NJCU
NEW JERSEY CITY UNIVERSITY

Section Number _____ Section Header: _____

Subject: Information Security Policy _____ Effective Date: _____

Responsible Office: Department of Information Technology Responsible Officer: Director of IT

TABLE OF CONTENTS

INTRODUCTION

The use of information technology (IT) in universities has created new administrative concerns, challenges and responsibilities. Organizational data and the technologies that provide access to that data must be protected from natural disasters and human threats. The focus of information security is to ensure protection of information and continuation of university operations.

Department of Information Technology provides convenient, comprehensive access to campus computing resources and data to authorized users. Security for data retrieval, computing and communications systems is an important issue on the New Jersey City University (NJCU) campus.

Preventing unauthorized access to any microcomputer system should be of utmost concern to all university personnel.

PURPOSE

This document outlines policies and practices that must be followed to ensure that risks are lessened or their effects mitigated. It is designed to assure the necessary security is created and managed in such a

way as to accommodate legitimate users of NJCU's network, desktop computers, servers and systems. Procedures must also be implemented to maintain compliance with Federal and State laws governing rights to privacy, computer systems protection and unauthorized disclosure of data.

SCOPE

All Deans, Directors, and Department Heads are responsible for the security of information resources in all offices under their jurisdiction and for implementing information security requirements on an office- wide basis. However, individual users have a responsibility to manage NJCU-owned personally identifiable information stored on their computers, regardless of who owns the computing device the data is stored on.

DEFINITIONS

Personal Computer

Within context of this policy, a personal computer is any desktop or laptop computer that contains personal or private information owned by NJCU.

Personally Identifiable Data

Personally identifiable data is any information provided by the student or employee that can be used to personally identify the individual.

Data Custodian

The data custodian is the unit or person assigned to supply services associated with the data. The custodian is:

- The unit (Department of IT) provides centrally supported administrative applications including backups and recovery or access to the campus network infrastructure.
- The operator or manager of a departmental computer system, server, or network of microcomputer workstations.
- The end-user of an individual microcomputer workstation.

Data User

The data user is the person who has been granted explicit authorization to access the data by the owner.

POLICY

The person assigned university owned computing hardware assumes full responsibility for the safekeeping of both the hardware and software. Acknowledgement of this responsibility is provided by completing the Data Confidentiality Form.

Upon termination of faculty or staff, the direct supervisor of the terminated employee will initiate network access account termination with Department of IT within 24 hours. Non-administrative data is owned by the department or project that creates and maintains the data or the person (faculty, staff or enrolled student) assigned to the login-ID associated with the data. In the event the data owner is no longer enrolled or employed at Armstrong, the data owner or Department Head must provide explicit authorization for other persons to access the data. Otherwise, data ownership will remain with the person assigned to the login-ID associated with the data or the data custodian may archive the data according to established operational and data archival procedures.

The administrative department having primary responsibility for creation and maintenance of the data content owns administrative data.

Custodian Responsibilities

- The custodian provides services in accordance with the directions from the owner and is responsible for:
- Provides a general security access system.
- Insures compliance of data users with security procedures.

Data User Responsibilities

- Use the data only for purposes specified by the owner.
- Comply with security measures specified by the owner or custodian (i.e. securing login-ID and password).
- Not disclose information or control over the data unless specifically authorized in writing by the owner of the data.

Hardware Security

The room(s) in which computers are kept should be locked when not in use. If this is not possible, consideration should be given to using a cable lock or other device to deter removal of the desktop unit. All transportable computers should be kept in a safe place at all times, including when such devices are in transit. Portable (laptop, notebook, etc.) computers must be handled as carry-on luggage when using public transportation.

If a desktop unit, peripheral device or other computing equipment is moved to a new permanent location or discarded, the department requesting the move or surplus must inform the Controller's Office and submit a completed Equipment Transfer form.

Data on equipment to be discarded must be destroyed.

KEY PERFORMANCE INDICATORS

The following success of the policy will be assessed annually using the following quantifiable measures:

1. All accounts belonging to students an employees no longer affiliated with the university are removed.
2. Spot checks verify that discarded computer hard drives have been wiped clean of data.

PROCEDURES

Accessing Data

All members of the university community who handle data must complete and sign the NJCU Data Confidentiality Form and submit it to the HR department before being granted access.

Moving Computer Inventory

Fill out and submit the Equipment Transfer form.

Destruction of data

All personally identifiable data should be deleted using an electronic shredder, set to a minimum of six passes. Discarded hard drives should be wiped out using the same shredding software for the data, then reformatted at the partition level.

CONTACT

This policy is managed by:

University Title: Director of Information Technology

Location: Rossey Hall, Room 58
Telephone: (201) 200-3350
Facsimile: (201) 200-2332
Email: itspolicies@njcu.edu

RELATED TOPICS

Policies

- Computer Disposal Policy
- Departmental Data Backup
- Policy Information Privacy
- Policy Information Disclosure Policy
- Peer-2-Peer Policy

Guidelines and Support Materials

- Subpoena & Warrant Processing Guidelines
- Desktop Security Guidelines
- Downloads & Executables
- Guidelines Virus Prevention Guidelines
- Software Installation Procedures

External References

- Gramm-Leach-Bliley Act of 1999

FORMS

- Data Confidentiality Form
- Equipment Transfer Form

Note: All documents and forms are available from the Department of IT website, Documents page and the University Policy website page.