Access Control Policy

ROWAN UNIVERSITY POLICY

Title: *Access Control Policy*
Subject: *Information Security*
Policy No: *ISO:2013:13*
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: ***06-01-2014***
Last Review: ***07-02-2018***

I. PURPOSE

To establish the access controls necessary to safeguard the University's electronic information and information systems.

II. ACCOUNTABILITY

Under the President, the Chief Information Officer and Director of Information Security shall ensure compliance with this policy. The Vice Presidents and Deans shall 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. It presents administrative, physical, and technical safeguards necessary to manage and control access to ROWAN's information systems.

IV. DEFINITIONS

1. ***Administrative Safeguards*** – consists of policies and administrative procedures that manage the selection, development, implementation, and maintenance of security measures that protect the university's electronic information and information systems.

2. ***Application*** – a computer program that processes, transmits, or stores University information and which supports decision-making and other organizational functions. It typically presents as a series of records or transactions. These records and transactions are generally accessible by more than one user.

3. ***Availability*** – the expectation that information is accessible by ROWAN when needed.

4. ***Business Unit*** – the term applies to multiple levels of the university, such as a revenue generating unit or a functional unit (e.g., Compliance, Human Resources, Information Resources and Technology (IR&T), Legal, and Finance). It may also be comprised of several departments.

5. ***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/HITECH penalties).

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

7. ***EPHI*** – electronic protected health information.

8. ***Generic Account*** – an account that is shared among a group of individuals, and typically used for devices like kiosks and clinical workstations. There is no corresponding employee account (i.e., RUID).

9. ***Guest Account*** – accounts provisioned to individuals not employed by ROWAN, but who have a justifiable business reason to access University resources.

10. ***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.

11. ***Least Privilege*** – giving every user, task, and process the minimal set of privileges and access required to fulfill their role or function. This includes access to information systems and facilities.

12. ***Physical Safeguards*** – physical measures to protect the facilities that house the University's electronic information and information systems.

13. ***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.

14. ***RUID*** – Reserved User ID.

15. ***Service Accounts*** – are accounts created by ROWAN's Active Directory or Domain Administrators teams to satisfy specific functions, such as communications between systems or to facilitate other operational requirements.

16. ***System Default Service Accounts*** – are accounts created by a software vendor to facilitate installation or provide out-of-the-box functionality.

17. ***ROWAN Community*** – faculty, staff, non-employees, students, attending physicians, contractors, covered entities, and agents of ROWAN.

18. ***Technical Safeguards*** – the technology, policies, and procedures used to control access to and protect the University's electronic information and information systems.

19. *User* – refers to any member of the ROWAN community, as well as to visitors and temporary affiliates, who have been explicitly and specifically authorized to access and use the University's data or information systems**.**

V. REFERENCES

1. Health Insurance Portability and Accountability Act of 1996 http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

2. Guest Account Registration Process

3. Statement of Principles

VI. POLICY

1. Access to the University's electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, all access is governed by law, other University policies, and the ROWAN Code of Conduct.

2. Persons or entities with access to the University's electronic information and information systems are accountable for all activity associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by the University, irrespective of the medium on which the information resides.

3. Access must be granted on the basis of least privilege - only to resources required by the current role and responsibilities of the person. In addition to the administrative, physical, and technical safeguards presented in this policy, the security requirements defined in the University's Information Classification policy must be followed.

4. Requirements:
    a. Access controls to the University's information systems must be established to ensure the confidentiality, integrity, and availability of the data accessible via those systems.
    b. Registration of Access
        i. With respect to registration of access to the University's information systems:
            - There must be a formal authorization process documented for access requests.
            - The requester's identity must be confirmed and authenticated.
            - User activity must be logged and tied to the user ID provisioned to the user.
            - User IDs must be unique and require a password.
            - Requests for access must be approved by the requester's manager.
    c. Registration of Access for Non-ROWAN Personnel
        - Individuals who are not members of the ROWAN community and who have a justifiable business reason to gain access to ROWAN information services must go through the guest account registration process.
        - Registration must follow the requirements listed in section VI (A.1.).
        - De-Provisioning of Access
        - Cancellation of access to all University information systems, facilities, and information services (e.g., remote access) must be done in accordance with the procedures listed in University policy, Cancellation of Access to University Assets.
    d. Information System Identity Access Management
        - Information systems must, at minimum, require a user ID and password.
        - Requests for a deviation from this requirement are limited to clinical systems which have been identified by the school or unit as requiring a different access method in order to provide patient care.
        - Deviations must be reviewed and approved by the Chief Information Officer.
        - User ID Naming Conventions
        - User ID naming conventions must follow IR&T standards.
        - Passwords
        - User IDs must have an associated password.
        - Passwords must be configured to follow IR&T standards and/or vendors'
        - recommendations for strong passwords.
    e. Generic Accounts

