CHAPTER 4 - Academic Affairs

4-5001 Use and Protection of Information Technology Resources

Advances in technology have enabled the implementation of a substantial number of desktop and computer-based application systems by NCF. These applications have become critical to the operation of NCF. It is essential, therefore, that adequate measures be used to protect the integrity and reliability of those computing systems and the NCF data they process. Each department must cooperate in ensuring a level of protection not only appropriate for the computers, mobile computing, communication, and data storage devices in its own environment, but also with regard to the level of protection used for the larger campus networks of which it may be a part.

NCF acquires, develops, and maintains software, computers, computer systems, and networks for NCF-related purposes as part of its infrastructure. NCF's computing resources and infrastructure are made available to users in support of NCF's instructional, research, community service missions, its administrative functions, its student and campus life activities, and to promote the free exchange of ideas among members of the NCF community and between the NCF community and local, national, and international communities. This Regulation governs the use of NCF computing resources and infrastructure and applies to all users of NCF's computing resources and infrastructure, whether or not affiliated with NCF, and also to all uses of those resources, whether from on campus or from remote locations. Users of these resources and infrastructure are responsible for reading and understanding this Regulation.

(1) Purpose. The purpose of this Regulation is to protect the computing resources and mobile computing, communications, and data storage devices of NCF by authorizing NCF's Office of Information Technology ("IT") to adopt operating standards and procedures upon recommendation of the Technology Advisory Committee and the President. This Regulation applies to all NCF and department computers, mobile computing, communications, and data storage devices, and includes the hardware, software, and NCF data used with these devices.

(2) Scope. Protecting NCF's ability to conduct its business extends beyond basic procedures for handling, storing, and disposing of information. This Regulation relates to NCF's Office of Information Technology and steps that it will take to protect computing resources.

(3) Definitions. As used herein, the following terms shall have the indicated definition:

(a) "Data" shall mean a collection of organized information, usually the results of experience, observation, or experiment, or a set of premises. This may consist of numbers, words, or images, particularly as measurements or observations of a set of variables.

(b) "Mobile Communications Device" shall mean cellular telephones, smart phones, and mobile computing devices equipped with wireless or wired communication capability.

(c) "Mobile Computing Device" shall mean laptop computers, tablet PCs, personal digital assistants, and similar mobile electronic devices that are capable of storing, processing, displaying, and communicating data.

(d) "Mobile Data Storage Device" shall mean USB storage devices, CD-ROMs, DVDs, mobile music players, and any other mobile electronic device or medium that is capable of storing data.

(e) "Academic Network" shall mean a network, separate from the campus administrative network, managed by an academic division for the purposes of teaching and research.

(f) "Administrative Network" shall mean those networks managed by NCF Office of Information Technology.

(4) Adoption of Operating Standards and Procedures. The Office of Information Technology shall be responsible for establishing, maintaining, and deploying appropriate operating standards and procedures NCF-wide to protect the computing resources under its control, including but not limited to computer software, desktop computers, mobile computing, communications, data storage devices, and the campus administrative network. Standards and procedures shall be adopted upon recommendation of the Technology Advisory Committee and the President, and address the following areas.

(a) Risk Management

1. Data Security. This includes defining user responsibilities to protect and safeguard user identifications and passwords, providing the means by which employees can remotely access sensitive or confidential resources from insecure networks such as wireless and public internet service providers. In addition, the disposition of NCF computing resources in the possession of terminated employees shall be addressed. Standards and procedures shall be developed, established, and maintained for the protection of confidential data against unauthorized access, regardless of form, computing environment or location. This shall include the use of mobile computing, communications, or data storage devices to store sensitive or confidential data as well as the management of data residing on the hard drives of any equipment that is transferred or surplused.

2. Standards and procedures shall also be established to control access to the administrative and academic data networks, as needed, to prevent unauthorized access to networks, computers and data, and to minimize intrusions and attacks by various types of malware. Individual departments, divisions, or other discrete operating units within the College may define "conditions of use" for academic networks under their control. These statements must be consistent with this overall Regulation, but may provide additional detail, guidelines, and/or restrictions including specifying the type of data that will be contained on the network, identifying data that is considered sensitive or confidential, granting and removal of access, management of systems and services, troubleshooting problems, compliance with NCF Regulations and state and federal audit guidelines and/or creating procedures that will act as compensating controls, and initiating disciplinary action against those responsible for inappropriate activity related to the academic network. These individual departments, divisions, or other discrete operating units are responsible for publicizing both the Regulations they establish and their policies concerning the authorized and appropriate use of the network for which they are responsible.

3. Equipment Protection. This includes reducing the risk of physical loss, damage, or theft to campus-based computer equipment and components, as well as mobile computing, communications, and data storage devices.

(b) Software Integrity. This includes managing computer application software and ensuring that any software installed on NCF equipment has been legally obtained.

(c) Business Continuity Planning. This includes assisting NCF's Risk Management Officer with ensuring that each division, unit, or department is prepared for the restoration and continuation of critical services in the event of a significant disruption of normal computer operations.

(d) Training. This includes defining training requirements for employees in the proper use and protection of desktop and mobile computer resources. These requirements shall also address provision and availability of appropriate hardware and software reference materials for employees.

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

(6) Communicating Technology Operating Standards and Procedures. The Office of Information Technology will be responsible for posting and maintaining all relevant information technology operating procedures on the Office of Information Technology campus portal page.

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

History: Adopted 04-27-02, as Policy 0-501; Revised and renumbered 09-13-08; Revised 06-29-10, 03-05-11, 05-12-12, 02-24-17 (technical amendment)