ROOSEVELT UNIVERSITY

RU Policy No. 7.14

Responsible Division: Information Technology Services

Originally Issued: 1/2021

Last Revised: 04/2022

Revised Effective Date: 04/2022

Information Security Policy

Policy Statement

The purpose of this policy is to assist Roosevelt University in its efforts to fulfill its responsibilities relating to the protection of information assets and comply with regulatory and contractual requirements involving information security and privacy. This policy framework consists of eighteen (18) separate policy statements, with supporting Standards documents, based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-171.

Although no set of policies can address every possible scenario, this framework, taken as a whole, provides a comprehensive governance structure that addresses key controls in all known areas needed to provide for the confidentiality, integrity and availability of the organization's information assets. This framework also provides administrators guidance necessary for making prioritized decisions, as well as justification for implementing organizational change.

This Information Security Policy serves to clearly establish Roosevelt University's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Roosevelt University fulfils these objectives through the implementation of a comprehensive University-wide Information Security Program.

The University reserves the right to modify or amend this Policy at any time, at its sole discretion. Any change to this Policy will become effective at the time designated above. This Policy does not constitute an express or implied contract between Roosevelt University and any past, present, or prospective student, employee (including administrator, faculty, or staff), contractor, or volunteer.

This Policy governs conduct on all of the University's properties. Unless otherwise stated, the term "Employee" as used in this Policy shall refer to all employees (including administrators, faculty, and staff), contractors, volunteers, lessees, and renters.

Policy

1.0 SCOPE

The scope of this policy includes all information assets owned and/or managed by the organization. All personnel and service providers who have access to or utilize assets of the organization, including data at rest, in transit or in process shall be subject to these requirements. This policy applies to:

- All information assets and IT resources operated by the organization;
- All information assets and IT resources provided by the organization through contracts, subject to the provisions and restrictions of the contracts; and
- All authenticated users of Roosevelt University information assets and IT resources.

2.0 IMPLEMENTATION

Roosevelt University needs to protect the confidentiality, integrity, and availability of data while providing information resources to fulfill the organization's mission. The Information Security Program must be risk-based, and implementation decisions must be made based on addressing the highest risk first.

Roosevelt University's administration recognizes that fully implementing all controls within the NIST Standards is not possible due to organizational limitations and resource constraints. The University must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practicable.

3.0 ROLES AND RESPONSIBILITIES

Roosevelt University has assigned the following roles and responsibilities:

1. **Chief Information Officer**: The Chief Information Officer is accountable for the implementation of the Information Security Program including:
    a. Security policies, standards, and procedures
    b. Security compliance including managerial, administrative, and technical controls

    The Chief Information Officer is to be informed of information security implementations and ongoing development of the Information Security Program design.

2. **Information Security Officer**: The Information Security Officer is responsible for the development, implementation, and maintenance of a comprehensive Information Security Program for Roosevelt University. This includes security policies, standards

and procedures which reflect best practices in information security. Roosevelt University may engage a third party to support or perform this role.

3. **Data Security Team**: This group is responsible for the design, implementation, operations and compliance functions of the Information Security Program for all Roosevelt University constituent units. The team is comprised of technology infrastructure staff, systems administrators, and application administrators. This team functions as the Information Security Program Office.
4. **Application Administrators**: These individuals are responsible for the implementation, operations and compliance functions of the Information Security Program for centralized and decentralized software applications or tools. All centralized and decentralized software applications must have an administrator specified to fulfil these responsibilities.

4.0 DATA, INFORMATION, AND SYSTEM CLASSIFICATION

Roosevelt University must establish and maintain security categories for both information and information systems. For more information, reference the Data Classification Policy.

5.0 PROVISIONS FOR INFORMATION SECURITY STANDARDS

The Roosevelt University Security Program is framed on National Institute of Standards and Technology (NIST) and controls implemented based on SANS Critical Security Controls priorities. Roosevelt University must develop appropriate control standards and procedures required to support the organization's Information Security Policy. This policy is further defined by control standards, procedures, control metrics and control tests to assure functional verification.

