1. **Policy Statement**
The university collects personal information about individuals only if permissible by law and university policy and when it meets appropriate business purposes. It is the university's policy to protect personal information it receives, handles, and stores in all instances, and to comply with laws pertaining to the safeguarding of personal information, including the New Jersey Identity Theft Prevention Act. In accordance with this policy and implementing guidelines, the university community must be educated and vigilant about requirements for collecting, retaining and restricting access to personal information and identifying potential security breaches (i.e. incidences where personal information may have been accessed by unauthorized persons), and reporting such security breaches to appropriate university personnel for immediate evaluation and action. The university shall be committed to carefully and expeditiously investigating potential security breaches. In situations where notification to potential victims of security breaches is determined to be required by law or otherwise appropriate, the university shall do so in the most expedient time possible and without unreasonable delay.

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 This Policy**
All Rutgers staff and faculty, whether full-time or part-time, and all others internally and externally who are granted access to university data.
50.3.9 SAFEGUARDING PERSONAL INFORMATION; IDENTITY THEFT COMPLIANCE POLICY


A. Definitions

1. “Breach of security” means the unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the university for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to university business or subject to further unauthorized disclosure.

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” in context of a “breach of security” - personal information means an individual’s first name or first initial and last name linked with any one or more of the following data elements: (i) social security number; (ii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account, (iii) State identification card number, (iv) driver’s license number, (v) date of birth. It also means health records when the disclosure of the information in question would reasonably be considered to be harmful or an invasion of privacy.

4. “Undue Delay” shall mean without unreasonable delay under the circumstances.

B. Education and Awareness

It is the policy of the university to educate the university community about the requirements for collecting, retaining, and restricting access to personal information including the identification and reporting of potential security breaches and university policies and guidelines related thereto. IPS, as part of its security awareness program, will incorporate information that promotes awareness of these issues. This shall include the issuance of periodic notices to the university community of this policy and useful information regarding how to protect personal information, identify potential breaches of
security and the immediate required steps that must be followed. Examples of potential security breaches that may contain personal information include: a stolen laptop or smartphone, a compromised desktop or server, a successful phishing attempt for a netid and password, a compromised web application or database.

C. Reporting Security Breaches

Any unit or individual aware of a potential breach of security containing personal information must immediately report the potential breach of security to their supervisor or unit head and the Office of Information Protection and Security (IPS) at 848-445-8011 or rusecure@rutgers.edu.

D. Investigation of Reported Security Breaches

Without undue delay, upon receiving notification of a report, IPS shall make an initial evaluation and determine if it is possible that there has been a breach of security. If IPS determines that it is possible that there has been a breach of security, it shall expeditiously refer the matter to the Information Protection Team (IPET). IPET shall be comprised of the following individuals and representatives of the following offices:

- Director of the Office of IPS (shall serve as Chair of IPET)
- Director of Privacy
- Office of the Senior Vice President and General Counsel
- Office of Student Affairs
- Office of the Registrar
- Newark Chancellor Designee
- Camden Chancellor Designee
- RBHS Chancellor Designee

The IPET also may be advised by or seek advice from representatives of the following units as needed:

- Rutgers University Police Department
- Risk Management Department
- Unit in which the incident occurred
- University Communications and Marketing
- Any other unit or department that the IPET determines may provide assistance

Without undue delay, and upon receiving a referral from IPS, the Chair of IPET shall convene a meeting to expeditiously conduct a fact-finding investigation concerning the potential breach of security or compromise of systems. All members of IPET are required to participate in the meeting, but the excused absence of any members should not delay the meeting or the investigation. IPET is encouraged to speak directly to persons who may have information regarding the matter being investigated (e.g., data owners). The investigation shall conclude without undue delay.

In conducting its investigation, members of IPET and any others assisting IPET, may be required to obtain and review personal information in electronic or hardcopy format related to the incident. Extreme care and caution should be used to ensure that such personal information is protected and that there are no further security breaches resulting from the investigation.

During the course of an investigation, the IPET committee has the authority to provision additional internal or external services, such as computer forensics, to help determine whether it was possible that an exploit of a vulnerability led to the exposure of protected information.
E. Report of IPET and Recommendation

1. Without undue delay, upon the conclusion of the investigation, the Chair of IPET shall oversee the preparation of a written report which shall include IPET’s: (i) factual findings, (ii) evaluating whether there has been a security breach, iii assessing whether the release of personal information is reasonably believed to have been accessed by an unauthorized person and if misuse of this information is reasonably possible, (iv) reasoning as to whether notification to potential victims of the security breach is required or appropriate, (v) if notification is required or appropriate, a proposal regarding the form, scope and manner of notification, and (vi) final recommendation.

2. The Chair of IPET shall forthwith submit the written report and recommendation to the Senior Vice President for Administration and Executive Vice President for Academic Affairs, and members of IPET shall make themselves available to answer any questions about the investigation and report. A copy of the report will be made available to the unit head from where the breach occurred, the head of internal audit, and the IPET members.

3. The Executive Vice President for Academic Affairs and the Senior Vice President for Administration shall make a written final determination regarding notification without undue delay.

F. Notification; State Police; Form; Method and Manner; Post Incident Review

1. Prior to effecting any notification and without undue delay, the Chair of IPET with the assistance of Rutgers Police shall report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigating and handling, which may include dissemination or referral to other appropriate law enforcement entities.

2. The notification shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies the university.

3. In cases where notification of more than 1,000 persons at a time is required, the Chair of IPET in conjunction with the appropriate Rutgers supportive staff shall also provide notification to all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis as defined by the federal "Fair Credit Reporting Act".

4. Units from which a security breach arises out of shall in coordination with other supportive units (e.g. Registrar, Alumni relations, Human Resources) be responsible for making notifications without undue delay. They should seek the assistance of IPS during the notification process. Once the notification is complete, Units must provide the chair of the IPET committee with the following for institutional record retention:

   a. a list of the individuals notified, date and method of notification
   b. a copy of the notification letter
   c. the name and title of the university official responsible for managing the notification process

5. Any notification shall whenever practicable take the form of the university’s draft notification letter, last revised 3/6/09. See http://rusecure.rutgers.edu/content/draft-breach-notification. The notice should,
at a minimum, advise the recipients of the breach of security, that the matter has been investigated by the university and has been reported to the State Police, provide steps that the recipient may take to protect themselves, and provide contact information pertaining to credit check agencies.

6. It is of paramount importance to deliver the notice in a manner designed to securely reach the intended recipients without undue delay. To that end, depending on the circumstances, the university will ordinarily use written notice or e-mail, but may also use such methods as posting information on a public webpage, or in university or statewide media.

7. In the case of reported breaches, whether notification is required or not, internal audit will review and consult with the unit head to determine whether or not any material weaknesses existed in the controls and processes leading to the breach, and suggest improvements to minimize future events.

G. Record Management

The Chair of IPET shall maintain the records pertaining to each reported incident for a period of no less than five (5) years. Those records shall include at a minimum electronic or hard copy documents concerning the initial report, investigation record, report and recommendation, final determination, report to State Police, response of the State Policy, and notification record if any (written notices and list of recipients).

H. Annual Report on Compliance

The Annual Report on Compliance to the Audit Committee of the Board of Governors, shall include a section reviewing and assessing the university's compliance with this policy and provide any recommendations for strengthening its efforts and processes in this area.

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)
- 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.