Acceptable Use Policy

Rowan University

Title: Acceptable Use Policy

Subject: Information Security

Policy No: ISO: 2013:01

Applies: University-wide

Issuing Authority: Senior Vice President for Information Resources and Chief Information Officer

Responsible Officer: Senior Vice President for Information Resources and Chief Information Officer

Date Adopted: 07-01-2013

Last Revision: 10-10-2016

Last Review: 06-23-2016

I. PURPOSE

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

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the University's Chief Information Security Officer shall implement and ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy.

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

1. Availability – the expectation that information is accessible by Rowan when needed.

2. Cloud Services – Consumer and business products, services and solutions delivered and consumed on-demand, using the cloud service providers' pooled resources, and delivered over a broad network, such as the Internet.

3. Confidentiality – the expectation that only authorized individuals, processes, and systems will have access to Rowan's information.

4. Confidential Information – the most sensitive information, which requires the strongest safeguards to reduce the risk of unauthorized access or loss. Unauthorized disclosure or access may 1) subject Rowan to legal risk, 2) adversely affect its reputation, 3) jeopardize its mission, and 4) present liabilities to individuals (for example, HIPAA and HITECH penalties). See the Information Classification policy for additional information.

6. **HITECH** – Health Information Technology for Economic and Clinical Health Act.

7. **Information System** – consists of one or more components (e.g., application, database, network, or web) that is hosted in a University campus facility, and which may provide network services, storage services, decision support services, or transaction services to one or more business units.

8. **Integrity** – the expectation that Rowan's information will be protected from improper, unauthorized, destructive, or accidental changes.

9. **Internal Information** – data that is owned by the University, is not classified Confidential or Private, and is not readily available to the public. For example, this includes employee and student identification numbers and licensed software.

10. **Mobile Computing Device** – including, but not limited to, laptops, netbooks, tablets, smartphones (BlackBerry, iPhone, etc.) and mobile broadband cards (also known as AirCards® and connect cards).

11. **Private Information** – sensitive information that is restricted to authorized personnel and requires safeguards, but which does not require the same level of safeguards as confidential information. Unauthorized disclosure or access may present legal and reputational risks to the University. See the University's Information Classification policy for additional clarification.

12. **Privileged Information** – refers to attorney-client communication.

13. **Public Information** – information that is readily available to the public, such as the information published on web sites.

14. **Removable Media** – including, but not limited to, CDs, DVDs, copier hard drives, storage tapes, flash devices (e.g., CompactFlash and SD cards, USB flash drives), and portable hard drives.

15. **Social Media** – refers to tools that allow the sharing of information and creation of communities through online networks of people.

16. **Rowan Community** – faculty, staff, non-employees, students, attending physicians, contractors, covered entities, agents, and any other third parties of Rowan.

V. REFERENCES

1. The Rowan University Code of Conduct

2. Breach Notification Policy

3. HIPAA Policy

4. IT Acquisition Policy

VI. POLICY

1. 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.

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" 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 is also governed by this policy.

6. The use of information systems acquired or created through 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.
Expectation of Privacy

7. Rowan recognizes that all members of the University 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 the 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:
   1. Emergency Problem Resolution
   2. 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.
   3. To create data backups of electronic information stored on Rowan's information systems.
   4. To respond to User Requests
   5. Such access shall require approval 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:
   1. 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.
   2. Compliance with a valid subpoena, court order, or discovery request. Requests will be reviewed by the Office of General Counsel.
   3. Audits, investigations, or inquiries undertaken by governmental entities or appropriate internal investigators or units. Requests will be reviewed by the Office of General Counsel.
   4. 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. Requirement - Office of the General Counsel:
   1. 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 network 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
   1. 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 policy's appendix for types of information that are considered sensitive and/or contact Rowan's Information Security Office for guidance.
   2. Users, at minimum, will ensure that they do not:
      1. 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.)
      2. Share their passwords with other individuals or institutions (regardless if they are affiliated with Rowan or not) or otherwise leave them unprotected.
      3. Attempt to uninstall, bypass, or disable security settings or software protecting the University's electronic information, information systems, or computer hardware.
      4. Engage in unauthorized attempts to gain access or use the University's electronic information, information systems, or another user's account. Technicians, Systems Administrators, and others with network access shall not engage in unauthorized access, use, or review of information or data.
      5. Use third party email services to conduct sensitive University business or to send or receive Rowan information classified as Confidential or Private or otherwise considered privileged or sensitive information.
      6. Use email auto-forwarding to send University information (regardless of classification) to non-Rowan email accounts (see Restricted Services).
      7. 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.
      8. As per the Joint Commission, they do not use texting for communicating health care orders (see Restricted Services).
   3. 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, thereby understanding that they will be held accountable for personal devices. (Refer to HIPAA policies located at www.rowan.edu/compliance).
   4. Violations of this policy may result in disciplinary action, up to and including termination, subject to applicable collective bargaining agreements as outlined in Attachment 1.

13. Restricted Services
   1. 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. Refer to Rowan's Information Classification Policy's appendix for types of information that are considered sensitive and/or contact Rowan's Information Security Office for guidance.

2. Restricted services include the following:
   1. 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 Rowan. 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
      1. The Rowan name or your Rowan email address cannot be used on social media sites for personal communications or postings.
      3. Using the Rowan name or email address on social media sites to post information in a manner that may be interpreted as representing an official position of Rowan, or which may misrepresent the University's viewpoint. All postings where the user is identified as a member of Rowan should clearly communicate that "The views and opinions expressed are strictly those of the author. The contents have not been reviewed or approved by Rowan University."
   3. Professional Social Media
      1. 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 Rowan, or which compromises the privacy of a member of the University community or its clients.
   4. Cloud Services
      1. Cloud Storage Tools
         1. 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 Rowan. Cloud storage tools include, but are not limited to:
            - iCloud
            - Carbonite
            - McAfee Online Backup
            - SkyDrive
      2. Data Sharing Tools
         1. 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 Rowan. Data sharing tools include, but are not limited to:
            - Box.net
            - Catch
            - Dropbox
            - Evernote
            - Google Docs
            - Google Drive
            - OpenDrive
            - SugarSync
   5. 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.
   6. Email Auto-Forwarding
      1. Full time faculty and staff are not permitted to automatically forward or redirect messages from their primary email address to a non-Rowan email address.
      2. Individuals associated with the School of Osteopathic Medicine (Faculty/Staff/Students) are not permitted to forward or redirect messages from their primary Rowan email address to a non-Rowan email address.
      3. Alumni and retired faculty may use email auto-forwarding provided they hold no other position at the University, including as a volunteer
   7. Texting
      1. Health Care Information
         - According to the Joint Commission, "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.
   8. Internet-based Video Conferencing
      1. Faculty and Staff
         - Internet-based video conferencing services, such as Skype, 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 that limits or restricts the possibility of non-authorized individuals from viewing or listening to sensitive information.
   9. Bit Torrent Software
14. NON-COMPLIANCE AND SANCTIONS

1. Violations of this policy may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a school, and may subject the violator to penalties stipulated in applicable state and federal statutes.

2. University Sanctions, Penalties, Fines and Discipline. Based on the severity of the incident and the level of severity (Low, Medium, High) the following will apply and be typical for each level:

   1. **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.
   
   2. **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.
   
   3. **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.

By Direction of the CIO:

________________________________________
Mira Lalovic-Hand,
VP and Chief Information Officer