Security Monitoring Policy

ROWAN UNIVERSITY POLICY

Title: Security Monitoring Policy
Subject: Information Security
Policy No: *ISO:2013:14*
Applies: University-Wide
Issuing Authority: Senior Vice President for Information Resources and Technology and Chief Information Officer
Responsible Officer: Information Security Officer
Date Adopted: 07/01/2013
Last Revision: 04/16/2024
Last Review: 04/16/2024

I. PURPOSE

The purpose of this policy is to ensure that information security and technology security controls are in place and effective. One of the benefits of security monitoring, which is a method used to confirm that the security practices and controls in place are being adhered to and are effective, is the early identification of security issues or new security vulnerabilities. This early identification can help to prevent security incidents or to at least minimize the potential impact of such incidents. Other benefits include compliance with audit, FERPA, HIPAA, and state requirements.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Information Security Officer shall implement and ensure compliance with this policy.

III. APPLICABILITY

This policy applies to all University departments, administrative units, and affiliated organizations that use University information technology resources to create, access, store or manage University Data to perform their business functions. The requirement applies to enterprise information systems or systems that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein.

IV. DEFINITIONS

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

V. POLICY

1. All Rowan University Information and Information Technology which includes but is not limited to: servers, workstations, and network access devices are subject to ongoing monitoring. The inappropriate use of these systems and/or networks which violates the University's policies or local, state and federal laws will be investigated as needed. The Information Security Office (ISO) will be responsible for conducting these investigations under the direction of the Information Security Officer.
2. The Chief Information Officer (CIO) holds ultimate authority for the coordination of all Information Technology (IT) resources across the University. Accordingly, to facilitate effective security monitoring, discovery, and incident response, administrators of University owned or managed IT systems outside

the direct management of Information Resources and Technology (IRT) must grant IRT personnel, Security Operations Department and the Director of the Information Security Office, comprehensive administrative access at the time of system implementation. This mandate encompasses all existing and future platforms and systems excluding those dedicated to confidential research. It is incumbent upon system owners to actively maintain this access level for these IRT departments, ensuring continuity through any system updates or modifications to the systems or credentials.

3. The Information Security Officer has the right to disclose the contents of electronic files, as required by law, Internal Audit, or General Counsel.
4. All security monitoring will be performed by ISO unless authorized by the Information Security Officer.
5. All security-related anomalies or other suspicious activity should be reported to the ISO for investigation.
6. All security investigations will be managed and/or coordinated by the ISO. **Departments are strictly prohibited from conducting their own internal security investigations.**
7. Automated tools will be used to provide real time notification of detected security events and vulnerabilities. Where possible, a security baseline will be developed and the tools will report exceptions. Where feasible, these tools will be deployed to monitor:

    a. Internet traffic
    b. Electronic mail traffic
    c. LAN traffic, protocols, and IT inventory
    d. System security parameters
    e. Privilege escalation
    f. Privilege group membership
8. Where feasible, the following files will be checked for signs of security issues and vulnerability exploitation at a frequency determined by risk:

    a. Intrusion detection system logs
    b. Firewall logs
    c. User account logs
    d. Network scanning logs
    e. System error logs
    f. Application logs
    g. Data backup and recovery logs
    h. Help Desk trouble tickets
    i. Telephone activity – call detail reports
    j. Network printer and fax logs
9. Where feasible, the following checks will be performed monthly or a frequency determined by risk:

    a. Password strength
    b. Unauthorized network devices
    c. Unauthorized personal web servers
    d. Unsecured sharing of devices
    e. Unauthorized connections
    f. Operating system and software licenses
10. Any discovery of security issues will be reported to ISO for follow-up investigation.
11. IRT may disconnect or disable accounts, systems and or networking devices when monitoring detects the following issues:

    a. Unauthorized devices or software
    b. Unauthorized group membership
    c. Unauthorized access

d. Other security incidents

VII. NON-COMPLIANCE AND SANCTIONS

Violation 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.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer