STANDARD STATEMENT

Pursuant to the OU Information Protection Policy, the University of Oklahoma Information Technology Business Unit is responsible for developing and managing the University’s strategy to prioritize Information Systems based on their classification, criticality, and business value.

This Standard reflects the University’s commitment to identify and implement security controls that mitigate risks to Information and Information Systems, to reasonable and acceptable levels. This Standard establishes the University’s framework for classifying University Information. Classification of University Information will aid in identifying baseline security controls for the protection of the Information. The examples below are not exhaustive, users should contact the System Security Governance, Risk and Compliance for assistance with classifying their Information.

University Information is information generated by or for, owned by, or otherwise in the possession of the University of Oklahoma that is related to the University’s missions of higher education, research, and service. University Information may exist in any format (i.e. electronic, paper). University Information System or Data Owners must classify information in accordance with the OU IT Information Classification Matrix.

SCOPE

This Standard applies to all University of Oklahoma Information generated by or for, owned by, or otherwise in possession of University Personnel in support of the University’s missions.

CONTROL DETAILS AND SAMPLE FORMAT

Each control group is organized under its group identification code and title.

Information about each control in a group is presented in the following format:

<table>
<thead>
<tr>
<th>Control ID #</th>
<th>Title</th>
<th>OU IT Control Number</th>
<th>Control Name</th>
</tr>
</thead>
</table>

RISK STATEMENT
[A high-level statement of the potential risk present by not addressing the control activity.]

CONTROL DESCRIPTION
[Detailed control description.]

INFORMATION SYSTEM CLASSIFICATION SCOPE

<table>
<thead>
<tr>
<th>Category A</th>
<th>Category B</th>
<th>Category C</th>
<th>Category D1</th>
<th>Category D2</th>
<th>Category E</th>
<th>Category F</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

IMPLEMENTATION

OU IT Control #
[University requirements for the implementation of information security controls.]

NOTES ON THE CONTROL DETAILS AND SAMPLE FORMAT

- CONTROL ID, CONTROL TITLE
The Control ID and Control Titles are brought in directly from HIPAA Administrative Simplification Regulation Text. OU IT Governance, Risk, and Compliance maintains a mapping of the common security and regulatory systems.
- **CLASSIFICATION SCOPE**
The Classification Scope identifies which Information Systems should apply the implementation requirements.

- **IMPLEMENTATION**
Implementation statements are meant to align with the law and regulations, State of Oklahoma Policy, Procedures, Standard and Guidelines, as well as University IT Policy and Standards.

**STANDARD CONTROL STATEMENTS**

Information Systems and Information are considered assets of the University. As assets, they must be classified and protected according to the risks associated with their classification.

<table>
<thead>
<tr>
<th>Control ID # - ID.AM-5</th>
<th>RISK STATEMENT</th>
<th>CONTROL DESCRIPTION</th>
<th>INFORMATION SYSTEM CLASSIFICATION SCOPE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>University Information Systems are not prioritized based on their classification, criticality, and business value to ensure data protection requirements align with business objectives and the University's risk strategy.</td>
<td>Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value</td>
<td>Category A ✓</td>
</tr>
</tbody>
</table>

**IMPLEMENTATION**

ID.AM-5-1 The University of Oklahoma has defined Category E – University Administrative and Financial Information as the default classification for all University Information. Information Protection requirements documented in the Category E – University Administrative and Financial Information Protection Standard must be applied at minimum for University Information Systems.

ID.AM-5-2 The University of Oklahoma System Security Governance, Risk, and Compliance (GRC) Team must classify information in accordance with the OU IT Information Classification Matrix; document and maintain a source of record for Information Systems and/or Information Assets in accordance with the OU System Security Assessment Process:

- (i) At the time of purchase, renewal, or design of Information Technology; or
- (ii) At the time of contract execution where security requirements are stated in contract language.

ID.AM-5-3 Information System or Data Managers must:

- (i) Identify and report the use of Information Systems that store, process, or transmit University Information as part of the OU System Security Assessment Process;
- (ii) Provide sufficient details during the System Security Assessment to allow for classification of University Information stored, processed, or transmitted by an Information System.