The Roosevelt University Security Program is based on NIST Special Publication 800-53. This publication is structured into 18 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements.

5.1 ACCESS CONTROL (AC)

Roosevelt University must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

5.2 AWARENESS AND TRAINING (AT)

Roosevelt University must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security

of organization information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

5.3 AUDIT AND ACCOUNTABILITY (AU)

Roosevelt University must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

5.4 ASSESSMENT AND AUTHORIZATION (CA)

Roosevelt University must: (i) periodically assess the security controls in organization information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organization information systems; (iii) authorize the operation of the organization's information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

5.5 CONFIGURATION MANAGEMENT (CM)

Roosevelt University must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

5.6 CONTINGENCY PLANNING (CP)

Roosevelt University must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the organization's information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

5.7 IDENTIFICATION AND AUTHENTICATION (IA)

Roosevelt University must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Roosevelt University information systems.

5.8 INCIDENT RESPONSE (IR)

Roosevelt University must: (i) establish an operational incident handling capability for organization information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organization officials and/or authorities.

5.9 MAINTENANCE (MA)

Roosevelt University must: (i) perform periodic and timely maintenance on organization information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

5.10 MEDIA PROTECTION (MP)

Roosevelt University must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) use encryption, where applicable, (iv) sanitize or destroy information system media before disposal or release for reuse.

5.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

Roosevelt University must: (i) limit physical access to information systems, equipment and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

5.12 PLANNING (PL)

Roosevelt University must develop, document, periodically update and implement security plans for organization information systems that describe the security controls in place or planned for the information systems as well as rules of behavior for individuals accessing the information systems.

5.13 PERSONNEL SECURITY (PS)

Roosevelt University must: (i) ensure that individuals occupying positions of responsibility within the organization are trustworthy and meet established security criteria for those positions; (ii) ensure that organization information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with Roosevelt University security policies and procedures.

5.14 RISK ASSESSMENT (RA)

Roosevelt University must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

5.15 SYSTEM AND SERVICES ACQUISITION (SA)

Roosevelt University must: (i) allocate sufficient resources to adequately protect organization information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures, through federal and state law and contract, to protect information, applications, and/or services outsourced from the organization.

5.16 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Roosevelt University must: (i) monitor, control and protect organization communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within organization information systems.

5.17 SYSTEM AND INFORMATION INTEGRITY (SI)

Roosevelt University must: (i) identify, report and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organization information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

5.18 PROGRAM MANAGEMENT (PM)

Roosevelt University must implement security program management controls to provide a foundation for the organizational Information Security Program.

6.0 ENFORCEMENT

Roosevelt University may temporarily suspend or block access to any individual or device when it appears necessary to do so in order to protect the integrity, security or functionality of organization and computer resources.

7.0 PRIVACY

Roosevelt University must make every reasonable effort to respect a user's privacy. However, personnel do not acquire a right of privacy for communications transmitted or stored on organization resources.

Additionally, in response to a judicial order or any other action required by law or permitted by official organization policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the organization, the University designates "responsible administrators" who may access, review, monitor and/or disclose computer files associated with an individual's account. The responsible administrators are: the President for cases involving members of the Executive Council, the Provost and Executive Vice President for cases involving academic deans and faculty, the Vice President for Human Resources for cases involving staff and administrators, and the Vice President/Dean of Students for cases involving students.

Entities Affected by this Policy

All Divisions of the University.

Related Documents

All University Policies, including: Acceptable Use of Electronic Resources; Data Classification Policy.

Revision and Implementation

The Chief Information Officer shall have the authority to revise this Policy, subject to the approval of the President's Executive Council.

All University Vice Presidents and Deans shall have the authority to establish any procedures necessary to implement this Policy.