The purpose of the Information Protection Policy is to provide direction and oversight over people, process, and technology employed to protect the confidentiality, integrity, and availability of University information and Information Systems (IS), while supporting the open, information-sharing needs of the University. Consequently, the security of Information Systems must include controls and safeguards to offset possible risks, as well as measures to ensure confidentiality, integrity and availability of University information and Information Systems.

The University of Oklahoma supports the Information Protection Policy where security measures must be taken to protect information and IS from unauthorized access, use, disclosure, disruption, modification, or destruction. The Information Protection Policy contains administrative, technical, and physical safeguards designed to protect University information and IS.

The intent of the Information Protection Policy is to:

- Define the Information Security Organization and overall roles and responsibilities related to information security.
- Comply with applicable laws, regulations, contractual obligations and OU policies.
- Identify Minimum Security Controls based on University mission.

This Information Protection Policy is not intended to prevent, prohibit, or inhibit the proper use of information assets as required to meet OU’s core mission and University’s academic, research and administrative goals.

The Information Protection Policy applies to:

- All information and Information Systems owned, leased, operated, or under the custodial care of the University;
- All information and Information Systems owned, leased, operated, or under the custodial care of third-parties operated on behalf of the University; and
- All individuals storing, processing, or transmitting University information.

In order to protect the confidentiality, integrity and availability of information and Information Systems, University of Oklahoma users must ensure their actions with respect to information and Information Systems that store, process, or transmit University information meet:

- OU IT Information Security Standards policy, and
- All applicable laws, University policies, and University contractual obligations

Individuals must report known non-compliance with this policy and associated Information Security
Standards to the University IT System Security GRC Office, ITGRC@ouhsc.edu, 405-271-2644.

Failure to comply with this policy and associated Information Security Standards may result in denied access to information and Information Systems, and disciplinary action, up to and including termination and dismissal.

**IT SECURITY PROGRAM MANAGEMENT**

**ID.AM Asset Management**
The University of Oklahoma Information Technology Business Unit must implement an Asset Management strategy that:

1. Identifies and records in an asset inventory, all physical Information Technology Assets. See OU IT Asset Management Standard.
2. Identifies and records in an asset inventory, all software platforms and applications. See OU IT Asset Management Standard.
3. Map Information System communication and data flows to ensure information protection strategies are appropriate to the University’s risk tolerance. See OU IT System Security Assessment Process.
5. Prioritizes Information Systems based on their classification, criticality, and business value. See OU Information Classification Standard.
6. Establish roles and responsibilities for all University Personnel, including third-party stakeholders.

**ID.BE Business Environment**
University of Oklahoma Business Units operating Information Technology must:

1. Submit a System Security Assessment request for Information Systems:
   a. At the time of purchase or design, and prior to use; or
   b. At the time of contract execution.
2. Identify and communicate to University Data Stewards, the University’s place in critical infrastructure.
   See:
   - OU IT Category A – Healthcare Information Protection Standard
   - OU IT Category B – Payment Card Data Protection Standard
   - OU IT Category C - Education Information Protection Standard
   - OU IT Category D1 – Confidential Research Information Protection Standard
   - OU IT Category D2 – Research Information Protection Standard
   - OU IT Category E – Admin and Finance Information Protection Standard
   - OU IT Category F – Public Information Protection Standard
3. Establish and prioritize Information Security strategy based on organizational mission, objectives, and activities. See OU IT Cybersecurity Roadmap.
4. Establish dependencies and critical functions for delivery of University defined critical services. See OU IT System Security Assessment Process.
5. Establish resilience requirements to support delivery of University defined critical services. See OU IT System Security Assessment Process.

**ID.GV Governance**
The University of Oklahoma Information Technology Business Unit must implement a Governance strategy that:

1. Establishes the University of Oklahoma Information Security Policy. See OU IT PSP Program.
(2) Aligns roles and responsibilities with internal roles and external partners.
(3) Manages the University’s legal and regulatory requirements regarding cybersecurity. See OU IT Legal and Regulatory Compliance Policy.
(4) Addresses cybersecurity risks through the use of governance and risk management process. See OU IT Risk Management Program.

ID.RA Risk Assessment
The University of Oklahoma Information Technology Business Unit must implement a Risk Assessment Strategy that:

(1) Identifies and documents OU IT asset vulnerabilities. See OU IT System Security Assessment Process.
(2) Receives threat and vulnerability information from information sharing forums and sources. See OU IT System Security Assessment Process.
(3) Identifies and documents threats, both internal and external. See OU IT System Security Assessment Process.
(4) Identifies potential business impacts and likelihood. See OU IT System Security Assessment Process.
(6) Identifies and prioritizes risk responses. See OU IT Risk Management Program.