**OU IT Information Classification Matrix**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category A</td>
<td>Healthcare Data</td>
</tr>
<tr>
<td>Description</td>
<td>Data that is legally regulated by the Health Insurance Portability and Accountability Act of 1996 to protect the confidentiality, integrity, and availability of the data. Healthcare data that has regulation that determines the requirements and penalties associated with release</td>
</tr>
<tr>
<td>Confidentiality</td>
<td><strong>Scope of access:</strong> Intended access by as few users as possible and based on minimum necessary or least privilege. <strong>Disclosure requirements:</strong> May not be disclosed outside those allowed by role or responsibility to know.</td>
</tr>
<tr>
<td>Business Impact</td>
<td>Seriously impairs the functioning of the University to provide Healthcare services, or results in material financial, legal or reputational loss.</td>
</tr>
</tbody>
</table>
| Examples | **Information Systems (IS) or documentation of IS with access to regulated data**  
**Protected Health Information (PHI)**  
- Medical records  
- Health Insurance Plan information  
- Healthcare service payments  
**Human Participant Research Information**  
- ePHI identifiers, see University of Oklahoma HIPAA Policy, De-Identification/Re-Identification of PHI.  
- Treatment records  
**OU Clinical Enterprise** |

### Category B – Payment Card Data

| Description | Data that is governed by Payment Card Industry (PCI) Data Security Standards to protect the confidentiality, integrity, and availability of the data. Payment Card data that has regulation that determines the requirements and penalties associated with release |
| Confidentiality | **Scope of access:** Intended for access only by those with a need to know. **Disclosure requirements:** May not be disclosed outside those allowed by role or responsibility to know. |
| Business Impact | Significantly impairs the functioning of the University or results in significant financial, legal or reputational loss. |
| Examples | **Business/Financial Data**  
- Cardholder name  
- Credit/debit card account number  
- Credit/debit card expiration date  
- Credit/debit card verification number |
<table>
<thead>
<tr>
<th><strong>Category C – Education</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
</tr>
<tr>
<td><strong>Business Impact</strong></td>
</tr>
<tr>
<td><strong>Examples</strong></td>
</tr>
</tbody>
</table>
| * exceptions apply | - FERPA student records (including Student ID)  
- Access device numbers (card number, building access code, etc.) used to protect student records information  
- Loan or scholarship information  
- Payment history  
- Student tuition bills  
- Student financial services information  
- Class lists or enrollment information  
- Transcripts and/or student grade reports  
- Student assessments  
- Student assignments  
- Student tests  
- Notes on student performance  
- Disciplinary action  
- Athletics or department recruiting information  

**Specific for students:** Class year  
- Participation in campus activities and sports  
- Weight and height (athletics)  
- Dates of attendance  
- Status |
| Description | Research data under which the University is obligated to protect the confidentiality and disclosure of data would impact the University’s mission to conduct research. |
| Confidentiality | **Scope of access:** Intended access by users with a “need to know” as required by their job function or role.  
**Disclosure requirements:** May not be disclosed outside those allowed by role or responsibility to know, requires notification to a funding Sponsor, and could result in a financial penalty if disclosed. |
| Business Impact | Seriously impairs the functioning of the University to provide Confidential Research services, or results in material financial, legal or reputational loss. |
| Examples * exceptions apply | • Contracts and contract data referencing the labels below:  
  o Export Controlled Research (ITAR)  
  o Controlled Unclassified Information (CUI)  
  o National Institutes of Health (NIH)  
  o IACUC Protocol(s)  
  o Animal Specimen Veterinary Records  
  o For Official Use Only (FOUO)  
  o Controlled Unclassified Information (CUI)  
  o Sensitive But Unclassified (SBU)  
  o Limited Official Use (LOU)  
  o Sensitive Unclassified Information (SUI)  
  o Law Enforcement Sensitive |
<table>
<thead>
<tr>
<th>Category D2 –Research &amp; Publications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Business Impact</strong></td>
</tr>
<tr>
<td><strong>Examples</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category E –University Administrative &amp; Financial</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Business Impact</strong></td>
</tr>
<tr>
<td><strong>Examples</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
• Records on spending, borrowing, net worth

**Anonymous Donor Information:** Last name, first name or initial (and/or name of organization if applicable) with any type of gift information (e.g., amount and purpose of commitment.)

