RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Audit and Monitoring					
Section #:	70.1.8	**Section Title:**	Information Technology: Information Technology Policies		**Formerly Book:**	N/A
Approval Authority:	Executive Vice President – Chief Financial Officer and University Treasurer		**Adopted:**	03/31/2021	**Reviewed:**	
Responsible Executive:	Senior Vice President & Chief Information Officer		**Revised:**			
Responsible Office:	Office of Information Technology (OIT)		**Contact:**	mailto:oit-policies@oit.rutgers.edu		

1. **Policy Statement**

   This policy is to protect Rutgers, The State University of New Jersey's assets, protect information systems from unauthorized activities, and to ensure compliance with applicable laws and regulations and, as needed, to comply with subpoenas, court orders and e-discovery.

2. **Reason for Policy**

   To establish an Audit and Monitoring policy for the University's Information Technology environment.

3. **Who Should Read This Policy**

   All members of the Rutgers University community.

4. **Resources**

   University Policy Library: Information Technology - Section 70

   University Policy Library: Clinical, Compliance, Ethics & Corporate Integrity - Section 100

   University Policy 30.4.5: Records Management

   University Policy 50.3.18: Data Breach Management

   University Policy 70.1.2: Information Classification

   University Policy 70.1.3: Incident Management

5. **Definitions**

   Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies, and operational procedures. [National Institute of Standards and Technology Special Publication 800-12]

Audit Log: A chronological record of information system activities, including records of system accesses and operations performed in a given period. [National Institute of Standards and Technology Special Publication 800-171]

Availability: The expectation that information is accessible by the University community when needed.

Confidentiality: The expectation that only authorized individuals, processes, and systems will have access to University information.

Guideline: Advice on the ways to comply with policy, written for non-technical users who have multiple options for secure information handling processes.

Information Owner: The official in a business unit that brings data into the University and who is responsible for its appropriate use and protection and retains that responsibility even when the information is shared.

Integrity: The expectation that the University's information will be protected from unintentional, unauthorized, or accidental changes.

Monitoring: Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected. [National Institute of Standards and Technology Special Publication 800-160]

Procedure: Step by step instructions and implementation details for personnel to perform specific tasks in ways that ensure that the associated preventive, detective, and response mechanisms work as planned.

Technology Standard: A formal document that establishes uniform engineering and technical configuration parameters and associated values, methods, practices, or processes that ensure management can secure University assets and comply with University policy and regulatory requirements.

6. **The Policy**

A. **Introduction:**

The University maintains information assets that are essential to the University's mission.

The University has the right and obligation to audit and monitor access to its electronic information, information systems, and information technology infrastructure, some of which are protected by federal and State laws and regulations. It uses the information produced from audit and monitoring activities to protect against, anticipate, and respond to threats to the confidentiality, availability, and integrity of its information assets and to ensure that policies and programs protecting its information assets continue to be effective.

These activities are not intended to restrict or utilize the content of legitimate academic and business communications

Requirements:

1. **Executive/Senior/Vice Presidents~~,~~ Chancellors, and Deans must:**

a. Ensure the implementation of this policy by the organizations under their purview.

b. Establish, maintain, and disseminate documentation, such as Technology

Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

2. **Directors and Department Chairs must:**

   a. Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

3. **Information Owners must:**

   a. Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

   b. If a security breach event is discovered, adhere to the security requirements outlined in University Policy 70.1.3: Incident Management.

   c. Identify transactions, events, or activities that are sensitive or critical to the appropriate function of the system or to the information housed in the system that are unlawful, unauthorized, suspicious, or indicative of unusual activity and ensure those actions are appropriately monitored. The actions may include but are not limited to:

      i. User activities that have not been explicitly authorized;

      ii. Excessive unsuccessful log-in attempts;

      iii. Attempts to use privileges that have not been authorized; and

      iv. Unauthorized modifications to information systems.

4. **System Owners must:**

   a. Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

   b. If a security breach event is discovered, adhere to the security requirements outlined in University Policy 70.1.3: Incident Management.

   c. Identify transactions, events, or activities that are sensitive or critical to the appropriate function of the system or to the information housed in the system that are unlawful, unauthorized, suspicious, or indicative of unusual activity and ensure those actions are appropriately monitored. The actions may include but are not limited to:

      i. All actions undertaken by system administrators who have elevated privileges and access rights;

      ii. User activities that are not explicitly authorized;

      iii. Excessive unsuccessful log-in attempts;

      iv. Attempts to use privileges that have not been authorized; and

      v. Unauthorized modifications to information systems.

d. Ensure Audit logs:

i. Are retained to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

ii. Contain sufficient information such that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

iii. Alert in the event of an audit logging process failure; and

iv. Are protected from unauthorized access, modification, and deletion.

e. Review the audit logs on a periodic basis, investigating and reporting on unauthorized or suspicious activity.

f. Cooperate when dealing with auditors, assisting as needed, and providing documentation that information identified as Critical or Restricted is properly protected when transmitted

5. **Office of Information Technology (OIT) must:**

a. Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

b. If a security breach event is discovered, adhere to the security requirements outlined in University Policy 70.1.3: Incident Management.

c. Identify transactions, events, or activities that are sensitive or critical to the appropriate function of the system or to the information housed in the system, that are unlawful, unauthorized, suspicious, or indicative of unusual activity and ensure those actions are appropriately monitored. The actions may include but are not limited to:

i. All actions undertaken by system administrators who have elevated privileges and access rights;

ii. User activities that are not explicitly authorized;

iii. Excessive unsuccessful log-in attempts;

iv. Attempts to use privileges that have not been authorized; and

v. Unauthorized modifications to information systems.

d. Ensure the clocks of all relevant information processing systems are synchronized to a single reference time source.

e. Ensure Audit logs:

i. Are retained to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

ii. Contain sufficient information such that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

iii. Alert in the event of an audit logging process failure; and

iv. Are protected from unauthorized access, modification, and deletion.

f. Review the audit logs on a periodic basis, investigating and reporting on unauthorized or suspicious activity.

g. Cooperate when dealing with auditors, assisting as needed, and providing documentation that information identified as Critical or Restricted is properly protected when transmitted.

6. **Non-Compliance and Sanctions**

Failure to comply with this policy may result in denial or removal of access privileges to the University's electronic systems, disciplinary action under applicable University policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable State and federal statutes.