i. In general, Generic Accounts are not permitted unless approved by the Information Security Office. In the event that they are approved, they must adhere to the following:
    - Generic accounts are subject to the requirements in this policy.
    - The accounts must be restricted to a specific device and named according to the device's naming convention.
    - Generic accounts must be restricted to kiosks or specialty devices where
    - standard authentication may impede the functionality of the device.

f. Guest Accounts
    - Guest accounts are subject to the requirements in this policy.
    - The accounts must be sponsored by a ROWAN employee who is responsible for the safeguarding of the information or information system as detailed in Section IV.
    - The accounts must have a lifecycle no longer than 12 months, after which they must be re-approved by the sponsor.

g. Service Accounts
    - Service accounts are subject to the requirements in this policy.
    - Service accounts can only be created by a member of ROWAN's Active Directory or Domain Administrators team to facilitate an identified operational need.
    - Service accounts do not expire.

h. System Default Service Accounts
    - Whenever possible, system default service accounts should be renamed or disabled as long as it does not adversely impact the operations of the application or other dependencies.
    - System default Service Accounts do not expire.

i. Physician Emergency Access Procedures to EPHI Information Systems (HIPAA § 164.312(a)(2)(ii)).
    - HIPAA requires that each school and unit establish documented emergency access procedures for EPHI information systems.
    - The procedures must satisfy the following two requirements:
    - The ability for physicians to access EPHI during a health emergency.
    - A contingency method for physicians to access EPHI if a natural or manmade disaster makes an information system unavailable.
    - Any deviation from HIPAA § 164.312(a)(2)(ii) must be documented and presented to the Office of Ethics, Compliance and Corporate Integrity and the Office of Legal Management.

j. Facility Access
    - Physical access to the facilities where information systems are housed must be limited to personnel specifically authorized to access those information systems in the facilities.
    - Access to the University's data centers must be approved by the data center manager and follow the Department of Public Safety's access request process.
    - Access to facilities is managed by the Department of Public Safety, and the access request process is documented in University policy, Identification Cards.

k. Separation of Duties
    - Access requests, authorization, and administrative responsibilities for information classified as Confidential or Private (otherwise considered sensitive) and their associated information systems should be separated.
    - Users should not have access privileges that would permit them to approve their own changes to an information system or electronic record.
    - If separation of duties is not possible due to staffing limitations, other mitigating controls must be in place to reduce the risk of fraud or tampering.

l. Access Entitlement Review
    - Access to information systems with information classified as Confidential or Private, or otherwise considered sensitive as per the University's Protection of Sensitive Electronic Information policy and Information Classification policy, must be, at minimum, reviewed quarterly.

- Access to information systems with non-sensitive information must be reviewed semi-annually.
- Access to the University's data centers must be reviewed semi-annually.

m. Responsibilities

i. Vice Presidents and Deans:
- Are responsible for safeguarding their organization's electronic information and information systems.
- Must ensure that each member of their organization understands the need to protect the University's electronic information and information systems.
- Must communicate this policy to all members of their organization.

ii. Business Unit Management:
- Are responsible for safeguarding their unit's electronic information and information systems.
- Must perform and comply with the policy requirements relevant to their position and responsibilities.
- Must ensure managers reporting to them perform and comply with the policy requirements relevant to their position and responsibilities.

iii. Information Owners (Data Stewards) must:
- Establish access authorization procedures to their electronic information and information systems.
- Establish physician emergency access procedures for EPHI information systems they own.
- Perform and comply with the policy requirements relevant to their information systems.
- Review access entitlements to their information systems as stipulated in this policy or when requested by IR&T, the Information Security Office, and/or Internal Audit.

VII. NON-COMPLIANCE AND SANCTIONS

1. Any individual who violates this policy shall be subject to discipline up to and including dismissal from the University, as well as civil and criminal penalties. Sanctions shall be applied consistently to all violators.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer