1. **Policy Statement**

   Each person with access to the Rutgers, The State University of New Jersey, computing resources is responsible for their appropriate use and by their use agrees to comply with all applicable University, School, and departmental policies and regulations, and with applicable State and Federal laws and regulations.

2. **Reason for Policy**

   This policy sets forth the acceptable uses regarding the access and use of the University's electronic information and information systems.

3. **Who Should Read This Policy**

   This policy applies to any individual responsible for the management, operation, and/or maintenance of the legacy UMDNJ information technology services and/or environment. If you are uncertain whether this policy applies to you, please contact your direct supervisor.

4. **Related Documents**

   N/A

5. **Contacts**

   oithelp@rutgers.edu

---

All regulations and procedures are subject to amendment.

Page 1 of 6
6. **The Policy**

70.2.8 **INFORMATION SECURITY: ACCEPTABLE USE**

Users are given access to Rutgers’ electronic information and information systems specifically to assist them in the performance of their jobs and education. They are not provided for personal use. They are responsible for all activity conducted using their computer accounts. Access and use of the University’s electronic information and information systems is a revocable privilege.

The University expects users will access and use the University’s electronic information and information systems in a manner that:

- Does not compromise the confidentiality, integrity, or availability of those assets; and
- Reflects the University’s standards as defined in the Code of Conduct and its body of policies, and in accordance with all applicable federal, state, and local laws governing the use of computers and the Internet.

These obligations apply regardless of where access and use originate: Rutgers office, classroom, public space, lab, at home, or elsewhere outside the University.

The rules stated in this policy also govern the use of information assets provided by the State of New Jersey, other state and federal agencies, and other entities that have contracted with Rutgers to provide services to their constituents and/or clients.

Schools, units, and departments may produce more restrictive policies. Therefore, users should consult with their department if there are any other restrictions in place that supplement this policy.

**Expectation of Privacy**

Information created, stored, or accessed using Rutgers information systems may be accessed and reviewed by Rutgers personnel to measure, monitor, and address the use, performance, or health of the University’s information systems, or to respond to information security issues. Internet usage may also be monitored when using the University’s network, including when using Rutgers’ remote access services. Additionally, data backups of electronic information stored on Rutgers’ information systems are made regularly and stored at off-site locations or across different campuses.

This information may be provided to an external party at the University’s discretion without prior notification. Therefore, users have no expectation of privacy when accessing, transmitting, receiving, creating, or storing personal information using the University’s information systems. This includes access to the Internet through a University information system, unless such communications are protected by law or privilege.

All electronic information created, stored, or transmitted by use of Rutgers’ information systems is the property of the University, unless otherwise explicitly noted.
I. Requirements:

President/CEOs, Vice Presidents and Deans must:

A. Distribute copies of this policy to all members of their organizations.

B. Ensure that each member of their respective organizations receives periodic training and awareness about acceptable use of Rutgers' electronic information and information systems.

C. Communicate any additional restrictions they have established governing their members use of the University's electronic information and information systems.

II. Prohibited Actions

The list of prohibited actions is not intended to be comprehensive. The evolution of technology precludes the University from anticipating all potential means of capturing and transmitting information. Therefore, users must take care when handling sensitive information. Refer to Rutgers' Information Classification policy's appendix for types of information that are considered sensitive and/or contact Rutgers's Information Protection and Security Office for guidance.

Users, at minimum, will ensure that they do not:

A. Distribute information classified as Confidential or Private, or otherwise considered or treated as privileged or sensitive information, unless they are an authoritative University source for, and an authorized University distributor of that information and the recipient is authorized to receive that information. (For examples of Confidential and Private information, see the appendix in the University's Information Classification policy.)

B. Share their passwords with other individuals or institutions (regardless if they are affiliated with Rutgers or not) or otherwise leave them unprotected.

C. Attempt to uninstall, bypass, or disable security settings or software protecting the University's electronic information, information systems, or computer hardware.

D. Engage in unauthorized attempts to gain access or use the University's electronic information, information systems, or another user's account.

E. Use third party email services to conduct sensitive University business or to send or receive Rutgers information classified as Confidential or Private or otherwise considered privileged or sensitive information.

