OAKLAND UNIVERSITY

ADMINISTRATIVE POLICIES AND PROCEDURES

860 INFORMATION SECURITY

SUBJECT: INFORMATION SECURITY

NUMBER: 860

AUTHORIZING BODY: PRESIDENT'S CABINET

RESPONSIBLE OFFICE: CHIEF OF STAFF

DATE ISSUED: MARCH 2005

LAST UPDATE: FEBRUARY 2026

RATIONALE:

In the course of carrying out its academic, research and clinical missions, faculty, staff, and students at Oakland University ("Oakland," "OU," or the "University") collect many different types of information, including financial, academic, medical, human resources, and other personal information. Federal and state laws and regulations, research agreements, contracts, and other industry standards impose obligations on the University to protect the information relating to faculty, staff, students, research subjects, and patients. This information is an important resource of the University, and any person who uses information collected by the University has a responsibility to maintain and safeguard its security, integrity, and availability.

POLICY:

A trusted and effective information technology (IT) environment with controls to ensure the security, integrity, and availability of Information Resources is vital to the University's ongoing mission of education, research, scholarship, and creative activity.

University Technology Services will:

1. Establish an overarching Information Security Program to establish an environment of internal controls designed to maintain, facilitate, and promote adequate protection of Information Resources through standards, procedures, guidelines, information-sharing, and training.

2. Protect Oakland University's electronic data through appropriate safeguards to ensure data privacy and security at each level of access and control.

Three Data Classifications: Confidential, Internal, and Public (Formerly referred to as Confidential, Operations Critical, and Unrestricted.)

- **Confidential Data**: Any information that is contractually protected as confidential information and any other information that is considered by the University appropriate for confidential treatment. See the Oakland University Data Classification Standard for examples of Confidential Data.
- **Internal Data**: Any information that is proprietary or produced only for use by members of the University community who have a legitimate purpose to access such data.
- **Public Data**: Any information that may or must be made available to the general public, with no legal restrictions on its access or use.

3. Foster collaboration among faculty, staff, researchers, students, and IT personnel to enhance security awareness and best practices. Recognizing the rapid evolution of technology, the University will adopt an adaptive security model to address emerging risks proactively.

4. Ensure access to Information Resources is governed, where possible, by role-based access controls (RBAC) and the principle of least privilege. University constituents will be granted access only to the resources necessary to fulfill their roles. Authentication mechanisms aligned with industry standards, including Multi-Factor Authentication (MFA), passkeys, and biometrics, will be implemented where applicable.

5. Support the responsibilities of Data Owners, Data Stewards, Data Custodians, and Data Users by providing clear guidelines and security measures to ensure appropriate data handling, storage, and transmission.

6. Manage security risks through administrative, technological, and physical controls. Regular risk assessments will be conducted to identify vulnerabilities, evaluate threats, and implement mitigating controls. Third-party vendors with access to University Information Resources will be subject to security reviews and contractual obligations.

7. Implement security and privacy controls to meet legal and regulatory requirements, including, but not limited to, FERPA, PCI, HIPAA, and other applicable state and federal laws.

8. Review Information Security Policies, standards, and procedures at least annually to ensure continued effectiveness and compliance with evolving threats, technological advancements, regulatory changes, and/or problems identified during risk assessments.

9. Ensure the resilience of IT operations by partnering with University stakeholders to develop a comprehensive Business Continuity Planning (BCP) framework. Critical systems and data will be identified, and contingency measures will be implemented to minimize operational disruptions, including redundancy, data backups, and recovery plans. Regular testing and updates of continuity plans will ensure preparedness for unforeseen events.

10. The University will establish an Incident Response (IR) program to detect, assess, respond to, and recover from security incidents in a timely manner. The IR Program will define roles and responsibilities, escalation procedures, and communication protocols. All incidents will be logged, analyzed, and reported as necessary to mitigate impact and enhance future resilience. The University will comply with relevant breach notification laws and coordinate with law enforcement or regulatory bodies when required.