PR.AC Access Control
University of Oklahoma Business Units operating Information Technology must implement an Access Control strategy that:

(1) Through the use of people, process, and technology must manage user and device identities or credentials in accordance with the OU IT Access Control Standard.
(2) Facilities storing, processing, or transmitting University information must employ physical access controls to prevent the theft of, tampering with, or destruction of information and Information Systems. See OU IT Facility Security Standard, and OU IT Workspace Security Standard.
(3) OU IT must provide secure remote access mechanisms to permit authorized users to access University information or Information Systems from outside the University of Oklahoma wired or other wireless network. See OU IT Remote Access Standard.
(4) Permits Information System Administrators or Data Managers the ability implement and document procedures to ensure that access rights are properly managed throughout their lifecycle. See OU IT Access Control Standard.
(5) OU IT must monitor, control, and protect the flow of University information (i.e., information transmitted or received by Information Systems). See OU IT Network Security Standard.

PR.AT Awareness and Training
The University of Oklahoma Information Technology Business Unit must implement an Awareness and Training Strategy that:

(1) Ensures that Users of Information Systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those Information Systems. See OU IT Awareness and Training Standard.
(2) Identifies and requires OU Admin Account Users complete role-based training.
(3) Identifies and requires University Senior Executives understand roles and responsibilities.
(4) Identifies and requires OU IT Purchasing to include contract language indicating the responsibility of the third party as it pertains cybersecurity risks identified during the System Security Assessment.
(5) Requires University Personnel responsible for implementing physical security controls to
undergo awareness training upon changes to the OU IT Facility Security and OU IT Workspace Security Standard.

PR.DS Data Security
University of Oklahoma Business Units operating Information Technology must implement a Data Security strategy that:

1. Protects University Information while being stored in accordance with OU IT Information Protection Standards.
2. Protects University Information while being transmitted in accordance with OU IT Information Protection Standards.

PR.IP Information Protection Process and Procedures
The University of Oklahoma Information Technology Business Unit must implement Information Protection Processes and Procedures that:

1. Establish baseline configuration requirements of Information Systems based on University mission and Information classification:
   - OU IT Category A – Healthcare Information Protection Standard
   - OU IT Category B – Payment Card Data Protection Standard
   - OU IT Category C - Education Information Protection Standard
   - OU IT Category D1 – Confidential Research Information Protection Standard
   - OU IT Category D2 – Research Information Protection Standard
   - OU IT Category E – Admin and Finance Information Protection Standard
   - OU IT Category F – Public Information Protection Standard
   - OU IT Network Security Standard
   - OU IT Server Security Standard
   - OU IT User Device Security Standard
   - OU IT Mobile Device Security Standard
2. Defines the documentation and approval required to make configuration changes to University Information Systems. See OU IT Change Management Standard.
3. Requires Information System or Data Owners to define an Information Backup plan. See OU IT Information Backup Standard.
4. Requires Information Systems or Data Owners properly dispose of storage media, which includes but is not limited to optical media (CDs or DVDs), magnetic media (tapes or diskettes), disk drives (external, portable, or removed from Information Systems), flash memory storage devices (SSDs or USB flash drives) and documents (paper documents, paper output, or photographic media). See OU IT Storage Media Security Standard.
5. Establishes a Cybersecurity Incident Response Plan that includes preparation, detection, analysis, containment, recovery, and user response activities to track, document, and report on incidents. See OU IT Security Incident Response Plan.

PR.PT Protective Technology
The University of Oklahoma Information Technology Business Unit must implement Protective Technology that:

1. Create and retain audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized, or inappropriate Information System activity. See OU IT Information System Logging Standard.
2. Requires storage media, which includes but is not limited to optical media (CDs or DVDs),
magnetic media (tapes or diskettes), disk drives (external, portable, or removed from Information Systems), flash memory storage devices (SSDs or USB flash drives) and documents (paper documents, paper output, or photographic media), be used and disposed of securely. See OU IT Storage Media Security Standard.

(3) Requires OU IT, Information System Owners, or Administrators to configure Information Systems to employ a role-based access control (RBAC) model that restricts Information System access to authorized users assigned a role. See OU IT Access Control Standard.

(4) Requires OU IT to monitor, control, and protect communications (i.e., information transmitted or received by Information Systems) at the external boundaries and key internal boundaries of Information Systems. See OU IT Network Security Standard.

