security. Only individuals with a business need will be granted access to confidential information.

(b) Sensitive Information. Sensitive Information is information that is not necessarily governed by state and/or federal laws but may still have a negative result on an individual or the College if it is obtained by someone not intended to receive the data. Examples of sensitive information include but are not limited to non-academic record information of current students or alumni. Great care should be given to providing access to sensitive information and will only be done so to support the business function of the College.

(c) Public Information. Public information is all other information that is not considered confidential or sensitive as specifically defined by Florida's Public Records laws.

(2) Policies and Procedures. The College shall develop policies and procedures to address information security. Below are the defined areas in which security controls for College data are applied.

(a) Physical Security of computing and paper resources are addressed by each department and their respective policies. Access to network and server data rooms are controlled and monitored by IT personnel. The rooms are secured with electronic door locks and access logs are maintained. The data rooms are also monitored with a recorded camera system.

(b) Personnel Security Checks and Screening is administered by the College's Human Resources Department. All faculty and staff offered employment at the College and all current employees in positions of "special trust" are required to complete a security background check and fingerprints

screening per Regulation 3-4003 Employee Security Checks and Screening.

(c) Logical Security to data resources is maintained by IT staff. Access to data is controlled on the basis of "least privilege", need to know, and separation of duties. Adequate security must be provided to ensure the protection and maintenance of integrity, confidentiality, and availability of the systems and information.

(d) Disaster Recovery and Planning. The College shall develop and maintain a current plan for dealing with emergency situations in the event of damage, failure, and/or other disabling events that could impact the critical business and academic processes of the College.

(e) Security Incident Response. The College shall develop and maintain a current plan for dealing with security events that may require the full participation of the IT personnel and College leadership to manage the outcome properly. See Incident Response Policy

(f) Security Awareness and Training. The College shall establish and maintain security awareness training program for staff and faculty.

Authority: Article IX, Sec. 7, Fla. Constitution; Fla. Board of Governors Regulations 1.001 and 3.0075

History: Adopted 09-08-12; Revised 02-24-17 (technical amendment)