F. Use email auto-forwarding to send University information (regardless of classification) to non-Rutgers email accounts (see Restricted Services).

G. Distribute or collect copyrighted material without the expressed and written consent of the copyright owner.
H. As per the Joint Commission on Accreditation of Healthcare Organizations, they do not use texting for communicating health care orders (see Restricted Services, section F - Texting).

III. Restricted Services

This list of restricted services is not intended to be comprehensive. The evolution of technology precludes the University from anticipating all potential means of storing, capturing and transmitting information. Therefore, when using third party technology services not explicitly restricted in this policy, users must exercise care to not compromise sensitive Rutgers information. Refer to Rutgers’ Information Classification policy’s appendix for types of information that are considered sensitive and/or contact Rutgers’ Information Protection and Security Office for guidance.

Restricted services include the following:

A. Social Media

1. Social media tools cannot be used to communicate or store University information classified as Confidential or Private or otherwise considered privileged or sensitive by Rutgers. Social media tools include, but are not limited to:

   - Social networking sites: e.g., Facebook, Google+, Myspace, LinkedIn
   - Blogs
   - Microblogging sites: e.g., Twitter
   - Wikis
   - Content-sharing services: e.g., YouTube (video) and Flickr (for photos, videos, etc.).

2. Online forums

   The Rutgers name or your Rutgers email address cannot be used on social media sites for personal communications or postings.

3. Using the Rutgers name or email address on social media sites to post information in a manner that may be interpreted as representing an official position of Rutgers, or which may misrepresent the University’s viewpoint. All postings where the user is identified as a member of Rutgers should clearly communicate that “The views and opinions expressed are strictly those of the author. The contents have not been reviewed or approved by Rutgers, the State University of New Jersey.”

B. Professional Social Media

The use of professional social media tools, such as Doximity and Sermo, cannot be used:

1. To discuss patient cases in a manner that compromises patient identity or privacy, or otherwise represents a violation of HIPAA’s Privacy or Security rules, state or local privacy laws, or University policies.
2. To communicate or post information that could potentially reveal information classified as Confidential or Private or otherwise considered privileged or sensitive by Rutgers, or which compromises the privacy of a member of the University community or its clients.

C. Cloud Services

1. Cloud Storage Tools

The use of third party cloud storage services cannot be used to store University information classified as Confidential or Private or otherwise considered privileged or sensitive by Rutgers. Cloud storage tools include, but are not limited to:

- iCloud
- Carbonite
- McAfee Online Backup
- SkyDrive

2. Data Sharing Tools

The use of data sharing tools cannot be used to share or store University information classified as Confidential or Private or otherwise considered privileged or sensitive by Rutgers. Data sharing tools include, but are not limited to:

- Box.net
- Catch
- Dropbox
- Evernote
- Google Docs
- Google Drive
- OpenDrive
- SugarSync

D. Third Party Email Services

Third party email services cannot be used to communicate or store University information classified as Confidential or Private or otherwise considered privileged or sensitive.

E. Email Auto-Forwarding

University information, regardless of classification, cannot be auto-forwarded to non-Rutgers email accounts.

F. Alumni and Retired Faculty

Alumni and retired faculty may use email auto-forwarding provided they hold no other position at the University, including as a volunteer.
G. Texting

1. Health Care Information

As per the Joint Commission on Accreditation of Healthcare Organizations, “It is not acceptable for physicians or licensed independent practitioners to text orders for patients to the hospital or other health care setting. This method provides no ability to verify the identity of the person sending the text and there is no way to keep the original message as validation of what is entered into the medical record.”

2. General Use

Users should take care texting other sensitive information, particularly when confirmation of receipt or the identity of the recipient is required for business or legal purposes.

H. Internet-based Video Conferencing

Internet-based video conferencing services, such as Skype, are limited to Rutgers business-use only and must be conducted using Rutgers equipment. They are to be used strictly for business collaboration between members of the Rutgers community or outside entities, or for educational purposes. Users must ensure that video communications are done in a setting that limits or restricts the possibility of non-authorized individuals from viewing or listening to sensitive information.

IV. Non-Compliance and Sanctions

Failure to comply with this policy may result in denial or removal of access privileges to the University’s electronic systems, disciplinary action under applicable University policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable state and federal statutes.