RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Acceptable Use Policy for Information Technology Resources				
Section #:	70.1.1	**Section Title:**	Information Technology: Information Technology Policies	**Formerly Book:**	Formerly Policy 70.2.23 (merged into Policy 70.1.1)
Approval Authority:	Executive Vice President – Chief Financial Officer and University Treasurer	**Adopted:**	02/01/2000	**Reviewed:**	04/06/2021
Responsible Executive:	Senior Vice President and Chief Information Officer	**Revised:**	08/31/2010; 01/23/2013; 10/10/2013; 07/03/2014; 10/27/2014, 08/22/2016; 02/27/2017 *(Reverted back to 10/27/2014 version)*; 12/13/2018; 04/06/2021		
Responsible Office:	Office of Information Technology (OIT)	**Contact:**	oitpolicies@rutgers.edu		

1. Policy Statement

Access to the University's information technology resources is a privilege that requires each authorized member to act responsibly and guard against inappropriate use and abuse. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable use.

2. Reason for Policy

This policy outlines the acceptable use of University information technology resources, which include, but are not limited to equipment, software, networks, systems, data storage devices, media, facilities, and stationary and mobile devices used to access Rutgers information technology resources, whether the technology or devices are personally owned, leased, or otherwise provided by the University. Information technology resources also include any and all Rutgers data, records, information, and record systems stored on or retrievable from such equipment, software, networks, systems, data storage devices, media, and facilities, or stationary and mobile devices.

3. Who Should Read This Policy

All members of the Rutgers University community.

4. Resources

University Policy: Information Technology - Section 70

University Policy: Clinical, Compliance, Ethics & Corporate Integrity - Section 100

University Policy 50.3.7: Copyright Policy

University Policy 60.1.12: Policy Prohibiting Discrimination and Harassment

University Policy 70.1.2: Information Classification

University Policy 70.1.3: Incident Management

University Policy 70.1.6: Email and Calendar Policy

Guidelines for Use of Email for Official Purposes

5. Definitions

Availability - The expectation that information is accessible by the University community when needed.

Confidentiality - The state of keeping information and/or materials private, with only authorized individuals, processes, and systems having access to view, use, or share.

Guidelines - Advice on the ways to comply with policy, written for non-technical users who have multiple options for secure information handling processes.

Integrity - The expectation that the University's information will be protected from intentional, unauthorized, or accidental changes.

Procedures - Step by step instructions and implementation details for personnel to perform specific tasks in ways that ensure that the associated preventive, detective, and/or response mechanisms work as planned.

Technology Standards - Established requirement of technical configuration parameters and associated values to ensure that management can secure University assets and comply with University policy and regulatory requirements. It is a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices.

6. The Policy

A. User Responsibilities

i. **Privacy** – Because the primary use of the University's communications and business systems is to further the institutional mission, members of the University community should not have the expectation of privacy in their use of electronic systems, whether work-related or personal. By their nature, electronic systems may not be secure from unauthorized access, viewing, or infringement. Although the University employs technologies to secure its electronic resources and does not monitor the content on a routine basis, as a rule confidentiality of electronic data cannot be assumed and the University reserves the right to examine all files and content without notification.

ii. **Intellectual Freedom** – It is the policy of Rutgers, the State University of New Jersey, to allow access for its community to local, national, and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Nevertheless, the University reserves the right to limit or restrict the use of its information technology resources based on applicable law, institutional policies and priorities, and financial considerations. Violations include but are not limited to:

- Certain categories of speech – defamation, obscenity, and incitement to lawlessness – not protected by the Constitution. The University reserves the right, at its sole discretion, to decline to post, to remove posted content, or to restrict University web sites

or computer accounts which contain or are used for personal expressions of a non-academic nature.

iii. **Each user may use only those information technology resources for which he or she has authorization. Violations include but are not limited to:**

- failing to take reasonable and necessary measure to safeguard the operating integrity of systems and their accessibility by others;
- sharing passwords or log-in IDs. Users are responsible for any activity conducted with their computer accounts;
- using resources without specific authorization;
- using another individual's electronic identity;
- accessing files, data, or processes without authorization.

iv. **Information technology resources must be used only for their intended purpose(s) relating to University business. Violations include but are not limited to:**

- misusing software to hide personal identity, or to interfere with other systems or users;
- misrepresenting a user's identity in any electronic communication;
- using electronic resources for deceiving, harassing, or stalking other individuals.
- sending threats, "hoax" messages, chain letters, or phishing;
- sending mass emails to the Rutgers community without following proper procedures;
- intercepting, monitoring, or retrieving without authorization any network or other electronic communication;
- using University computing or network resources for private advertising or other private commercial purposes;
- circumventing, disabling, or attempting to circumvent or disable security mechanisms without authorization;
- using privileged access to University systems and resources for other than official duties directly related to job responsibilities, with the exception of incidental private use;
- making University systems and resources available to those not affiliated with the University;
- using former system and access privileges without authorization after association with the University has ended or using system and access privileges to a former organization's resources without authorization after the transfer to the new organization.

v. **The access to and integrity of information technology resources must be protected. Violations include but are not limited to:**

- Using third party, cloud and non-cloud, systems not authorized or approved by OIT's Information Security Office to transmit, process, or store University data classified as Critical or Restricted per University Policy 70.1.2: Information Classification;
- creating or propagating malware, spyware, computer viruses, worms, Trojan Horses, or any other malicious code;
- preventing others from accessing an authorized service;
- developing or using programs that may cause problems or disrupt services for other users;
- degrading or attempting to degrade performance or deny service or to waste or unfairly monopolize computing resources laws;
- corrupting or misusing information;
- altering or destroying information without authorization.