**Other Donor Information:** Last name, first name or initial (and/or name of organization if applicable) with any of the following:

- Telephone/fax numbers, e-mail & employment information
- Family information (spouse(s), partner, guardian, children, grandchildren, etc.)
- Medical information

**Personally Identifiable Information (PII):** Last name and first name or initial, with any one of the following:

- Social Security Number
- Driver’s license number
- State ID card
- Passport number
- Federal Tax Information

**Authentication Verifiers**

- Passwords
- Cryptographic private keys

**Security/Safety Data**

- Emergency operations procedures and planning documents
- Facilities blueprints and utility documents
- Power plant
- OUPD data
- Disaster Recovery and Business Continuity plans

**Personal/Employee Data**

- OU Employee ID Numbers
- Income information and Payroll information
- Personnel records, performance reviews, benefit information
- Data and place of birth
- Worker’s compensation or disability claims

**Certain directory/contact information not designated by the owner as private**

- Name
- Campus address
- Email address
- Listed telephone number(s)
- Degrees, honors and awards
- Most recent previous educational institution attended
- Major field of study
- Dates of current employment, position(s)
- ID card photographs for University use

Management Data

- Detailed annual budget information
- Conflict of Interest Disclosures
- University's investment information

Information Technology Information

- Server Event Logs
- Non-published Information Technology Policy, Standard and Procedures
- Network diagrams
- Technical blueprints
- Security documentation and procedures
- Licensed software/software license keys

<table>
<thead>
<tr>
<th>Category F – Public</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
</tr>
<tr>
<td><strong>Business Impact</strong></td>
</tr>
<tr>
<td><strong>Examples</strong></td>
</tr>
<tr>
<td>* exceptions apply</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

SUPPORTING POLICY AND STANDARDS
- Information Protection Policy
- OU IT Acceptable Use Policy
- University of Oklahoma HIPAA Privacy and Security Policies

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 800-171, Controlled Unclassified Information
- Gramm-Leach-Bliley Act (GLBA)
- Family Education Rights and Protection Act (FERPA)

ENFORCEMENT AND COMPLIANCE

Failure to comply with this standard 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, 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 be documented using the IT Policy and Standards Exception Process by a Business or Process Owner owning the risk and approved in advance by an authorized IT Executive (an owner of the IT Policy that governs the policy/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>01/18/2019</td>
<td>1.0</td>
<td>OU IT Systems Security</td>
<td>Baseline Version</td>
</tr>
<tr>
<td>10/22/2019</td>
<td>1.0</td>
<td>OU IT GRC</td>
<td>Line 29, defined GRC abbreviation. Line 46 Business Impact, revised to reflect education services. Line 47 Business Impact, revised to reflect confidential research services. Line 49 Business Impact, revised to “operate services”.</td>
</tr>
</tbody>
</table>
| 10/30/2019    | 1.0     | OU IT GRC       | Added to Page – Category C Examples:  
- Access device numbers (card number, building access code, etc.) used to protect student records information  
- Library paid subscription electronic resources  

Added to Page 4 – Category D1 Examples:  
- For Official Use Only (FOUO)  
- Controlled Unclassified Information (CUI)  
- Sensitive But Unclassified (SBU)  
- Limited Official Use (LOU)  
- Sensitive Unclassified Information (SUI)  
- Law Enforcement Sensitive  
- DEA Sensitive  
- Official Use Only (OUO)  
- Department Of Defense (DoD) Technical Information  
- Distribution Statements on Technical Documents  
- Sensitive Security Information  
- Protected Critical Infrastructure Information  
- Unclassified Controlled Nuclear Information  
- Export-Controlled Information  
- DFARS 252.204-7012  

Added to Page 5 – Category D2 Examples:  
- De-identified research data  

11/13/2019    | 1.0     | OU IT GRC       | Added “Treatment records” and “OU Clinical Enterprise” to the Category A examples.  

Added to Line 46, Control ID.AM-5-1: The University of Oklahoma has defined Category E – University Administrative and Financial Information as the default classification for all University Information. Information Protection requirements documented in the Category E – University Administrative and Financial Information Protection Standard must be applied at minimum for University Information Systems.  

Added “Student assessments”, “Student assignments”, and “Student tests” to the Category C examples. |
| 12/06/2019    | 1.0     | OU IT GRC       | Added Supporting Policy and Standards Section |

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>02/11/2020</td>
<td>Chief Information Officer</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>10/22/2019</td>
<td>OU IT GRC for consolidation of comments.</td>
</tr>
</tbody>
</table>