Security Monitoring Policy

ROWAN UNIVERSITY POLICY

Title: *Security Monitoring Policy*
Subject: *Information Security*
Policy No: *ISO:2013:14*
Applies: *University-Wide*
Issuing Authority: *Information Security Office - Director of Information Security*
Responsible Officer: *Vice President for Information Resources and Chief Information Officer*
Adopted: *07/01/2013*
Amended: 06/01/2014
Last Revision: 07/02/2018

I. PURPOSE

A. The purpose of the Security Monitoring Policy is to ensure that information security and technology security controls are in place and effective. One of the benefits of security monitoring 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, FERBA, HIPAA, and state requirements.

B. Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective.

II. ACCOUNTABILITY

A. Under the direction of the President, the Chief Information Officer and the University's Director of Security Information shall implement and ensure compliance with this policy.

III. APPLICABILITY

A. 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

A. *Automated tools* - Is software that executes pre-scripted tests on software applications or hardware devices.

B. *Breach* - Is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.

C. *Electronic Mail* - A method of exchanging digital messages from an author to one or more recipients

D. *Firewall* - Is a software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set.

E. *Infrastructure* – Is the hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network.

F. *Information Security Office (ISO):* Department responsible to the executive management for administering the information security functions within the University. The ISO is the Rowan University internal and external point of contact for all information security matters.

V. REFERENCES

A. Information Security Policy

VI. POLICY

A. 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 Director of Information Security.

B. The Director of Information Security has the right to disclose the contents of electronic files, as required by law, Internal Audit, or General Counsel.

C. All security monitoring will be performed by the ISO unless authorized by the Director of Information Security.

D. All security-related anomalies or other suspicious activity should be reported to the ISO for investigation.

E. All security investigations will be managed and/or coordinated by the ISO. **Departments are strictly prohibited from conducting their own internal security investigations.**

F. 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:

1. Internet traffic
2. Electronic mail traffic
3. LAN traffic, protocols, and IT inventory
4. System security parameters
5. Privilege escalation
6. Privilege group membership

G. Where feasible, the following files will be checked for signs of security issues and vulnerability exploitation at a frequency determined by risk:

1. Intrusion detection system logs
2. Firewall logs
3. User account logs
4. Network scanning logs
5. System error logs

6. Application logs
7. Data backup and recovery logs
8. Help Desk trouble tickets
9. Telephone activity – call detail reports
10. Network printer and fax logs

H. Where feasible, the following checks will be performed monthly or a frequency determined by risk:

1. Password strength
2. Unauthorized network devices
3. Unauthorized personal web servers
4. Unsecured sharing of devices
5. Unauthorized connections
6. Operating system and software licenses

I. Any discovery of security issues will be reported to the ISO for follow-up investigation.

J. The IRT department may disconnect or disable accounts, systems and or networking devices when monitoring detects the following issues:

1. Unauthorized devices or software
2. Unauthorized group membership
3. Unauthorized access
4. 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