Acceptable Use Policy

ROWAN UNIVERSITY POLICY

Title: Acceptable Use Policy
Subject: Information Security
Policy No: ISO:2013:01
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Director of Information Security
Date Adopted: 07/01/2013
Last Revision: 02/28/2019
Last Review: 02/27/2019

I. PURPOSE

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

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and Director of Information Security shall ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy in their respective areas.

III. APPLICABILITY

This policy applies to all members of the Rowan Community who access and use the University's electronic information and information systems.

IV. DEFINITIONS

Refer to the Rowan University Technology Terms and Definitions for terms and definitions that are used in this policy.

V. POLICY

1. The University expects users will access and use the University's electronic information and information systems in a manner that:
    a. Does not compromise the confidentiality, integrity, or availability of those assets; and
    b. Reflects the University's standards as defined in the Code of Conduct/Statement of Principles and its body of policies, and in accordance with all applicable federal, state, and local laws governing the use of computers and the Internet.
2. These obligations apply regardless of where access and use originate: Rowan office, classroom, public space, lab, at home, or elsewhere outside the University.
3. 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 Rowan to provide services to their constituents and/or clients.
4. 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.
5. This policy and Rowan's Code of Conduct/Statement of Principles also govern access and use of the University's electronic information and information systems originating from non-Rowan computers, including personal computers and other electronic devices. The access and use of electronic information provided by research and funding partners to Rowan are also governed by this policy.
6. The use of information systems acquired or created through the use of University funds, including grant funds from contracts between the University and external funding sources (public and private), are covered by this policy. This includes University information systems that are leased or licensed for use by members of the Rowan Community. Users are given access to Rowan's 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.
7. Rowan recognizes that all members of the Rowan Community have an expectation of privacy for information in which they have a substantial personal interest. However, this expectation is limited by Rowan's need to comply with applicable laws, protect the integrity of its resources, and protect the rights of all users and the property and operations of Rowan University. As such, Rowan reserves the right to access, quarantine, or hold for further review any files or computing devices on Rowan's network or its information technology resources if there is just cause to believe that university policies or laws are being violated or if such access is necessary to comply with applicable law or conduct university business operations.

8. Information created, stored, or accessed using Rowan information systems may be accessed and reviewed by Rowan personnel for legitimate systems purposes, including but not limited to the following:

    a. Emergency Problem Resolution
    b. 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 Rowan's remote access services.
    c. To create data backups of electronic information stored on Rowan's information systems.
    d. To respond to User Requests approved by the Office of General Counsel.
9. Information may be accessed, reviewed, and provided to an external party at the University's discretion without prior notification with adequate cause and subject to review of the Office of General Counsel to comply with applicable law and to conduct normal university operations. Examples include, but are not limited to the following:

    a. Compliance with the New Jersey Open Public Records Act ("OPRA") which requires disclosure of electronic records and other data on the Rowan system subject to exemptions under OPRA. Requests will be reviewed by the Records Custodian/OPRA officer in conjunction with the Office of General Counsel.
    b. Compliance with a valid subpoena, court order, or discovery request. Requests will be reviewed by the Office of General Counsel.
    c. Audits, investigations, or inquiries undertaken by governmental entities or appropriate internal investigators or units. Requests will be reviewed by the Office of General Counsel.
    d. To conduct necessary business operations.
10. All electronic information created, stored, or transmitted by use of Rowan's information systems is the property of the University, unless otherwise explicitly noted.
11. Technicians and System Administrators have greater ability to access information stored on and transmitted through Rowan's information systems. As such, Technicians, Systems Administrators, and others with privileged access shall not access such information unless such access is necessary for the purposes outlined above, for systems purposes, or unless such access is supported by adequate cause and reviewed by the Office of General Counsel.
12. Prohibited Actions

    a. 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 Rowan's Information Classification and Data Governance policies for types of information that are considered sensitive and/or contact Rowan's Information Security Office for guidance.
    b. Users, at minimum, will ensure that they do not:

        i. 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.
        ii. Share their passwords with other individuals or institutions (regardless if they are affiliated with Rowan or not) or otherwise leave them unprotected.
        iii. Attempt to uninstall, bypass, or disable security settings or software protecting the University's electronic information, information systems, or computer hardware.
        iv. Engage in unauthorized attempts to gain access or use the University's electronic information, information systems, or another user's account. Users with privileged access, such as Technicians and Systems Administrators, shall not engage in unauthorized access, use, or review of information or data, without appropriate approvals.
        v. Use third-party email services to conduct sensitive University business or to send or receive Rowan information classified as Confidential, Private or Internal or otherwise considered privileged or sensitive information.
        vi. Use email auto-forwarding to send University information (regardless of classification) to non-Rowan email accounts (see Restricted Services).
        vii. Distribute or collect copyrighted material without the expressed and written consent of the copyright owner or without lawful right to do so, such as in the case of fair use.
    c. User understands the HIPAA Privacy Security rules, especially with regard to Sensitive Electronic Information (SEI), Private Health Information (PHI), and Personally Identifiable Information (PII) and will abide by these rules, including understanding that they will be held accountable for the use of personal devices for conducting University business. (Refer to HIPAA policies located at www.rowan.edu/compliance).
13. Restricted Services

    a. 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 Rowan information, particularly when confirmation of receipt or the identity of the recipient is required for business or legal purposes. Refer to Rowan's Information Classification and Data Governance policies for types of information that are considered sensitive and/or contact Rowan's Information Security Office for guidance.
    b. Restricted services include the following:

        i. Social Media

            1. Social media tools or web content platforms cannot be used to communicate or store University information classified as Confidential or Private or otherwise considered privileged or sensitive by Rowan. Social media tools include, but are not limited to: Facebook, Twitter, LinkedIn, Instagram, Medium, Reddit, YouTube and Flickr.
            2. For additional requirements on the use of social media, see the Social Media Policy.
        ii. Professional Social Media

            1. Professional social media cannot be used to communicate or store University information classified as Confidential or Private or otherwise considered privileged or sensitive by Rowan.
            2. The use of professional social media tools, such as Doximity and Sermo, cannot be used:

                a. 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.
                b. To communicate or post information that could potentially reveal information classified as Confidential or Private or otherwise considered privileged or sensitive by Rowan, or which compromises the privacy of a member of the University community or its clients.

c. For additional requirements on the use of social media, see the Social Media Policy.

iii. Cloud Services, Collaboration and Storage

1. Third-party cloud storage services cannot be used to store University information classified as Confidential.
2. Google Drive is approved for Private, Internal and Public data. For additional information on the use of Google Drive, see Google Apps: Appropriate Data Use.
3. The use of non-approved third-party cloud storage services cannot be used to store University information classified as Confidential or Private or otherwise considered privileged or sensitive by Rowan. Cloud storage tools include, but are not limited to: iCloud, Carbonite, OneDrive, Box, Dropbox, Evernote, OpenDrive and SugarSync.

iv. Third Party Email Services

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

v. Email Auto-Forwarding

1. With the exception of current undergraduate and other non-medical students, members of the Rowan Community are not permitted to automatically forward or redirect messages from a Rowan email address to a non-Rowan email address

vi. Texting

1. Texting cannot be used to communicate or store University information classified as Confidential.

vii. Video Conferencing

1. Video conferencing services are limited to Rowan business-use only and must be conducted using Rowan equipment. They are to be used strictly for business collaboration between members of the Rowan Community or outside entities, or for educational purposes. Users must ensure that video communications are done in a setting or configured to restrict the possibility of non-authorized individuals from viewing or listening to sensitive information.

viii. Chat

1. The use of non-approved chat services cannot be used to communicate or store University information classified as Confidential or Private or otherwise considered privileged or sensitive by Rowan. Chat tools include, but are not limited to: Slack and HipChat.
2. Jabber is approved for Private, Internal and Public data.

ix. BitTorrent Software

1. BitTorrent software (or other file sharing software) used to download and share movies, music, and other copyrighted media is strictly forbidden unless it is used for Rowan business or academic purposes. The use of this software must be approved by the Dean or Department Head/Chair, and the Information Security Office.

VI. POLICY COMPLIANCE

1. Violations of this policy may subject the violator to disciplinary actions up to or including termination of employment or dismissal from school, subject to applicable collective bargaining agreements and may subject the violator to penalties stipulated in applicable state and federal statutes. Students who fail to adhere to this Policy or the Procedures and Standards will be referred to the Office of Student Affairs and may be expelled. Affiliates, contractors and vendors who fail to adhere to this Policy and the Procedures and Standards may face termination of their business relationships with the University. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization.
2. University sanctions, penalties, fines and discipline for employees will be based on the severity of the incident per below:

    a. *Low* – retraining and to be reviewed with the employee during annual appraisal. Also, any cost shall be borne by the Department. The Department Chair or VP will determine how these funds will be assigned.
    b. *Medium* – retraining and to be reviewed with the employee during annual appraisal. Discipline will be considered up to and including dismissal from the University. Also, all costs will be borne by the Department. The Department Chair or VP will determine how these funds will be assigned.
    c. *High* – retraining and to be reviewed with employee during annual appraisal. Discipline will be unpaid suspension for a minimum of three (3) days with a consideration of up to and including dismissal from the University. Civil and criminal penalties may apply. Also, all costs will be borne by the Department. The Department Chair or VP will determine how these funds will be assigned. The Deans of each College, Vice Presidents, and University President, with the assistance of the Department of Human Resources, will enforce the sanctions appropriately and consistently to all violators regardless of job titles or level within the University and in accordance with bargaining agreements for represented employees.

VII. ADDITIONAL INFORMATION

1. Rowan University Statement of Principles
2. Breach Notification Policy
3. HIPAA Policy
4. IT Acquisition Process (ITAP)
5. Information Classification Policy
6. Data Governance Policy

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer