NJCU
NEW JERSEY CITY UNIVERSITY

Section Number _____ Section Header: _____

Subject: **Information Privacy Policy** Effective Date: March 2003

Responsible Office: Department of Information Technology Responsible Officer: _____

TABLE OF CONTENTS

INTRODUCTION

New Jersey City University cherishes the diversity of values and perspectives endemic in an academic institution and so is respectful of freedom of expression. The University does not condone censorship, nor does it endorse the systematic inspection of electronic files or monitoring of network activities related to individual activities. However, there are legitimate reasons for persons other than the account holder to access computer files or computers or network traffic: ensuring the continued integrity, security, or effective operation of University systems; to protect user or system data; to ensure continued effective departmental operations; to ensure appropriate use of University systems; or to satisfy a lawful court order.

PURPOSE

An NJCU employee, consultant, or contractor (designated as "employee(s)") as part of the nature of their work may encounter confidential information, particularly through the use of University computing facilities. Such confidential information may include academic records, compensation and other financial information. Personnel engaged in NJCU authorized activity shall not access, acquire, use, copy, or transfer confidential information except to the extent necessary to fulfill their assigned duties and responsibilities. Improper access to or unauthorized disclosure of confidential information may be a violation of federal law and could result in, among other things, loss of all federal financial assistance to the University.

SCOPE

This policy applies to all New Jersey City University faculty, students, and staff, including employee supervisors and administrators, computer and network technicians, and contracted workers who have been assigned the task of maintaining New Jersey City University information technology systems in central campus computing center, the data network, or in departments.

This policy covers:

- Data and other files, including electronic mail and voice mail, stored in individual computer accounts on University-owned centrally-maintained systems;
- Data and other files, including electronic mail and voice mail, stored in individual computer accounts on systems managed by the University on behalf of affiliated organizations (e.g., the Alumni Association);
- Data and other files, including electronic mail or voice mail, stored on personally-owned devices on University property (e.g., residence hall rooms);
- Data and other files, including electronic mail or voice mail, stored on University-owned computers assigned to a specific individual for their use in support of job functions; and
- Telecommunications (voice or data) traffic from, to, or between any devices described above.

POLICY

Employees shall take all appropriate action, whether by instruction, agreement or otherwise, to insure the protection, confidentiality and security of confidential information. Persons who exceed their authority in using confidential information or who gain access to such information through unauthorized means, including the use of University computing facilities, should realize that their conduct is in violation of University policy and will be dealt with accordingly. Such conduct may also be in violation of state and federal law.

Stored computer information, voice and data network communications, and personal computers may not be accessed by anyone other than the person to whom the computer account in which the information has been stored is assigned, or from whom the communication originated, or to whom the device has been assigned, outside of the provisions of this policy.

The University considers any violation of appropriate use principles to be a serious offense and reserves the right to copy and examine any files or information resident on University systems allegedly related to inappropriate use. Violators are subject to disciplinary action including loss of all University computing privileges and possible criminal charges including civil damages. Offenders also may be prosecuted under various state & federal laws including (but not limited to) the Privacy Protection Act of 1974,The Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication of 1989, Interstate Transportation of Stolen Property, and the Federal Electronic Communications Privacy Act. Access to the texts of these laws is available through the Reference Department of the Library. Violators may also cause the University to be liable to civil or criminal penalties.

KEY PERFORMANCE INDICATORS

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

1. Permissions and rational for emergency access documented per issue.
2. No breaches of privacy

PROCEDURES

A technician or administrator may access or permit access to the resources described above, if he or she

1. Has written (verifiable email or paper) permission from the individual to whom the account or device or communication has been assigned or attributed; or
2. In an emergency situation, has a reasonable belief that a process active in the account or on the device is causing or will cause significant system or network degradation, or could cause loss/damage to system or other users' data; or
3. Receives a written request from the senior executive officer of a department to access the account of a staff or faculty member who is deceased, terminated, or is otherwise incapacitated or unavailable, for the purposes of retrieving material critical to the operation of the department; or
4. Receives a written request from the appropriate campus Dean of Students or equivalent, on behalf of the parents or estate manager of a deceased student; or
5. Receives a written authorization from the appropriate campus Dean of Students or equivalent, for situations where there is reasonable belief that a student to whom the account or device is assigned or owned has perpetrated or is involved in illegal activities using the accounts or device in question; or
6. Receives a written authorization from the appropriate campus Dean of Students or equivalent, for situations where there is reasonable belief that a student to whom the account or device is assigned or owned has perpetrated or is involved in violations of University policy using the accounts or device in question; or
7. Receives a directive from the Director of Internal Audit when Audit staff are engaged in investigations of fiscal misconduct;

In the event that University officials are notified of a University or law enforcement investigation for alleged misconduct or illegal activity on the part of a member of the NJCU community, contents of an individual's e-mail, other computer accounts, office computer, or network traffic may be copied and stored to prevent destruction and loss of information, pending formal review of that material. Subsequent release of the stored materials must be in accordance with the above-specified criteria.

Except when inappropriate or impractical, all efforts will be made to notify the involved individual prior to accessing the computer account or device, or before observing network traffic attributed to them. Where prior notification is not appropriate or possible, all efforts will be made to notify the involved individual as soon after

Transgression of policy should be reported to the Department of Information Technology.

RELATED DOCUMENTS

- Responsible Use of Computing Resources
- General Principles and Guidelines
- Email as Official Communications