Ocean County College, Toms River, NJ

INFORMATION SYSTEMS
GENERAL

Information Systems Audit #9600

POLICY

Purpose

To establish a foundational framework for auditing and accountability that supports data security, regulatory compliance, and institutional integrity.

Scope

This policy applies to all systems, applications, and data—whether sensitive or public—owned, managed, or processed by Ocean County College (OCC) and its authorized personnel.

Policy Statement

Ocean County College is committed to protecting the confidentiality, integrity, and availability of institutional data. To ensure accountability for user actions and support incident response and forensic investigations, OCC will maintain an audit and accountability framework aligned with applicable laws, regulations, and recognized cybersecurity standards.
Key principles include:

- Implementing audit mechanisms to monitor system activity
- Protecting audit logs from unauthorized access or tampering
- Retaining audit data for appropriate durations
- Ensuring compliance with the Gramm-Leach-Bliley Act (GLBA) and NIST SP 800-171, Revision 3
- Handling records in accordance with N.J.A.C. Title 15, Chapter 3 – Records Retention

The IT Governance Council is responsible for oversight, enforcement, and periodic review of this policy.

Exceptions

Exceptions to this policy must be documented and approved by the IT Governance Council. Each exception must include a justification and a risk mitigation plan.

ADOPTED: October 9, 2025

PROCEDURE

Objective

To define the operational procedures that support the implementation of OCC's Information System Audit and Accountability Policy.

1. **Audit Logging Requirements**
   - All systems that store, process, or transmit sensitive data must generate audit logs capturing user access, administrative actions, and system events.
   - Logs must include timestamps, user identifiers, event types, and system sources.
2. **Log Protection and Retention**
   - Audit logs must be stored in secure, access-controlled environments.
   - Logs must be retained for a minimum of one year or longer if required by applicable regulations.
   - Logs must be reviewed regularly for anomalies or unauthorized activity.
3. **Data Classification and Safeguards**
   - Personal Identifying Information (PII) and other sensitive data must be protected at both system and user levels, as defined in the Data Classification #2220 Policy and Procedure.
   - Systems must implement encryption, access controls, and monitoring appropriate to the data classification.
4. **Data Retention and Disposal**
   - Data retention practices will be reviewed periodically to minimize unnecessary storage of sensitive information.
   - Records will be retained and disposed of in compliance with N.J.A.C. Title 15, Chapter 3 – Records Retention.
   - Physical media containing sensitive data must be stored securely, programmatically wiped, and/or physically destroyed when no longer in use.
5. **Exception Management**
   - Exceptions must be submitted to the IT Governance Council with:
     - A description of the system or application
     - Reason for exception
     - Risk mitigation strategies

ADOPTED: October 9, 2025