REFERENCES

- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI) Data Security Standards
- National Institute of Standards and Technology Special Publication 800-17, Controlled Unclassified Information
- Gramm-Leach-Bliley Act (GLBA)
- Family Education Rights and Protection Act (FERPA)

ENFORCEMENT AND COMPLIANCE

Failure to comply with this policy or other applicable laws, policies, and regulations may result in the limitation, suspension, or revocation of user privileges and may further subject the user to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, University policies, and applicable laws. This policy is enforced by the OU Chief Information Officer. Internal Audit, or other departments, may periodically assess compliance with this policy and may report violations to the Board of Regents.

IT EXCEPTIONS

The CIO acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this standard. Such instances must call the Information Protection Policy exception process. Each exception request is carefully considered by the Information Owner, Information System Owner, OU IT Security Advisory Council and the CIO. See OU IT Information Protection Policy Exception Standard.

Table 1 Revision History

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Version</th>
<th>Revised By</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/14/2019</td>
<td>1.0</td>
<td>OU IT, April Lee</td>
<td>Baseline Version</td>
</tr>
</tbody>
</table>
| 10/21/2019    | 1.0     | OU IT, April Lee    | Line 6, replaced “while supporting the open, information-sharing needs of OU’s community members” with “while supporting the open, information-sharing needs of the University.” Line 19, removed the term “business” from “University business mission.” Line 31, Replaced "All individuals accessing, using, holding, or managing University information or Information Systems on behalf of the University” with "All individuals storing, processing, or transmitting University information," Line 70, Repalced "103-01 The University of Oklahoma has identified and communicated three...
business missions:
1) Healthcare,
2) Higher Education, and
3) Research.
Information System Owners and/or Information System Administrators must report to OU IT GRC, at the initiation of an Information System, the Information System's role in supporting the University's business missions." with "University of Oklahoma Business Units operating Information Technology must:
(1) Submit a System Security Assessment request for Information Systems:
   a. At the time or purchase or design, and prior to use; or
   b. At the time of contract execution.
(2) Identify and communicate to University Data Stewards, the University's place in critical infrastructure.
See:
OU IT Category A – Healthcare Information Protection Standard
OU IT Category B – Payment Card Data Protection Standard
OU IT Category C - Education Information Protection Standard
OU IT Category D1 – Confidential Research Information Protection Standard
OU IT Category D2 – Research Information Protection Standard
OU IT Category E – Admin and Finance Information Protection Standard
OU IT Category F – Public Information Protection Standard
(3) Establish and prioritize Information Security strategy based on organizational mission, objectives, and activities. See OU IT Cybersecurity Roadmap.
(4) Establish dependencies and critical functions for delivery of University defined critical services. See OU IT System Security Assessment Process.
(5) Establish resilience requirements to support delivery of University defined critical services. See OU IT System Security Assessment Process."

Line 127, Replaced "108-03 University information and Information System users must be made aware of their obligation to know and follow the OU IT Acceptable Use Policy and OU IT Acceptable Use of Network Services Policy," with a requirement that OU IT implement an awareness and training strategy that "(1) Ensures that Users of Information Systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those Information Systems. See OU IT Awareness and Training Standard."

Line 135, Replaced "pertains to Information Security" with "pertains to cybersecurity risks identified during the System Security Assessment." Line 143, Replaced "109-03 Information System Owners or Information System Administrators must encrypt University-owned workstations located in off-campus clinic facilities subject to HIPAA and University-owned workstations located in public
clinical areas (e.g., reception, waiting, or check-in areas)."

"(1) Protects University Information while being stored in accordance with OU IT Information Protection Standards.
(2) Protects University Information while being transmitted in accordance with OU IT Information Protection Standards."

Line 212, Added "University policies" to the default enforcement and compliance language. Line 221, Added “See OU IT Information Protection Policy Exception Standard” to line 221. This document will be added to the OU IT PSP Roadmap.

Table 2 Approval History

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Approved by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>1/12/2020</td>
<td>Interim President, Joseph Harroz</td>
</tr>
</tbody>
</table>

Table 3 Review History

<table>
<thead>
<tr>
<th>Version</th>
<th>Review Date</th>
<th>Reviewed by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>12/10/2019</td>
<td>Information Security Review Board</td>
</tr>
<tr>
<td>1.0</td>
<td>12/15/2019</td>
<td>Security Governance Advisory Council</td>
</tr>
</tbody>
</table>