Security System Development Life Cycle Policy

ROWAN UNIVERSITY POLICY

Title: Security - System Development Life Cycle (S-SDLC) Policy
Subject: Information Security
Policy No: ISO:2013:16
Applies: University-wide
Issuing Authority: Vice President for Information Resources and Chief Information Officer
Responsible Officer: Director of Information Security
Date Adopted: 07/01/2013
Last Revision: 08/08/2018
Last Review: 08/08/2018

I. PURPOSE

The purpose of this policy is to define requirements for system security planning and management to improve protection of university information system resources.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Director of Information Security 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

1. ***"Confidential data"* -** Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.
2. **"*Enterprise information system*" -** An information system and/or server providing services commonly needed by the University community and typically provided by the IERP and or the IRT units. Departmental information systems provide services specific to the mission and focus of individual departments, administrative units, or affiliated organizations.
3. **"*Information Resources and Technology*" (IRT)** – the Rowan University department responsible for the governance of all information and technology.
4. **"*Institutional Effectiveness, Research & Planning*" (IERP) -** The Office of Institutional Effectiveness, Research & Planning (IERP) is Rowan University's official source for all data and statistics used for assessment, state and federal reporting.
5. **"*Information Technology Infrastructure Library*" (ITIL) -** Provides a cohesive set of best practice to Information Technology Service Management.
6. **"*Live data*" -** Data accessible to users through systems that are in production environment (i.e., live)
7. **"*National Institute of Standard Technology*" (NIST) -** NIST is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.
8. **"*Sanitized*" -** Is the process of removing sensitive information from a document or other medium, so that it may be distributed to a broader audience.

9. **"*System Administration and Network Security*" (SANS) -** SANS is a private U.S. company that specializes in information security and cybersecurity training, and security design and implementation best practices.
10. **"*Sensitive*" -** Any information that can be used for the purpose of identification.
11. **"*University Data*" -** Any data related to Rowan University functions that are a) stored on University information technology systems, b) maintained by Rowan faculty, staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).
12. **"*Vulnerability*" -** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

V. REFERENCES

1. Information Security Policy

VI. POLICY

1. Security has to be considered at all stages of the life cycle of an information system (i.e., feasibility, planning, development, implementation, maintenance, and retirement) in order to:

    a. ensure conformance with all appropriate security requirements,
    b. protect sensitive information throughout its life cycle,
    c. facilitate efficient implementation of security controls,
    d. prevent the introduction of new risks when the system is modified, and
    e. ensure proper removal of data when the system is retired. This policy provides guidance to ensure that systems security is considered during the Acquisition, Development and Maintenance and Testing Stages of an information system's life cycle.
2. The Director of Information Security defines the strategy for the appropriate security of all software and web applications, as well as to monitor, establish and enforce remediation timelines and sanctions for non-compliant systems campus-wide. The Information Security Office (ISO) will establish security standards for the acquisition, development, deployment and maintenance of all software and web applications handling sensitive information or that are accessible from off campus. These standards will ensure that fundamental security principles are incorporated, such as those generally incorporated into the National Institute of Standard Technology (NIST), Information Technology Infrastructure Library (ITIL) and System Administration and Network Security (SANS) frameworks.
3. **Acquisition** - All campus software and web application acquisitions or upgrades involving handling of information and/or access from off campus must be reviewed and approved by the Director of Information Security or his/her designee(s) in writing prior to purchase or implementation. All contracts for work involving handling of information and/or access from off campus must also be reviewed and approved by the Director of Information Security or his/her designee(s) in writing prior to acquisition.
    a. Vendor acquisitions - If an enterprise information system or component of that system is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of this policy and any special security requirements of the system. The vendor must allow testing of the system's security controls by the ISO or an independent third party, if needed.
4. **Development** - All application and web developers must familiarize themselves and follow the campus Application Development Standards to ensure they are employing secure procedures for any application or web development involving University data. All application code for such applications must be reviewed and approved in writing by the ISO prior to deployment. All significant changes in application code must also be reviewed for vulnerabilities prior to deployment. All applications or web processes handling, processing or storing critical or sensitive University information must be housed only within secured data centers approved by the Director of Information Security and run on secured systems meeting all applicable security policies and standards approved by the ISO.
    a. System security plans and documentation - System security plans and documentation must be prepared for all enterprise information systems or other systems under development 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. Such plans should provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements through all stages of the system's life cycle. When the system is modified in a manner that affects security, system documentation must be updated accordingly.

b. Separate development, testing, and production environments - System development, testing, and production should be performed in separate environments.

5. **Maintenance and Testing** - Access to source code and other critical system resources during testing, development, or production must be limited to only authorized personnel with an authorized work-related need.
    a. Test data - Testing of enterprise information systems should be done with fabricated data that mimics the characteristics of the real data, or on copies of real data with any confidential data appropriately sanitized. Testing should not be done on live data due to the threat to its confidentiality and/or integrity. Testing that requires the use of live data or confidential data must have appropriate security controls employed.
    b. Vulnerability management - An assessment of the system's security controls and a vulnerability assessment that seeks to identify weaknesses that may be exploited must be performed on all new enterprise information systems or ones undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed on production enterprise information systems and appropriate measures taken to address the risk associated with identified vulnerabilities. Vulnerability notifications from vendors and other appropriate sources should be monitored and assessed for all systems and applications associated with enterprise information system.
6. **Responsibilities**:
    a. Information Security Office (ISO) - Coordinates the development, review, and approval of system security plans as well as the identification, implementation, and assessment of common security controls; oversees periodic vulnerability assessments for enterprise information systems; and coordinates implementation of other assessments as needed with information system security administrators.
    b. System Administrator - Ensures the implementation of appropriate operational security controls for an information system; coordinates with the ISO in the identification, implementation, and assessment of common security controls; plays an active role in developing and updating a system security plan and coordinating with an information system owner any changes to the system and assessing the security impact of those changes. This role may be filled by someone directly involved with the development, maintenance, and/or operation of the information system.

VII. NON-COMPLIANCE AND SANCTIONS

1. Violations of this policy may require the removal of any unapproved IT Resources at the department's or school's expense, and may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a school.

By Direction of the CIO:

Mira Lalovic-Hand,
SVP and Chief Information Officer