Sanctions:

Failure to comply with the requirements of this policy will be considered inappropriate use of the University's Information Resources and, therefore, a violation of OU AP&P #890 Acceptable Use Policy. Sanctions for violating this policy will be implemented in accordance with the sanctions section of OU AP&P #890 Acceptable Use Policy.

SCOPE AND APPLICABILITY:

This policy is University-wide and applies to all individuals who access, use, or control Information Resources at the University.

DEFINITIONS:

- Capitalized terms used herein without definition are defined in the IT Terminology Standard.

PROCEDURES:

This Policy defines the key functions and roles in the Information Security Program, authorizing responsible personnel to execute security policies.

A. **Executive Management**

University senior officials (e.g., Provost, Deans, VPs, Department Chairs), following guidance from the Oakland University IT Governance Committee, are responsible for overseeing security compliance in their areas by:

- Ensuring System Owners and Data Owners appropriately identify, categorize, and protect data according to University policies and standards.
- Providing security training on Sensitive Data handling.
- Requiring IT Custodians to maintain an inventory of Information Resources and report to the Information Security Office.

B. **Security, Policy & Compliance Governance**

The IT Risk and Security/Compliance Steering Committee (ITRSCSC) is responsible for providing high-level strategic oversight for IT risk and security management, aligning efforts with university objectives, and ensuring compliance with regulations.

C. **Security Management**

The Information Security Office (ISO) within University Technology Services (UTS) is responsible for:

- Developing, documenting, and disseminating Information Security Policies and Standards.
- Selecting Security awareness training content for University personnel.
- Developing materials and advising the ITRSCSC.
- Translating Information Security Policies into technical requirements, standards, and procedures.
- Collaborating with Data and System Owners to determine appropriate means of securing Information Resources.
- Approving security exceptions or coordinating approval, as required, with the Chief Finance Officer and General Counsel.

Authority granted to UTS and the ISO by Executive Management includes:

- Monitoring network traffic and data transmissions.
- Conducting vulnerability scans, security assessments, and audits.
- Disconnecting non-compliant systems from the University network.
- Erasing University data on personal endpoints when required.
- Leading Incident Response efforts for security breaches.

The Chief Information Security Officer (CISO) manages the Information Security Program (ISP).

D. **Data Ownership**

Data Owners (Directors, Faculty, Research/Administrative Officers) are responsible for:

- Categorizing, setting retention standards, and inventorying University Data in alignment with OU classifications (Confidential, Internal, Public) as defined in

the OU Data Classification Standard and regulatory standards such as PCI and HIPAA.
- Establishing security requirements in coordination with the Information Security Office.
- Approving data access requests.
- Ensuring compliance with the Sanitization and Disposal of Information Resources.

E. **System Ownership**

System Owners (Faculty, Researchers, Administrative Officers) will manage IT systems by:

- Classifying Systems based on Data Owners' Data Classifications.
- Ensuring Sensitive Data systems undergo risk assessments.
- Establishing and implementing security controls with the Information Security Office.
- Maintaining system inventories and audit logs.
- Approving appropriate access to Systems.
- Ensuring compliance with the Sanitization and Disposal Policy.

F. **Technical Ownership**

IT Custodians will ensure secure infrastructure by:

- Maintaining Endpoint inventories.
- Conducting System and Network security checks and log reviews.
- Performing self-audits and reporting to the Information Security Office.
- Implementing technical security controls for data protection and following the Sanitization and Disposal Policy.

G. **System & Data Usage**

Users (faculty, staff, students, contractors) must:

- Follow the Oakland University Acceptable Use Policy.
- Take reasonable steps, including completing assigned training, to prevent unauthorized data access.
- Ensure appropriate security controls on the Systems they use are in place.

H. **Applicable Laws, Regulations, and Industry Standards**

The University shall adhere to applicable federal, state, local laws, and industry regulations and standards.

RELATED POLICIES AND FORMS:

- OU AP&P #890 Acceptable Use

APPENDIX: