NEW COLLEGE OF FLORIDA
REGULATIONS MANUAL

CHAPTER 4 - Academic Affairs

4-5003 Information and Communication Security Program

(1) Purpose. The purpose of this Regulation is to establish an Information and Communication Security Program in accordance with Chapter 282.318, Florida Statutes, also known as the “Enterprise Security of Data and Information Technology Act." The regulation is intended to ensure that NCF is in compliance with the Act; that only authorized employees are given access to information technology systems and resources (“information technology”); and that employees who are terminated or transferred will not retain information technology access privileges.

(2) Scope. An information and communication security program is not limited solely to technology. While technology will be a part of the program, other areas such as personnel; environment; utilities; purchasing practices; and public safety will also play a part. This program applies at NCF and to information and information technology systems when used remotely from the NCF location. This regulation shall also apply in cases of an employee leave of absence and other situations where access privileges may need to be suspended.

(3) Adoption of Operating Standards and Procedures. All information utilized in the course of business and education at NCF is considered an asset, and as such, administration, faculty, staff and students are responsible and accountable for its viability and protection. It is a management responsibility to maintain information security and integrity through administration of appropriate legal, auditable controls to protect NCF information from unauthorized, intentional or accidental disclosure, modification, destruction, denial, or misappropriation.

The Director of Technology Support is NCF’s designated Information Security Officer (ISO) Information and communication security shall be the operational responsibility of the ISO and responsibility for developing and coordinating the security program shall rest with the ISO.

Operating standards and procedures shall be adopted with the approval of the President, and shall address the following areas:

(a) Physical Environment. This includes protecting physical facilities, such as buildings, other structures or vehicles that house information technology system and network components. Physical and environmental standards and procedures must also include provisions for addressing natural threats such as hurricanes; man-made threats such as theft; environmental threats such as toxic chemical spills and physical threats such as fire, roof leakage or power outages.

(b) Data and Software. This includes controlling and protecting data and software from damage or unauthorized use; ensuring departmental data use is in compliance with all necessary standards such as Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Electronic Communication Privacy Act (ECPA), and Gramm-Leach-Biley Act of 2000 (GLB); ensuring that data confidentiality, integrity and accuracy are appropriately safeguarded; and ensuring that only legally obtained and licensed software is being installed and used.

(c) Physical Access. This includes establishing who is permitted access to secured areas where information technology systems and network components are housed and the means by which access will be granted and terminated. These standards and procedures will also define the degree of access controls required such as locks, special keys, biometric access devices, alarm systems, monitoring devices and/or closed circuit cameras.

(d) Logical Access. This includes establishing who has authorization to log into information technology databases, application systems, operating systems, servers and network components and the means by which access will be granted and terminated. This also includes maintaining and updating standards for password or PIN complexity, length, and expiration span as future needs may dictate.

(e) Records Management. This includes controlling access and managing risks to the physical safety, confidentiality, integrity, accuracy and security of permanent records within each department which are maintained electronically on campus servers or hosted servers collocated co-located at other sites.

(f) Communication. This includes defining what, how, where, when and by whom necessary and relevant information will be distributed or made available to NCF staff, faculty and students regarding IT availability, outages, down time, maintenance, upgrades and problems both scheduled and unscheduled.

(4) Accountability. Deans, Directors, Department Heads, and Division Chairs shall be responsible for ensuring that operating standards and procedures established in accordance with this regulation are adhered to within their respective areas.

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

History: Adopted 03-05-11; Revised 03-02-17 (technical amendment)