THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Rutgers Policy

Section: 50.3.9

Section Title: Legal Matters

Policy Name: Identity Theft Compliance Policy

Formerly Book: N/A

Approval Authority: Executive Vice President for Academic Affairs and Senior Vice President and Chief Financial Officer

Responsible Executive: Vice President for Information Technology

Responsible Office: Office of Information Technology

Originally Issued: 7/24/2006

Revisions: not applicable

Errors or changes? Contact: oitpolicy@rutgers.edu

1. Policy Statement

It is the university's policy to protect personal information it receives, handles, and stores, and to comply with the "New Jersey Identity Theft Prevention Act." Therefore, any breach of security or compromise of systems containing personal information must be reported immediately to the Office of Information Protection and Security (IPS) and the local unit head. Based on the nature of the breach and the information involved, the compromise will be evaluated by the Information Protection Evaluation Team (IPET) and a decision made regarding notification in accordance with the New Jersey Identity Theft Prevention Act.

The university will collect personal information about individuals only if permissible by law and university policy and when it meets appropriate business purposes. In the event of a security breach involving personal information, any required notifications will be carried out in accordance with New Jersey law and university policy.

2. Reason for Policy

To ensure university compliance with the New Jersey Identity Theft Prevention Act, which went into effect on January 1, 2006 (L.2005, C226).

To assist in both the prevention and detection of identity theft by outlining guidelines for collecting, retaining, and restricting access to personal information.

3. Who Should Read Policy

- Provosts and vice presidents
- Deans, directors, chairs, and department heads
- University administrators

- ♣ Administrative staff
- ♣ Financial staff
- ♣ Technical Staff
- ♣ Anyone granted access to Rutgers University data

4. **Related Documents**
New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 through 56:8-166

Identity Theft Reporting Guidelines

5. **Contacts**
Information Protection and Security Office
732/445-8011
rusecure@rutgers.edu

6. **The Policy**

50.3.9, IDENTITY THEFT COMPLIANCE POLICY

I. Reporting Security Breaches

Any unit or individual aware of a potential breach of security or compromise of systems containing personal information must immediately report the potential breach of security or compromise of systems to the Office of Information Protection and Security (IPS) and the local unit head.

A. Definitions

1. A breach of security means the unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information.

2. Compromise of systems means an apparent exploit of a vulnerability in system software, hardware or a procedural weakness that may provide unauthorized access to the system environment.

3. Personal information includes, but is not limited to:
   - Individual names
   - Social Security numbers
   - Credit or debit card numbers
   - State identification card numbers
   - Driver's license numbers
   - Dates of birth
   - Health records when the disclosure of the information in question would reasonably be considered to be harmful or an invasion of privacy

B. Evaluation and Response to Reported Security Breaches

IPS will make an initial evaluation of the report to determine if the matter requires referral to the Information Protection Evaluation Team (IPET). This team will then conduct fact finding concerning the potential breach of security or compromise and prepare a written report assessing whether personal information is reasonably believed to have been accessed by an unauthorized person and if misuse of this information is reasonably possible. The IPET report will include a recommendation concerning the university's responsibility to provide notification under the New Jersey Identity Theft Prevention Act (Act) and the form of any such recommended notification. This report and recommendations will be directed to the Executive Vice President for Academic Affairs, the Senior Vice President and Chief Financial Officer, and other senior staff in accordance with the Identity Theft Reporting Guidelines.

The Executive Vice President for Academic Affairs and the Senior Vice President and Chief Financial Officer shall make the final determination regarding notification. This notification shall be made in the most expedient time practical and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification will be made in accordance with the Identity Theft Reporting Guidelines.

II. Requirements for Collecting, Retaining, and Restricting Access to Personal Information

A unit or individual may compile or maintain personal information if required by law or for valid business purposes. In so doing, the unit or individual is accountable and will be held responsible for adhering to the following guidelines:

A. A Unit or Individual Shall:

- Maintain this information in a secure fashion in accordance with industry best practices (see http://rusecure.rutgers.edu/ for guidance).
- Destroy, or arrange for the destruction of, personal information when there no longer is a legal or business purpose for retention of this information and in conformity with all applicable records retention policies.
- Restrict access to personal information to only those persons needed to maintain systems, maintain data, meet legal requirements or perform valid business functions.

B. A Unit or Individual Shall NOT:

- Publicly post or publicly display, or intentionally communicate or otherwise make available to the general public any personal information.
- Require an individual to send personal information over the network unless it meets a valid business purpose and a secure network transmission is used.
- Transfer data containing personal information to another unit, private entity or public entity over the network unless it meets a valid business purpose and a secure network transmission is used.
- Mail personal information on a post card or on any other mailer not requiring an envelope. Mailed personal information must not be printed on the envelope or visible within the envelope without it being opened.
- Require an individual to use his or her Social Security number to access an Internet web site or other network resource, unless a password or unique personal identification or other authentication device is also required to access the site or resource.
- Display a Social Security number as entered to access an Internet web site or other network resource.
- Print an individual's Social Security number on any materials that are mailed to the individual unless required by law, or as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm accuracy of the Social Security number.

- Print an individual's Social Security number on any card required for the individual to access products or services provided by the university.