vi. **Applicable State, federal, and local laws and University policies must be followed. Violations include but are not limited to:**

a) Laws

- failure to respect the copyrights and intellectual property rights of others;
- making more copies of licensed software than the license allows;
- downloading, using, or distributing illegally obtained media (e.g., software, music, movies);
- uploading, downloading, distributing, or possessing electronic content explicitly prohibited by State, federal or local law (i.e., child pornography).

b) Policies

- accessing, storing, or transmitting information classified as Critical or Restricted (e.g., social security numbers, patient health information, driver's license numbers, credit card numbers) without a valid business or academic reason or transmitting such information without using appropriate security protocols (e.g., encryption);
- distributing data/information classified as Critical or Restricted, unless acting as an authoritative University source and an authorized University distributor of that data/information and the recipient is authorized to receive that data/information;
- transmitting unencrypted Critical or Restricted information over open public networks such as the internet or unencrypted email;

- using social media to communicate or store University data/information classified as Critical or Restricted;

- using third party cloud storage or data sharing tools (i.e., iCloud, Carbonite, Dropbox) to store University information classified as Critical or Restricted without prior OIT approval.

vii. **University business should be conducted using University-provided information technology systems, resources, and services.**

viii. **Accessing information and Records:** Recognizing that not all circumstances can be anticipated, access to information and records residing on University information technology resources will ordinarily be governed by the following:

a) University Responsibilities: The University's obligations in relation to information technology resources include ensuring compliance with applicable laws and University policies and procedures, protecting the integrity and operation of its resources, and preserving information as necessary to protect the interests of the University and to enable it to satisfy these obligations. Accordingly, the University may access Rutgers-related electronic information on any device on which it is stored or may be accessed, and may access a user's records and information stored on University information technology resources systems or equipment for the above-mentioned purposes. Such access must be for specific, articulable reasons, must be appropriately circumscribed, and is limited to authorized personnel. The University understands that some users may have personal information and/or records on University systems and it respects the privacy of all users as to such information insofar as possible in complying with its above-mentioned obligations.

i. Standards for Accessing or Monitoring Information and Records: The University may access or monitor any/all information, records, record systems, and/or information technology resources in the following circumstances:

1. As necessary or appropriate to avert reasonably anticipated or already apparent threats or hazards to University information, records, or information technology resources. An example includes scanning to detect computer viruses;

2. As and when required by law or to comply with legal or contractual obligations of the University;

3. In connection with a legal proceeding in which the Office of General Counsel is involved or an investigation conducted by or on behalf of the Office of Employment Equity or University Ethics and Compliance, for which access is necessary or appropriate;

4. When there is reasonable cause to believe that the employee has engaged in misconduct, has violated University policies or regulations, or may have used University resources improperly and that the information and records to be accessed or monitored are relevant to the misconduct or violation in question;

5. When the University otherwise has a legitimate need to access the information, records, or information technology resources.

Reasonable efforts will be made to notify the individual of the need for access to information or records in which the individual has a

substantial personal interest in information or records stored on or transmitted through the University's information technology resources or other electronic system unless prohibited by law, inconsistent with University policy, or inconsistent with the University carrying out its normal operations and/or aforementioned obligations.

ii. Preserving and Protecting Records: In circumstances where the University determines that there may be a specific risk to the integrity or security of records, data, information, or information technology resources, the University may take measures to protect or preserve them. For instance, the University may take a "snapshot" of a computing account to preserve its status on a given date, copy the contents of a file folder, or restrict user access to information technology resources in whole or in part.

b) Employee Obligations

i. Standards of Employee Conduct for Accessing or Monitoring Records: It is a violation of this policy for an employee to monitor information technology resources or record systems or access records beyond the standards established within this policy. It is also a violation of the policy if the University has granted access to the employee (to monitor or access records or systems) and the employee has accessed or monitored records or record systems for purposes other than the purposes for which the University has granted access.

ix. **Telecommuting and its Impact to Security and Privacy**

University policies, procedures, laws and regulations are applicable at all times. Individuals accessing University resources, systems, and information from alternate places of work (i.e. telecommuting from home, temporary office space, or while traveling) must adhere to all University policies, procedures, laws, and regulations.

a) Information Users Must:

i. Access University resources, systems, and information via approved secure channels that enforce the classification of the data in use per University Policy 70.1.2: Information Classification and all regulatory requirements pertaining to the resources.

ii. Use only University-approved software for conducting University business including but not limited to email, video conferencing, and collaboration software.

iii. Use only University-approved devices for conducting University business including but not limited to laptops, computers.

iv. Keep University and personal data or email from being co-mingled.

v. Ensure all personal devices used to access the Internet (modems, WiFi, etc.) are up-to-date with regard to operating systems, application software versions, and antivirus protection.

vi. Adhere to the following practices to protect University information:
   a. Utilize multifactor authentication,
   b. Clean desk / clear screen,
   c. Log off / lock all devices when unattended or not in use, and

d. Secure University equipment in a locked drawer or room when not in use.

vii. Be alert for fraud, suspicious email, phishing, and scams that will attempt take advantage of the situation.

viii. Ensure printed information and other media are protected from theft and accidental disclosure and are disposed of in a manner that enforces the classification of the data (e.g. shredded).

ix. Backup and save University work product only to secured network drives.

A. Encrypt data classified as Restricted or Critical per University Policy 70.1.2: Information Classification that is to be transmitted.

B. Report loss or theft of a Mobile Computing Devices, Removable Media or media immediately to the OIT Help Desk, University Ethics and Compliance, and the Organization of Risk Management per University Policy 70.1.3: Incident Management.

B. 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.