1.0 OVERVIEW AND PURPOSE

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All Lamar University data, whether electronic or printed, should be classified. The data owner, who is responsible for Data Classification, should consult with legal counsel on the classification of data as Confidential, Agency-Sensitive, or Public. Consistent use of data classification reinforces with users the expected level of protection of Lamar University data assets in accordance with Lamar University Security Policy.

The purpose of the Lamar University Data Classification Policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

2.0 SCOPE

The Lamar University Data Classification Policy applies equally to all individuals who use or handle any Lamar University Information Resource.

Lamar University data created, sent, printed, received, or stored on systems owned, leased, administered, or authorized by Lamar University are the property of Lamar University and its protection is the responsibility of the Lamar University owners, designated custodians, and users.

3.0 DEFINITIONS

Confidential - Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act)

LU Sensitive - Sensitive data that may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection.

Public - Information intended or required for public release as described in the Texas Public Information Act.
## 4.0 POLICY

The Data classification Matrix attached show recommended data classification.

### Data Classification Matrix

<table>
<thead>
<tr>
<th>Legal Requirements</th>
<th>Confidential</th>
<th>LU Sensitive</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High level of sensitivity</td>
<td>Moderate level of sensitivity</td>
<td>Low level of sensitivity</td>
</tr>
<tr>
<td>Protection of data is required by law, reduces liability and negative publicity</td>
<td>Protection of data will prevent poor business decisions, inaccurate research conclusions, potential liability, and moderate negative publicity</td>
<td>Public information that is intended for release to the public and its unauthorized disclosure would have no negative impact. While unauthorized disclosure of public information is against Lamar University Policy, it would not adversely impact Lamar University.</td>
<td></td>
</tr>
</tbody>
</table>

### Risk

- Long-term loss of reputation
- Long-term loss of research funding
- Long-term loss of critical campus or departmental services
- Unauthorized tampering of research data
- Short-term loss of reputation
- Short-term loss of research funding
- Short-term loss of departmental services
- Unauthorized tampering of research data
- Loss of data with no impact to the university
- Inaccurate general information

### Data Examples

- Health related research & medical records.
- Personnel information & HR records.
- University Financial data
- Credit cards
- Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or
- Lamar University operational information
- Lamar University personnel records
- Lamar University information security procedures
- Lamar University internal communications
- Lamar University Project data
- Lamar University HR data that is not sensitive
- Institutionally published public data
- Academic course descriptions
- Directory information

---

10.02.03 DATA CLASSIFICATION POLICY
1. **Social Security Numbers**: *Confidential data*
   a. Prohibited from disclosure, should not be collected except when required by law.
   b. Confidentiality is required.
   c. Need for Integrity is high.
   d. Need for Availability is limited (should not be available for most purposes)

2. **Blogs**: *Public data*
   a. Blogs are open documents, to be shared with the public. Their contents may be subject to change without serious implications for the hosting individual or department. They are not necessary to the ongoing mission of the University and can, therefore, be removed or taken offline temporarily without serious consequence.
   b. Confidentiality is low
   c. Need for Integrity is low
   d. Need for Availability is low

3. **Digital Research Data**: *Confidential data*
   a. Generally speaking research data requires the highest level of security, because of the need for integrity and originality. There may be cases in which the research is not intended for publication or of a special nature that permits a classification of LU sensitive.
   b. The University still recommends that all research be protected as though it belongs to Confidential category.
   c. Confidentiality is high
   d. Need for Integrity is high
   e. Need for Availability is medium

**5.0 ENFORCEMENT**

Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Lamar University Information Resources access privileges, and to civil and criminal prosecution.
### 6.0 RELATED DOCUMENTS

**Appendix A: Personally Identifiable Information For Human Resources**

<table>
<thead>
<tr>
<th>Confidential</th>
<th>Lamar Sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number</td>
<td>Birth Place</td>
</tr>
<tr>
<td>Drivers License Number</td>
<td>Race</td>
</tr>
<tr>
<td>Credit Card Number</td>
<td>Ethnic Origin</td>
</tr>
<tr>
<td>Bank Account Number &amp; Routing Number</td>
<td>Performance appraisals</td>
</tr>
<tr>
<td>Birth Date</td>
<td>Union Membership</td>
</tr>
<tr>
<td>Age</td>
<td>Gender</td>
</tr>
<tr>
<td>Personnel Records</td>
<td>Citizenship</td>
</tr>
<tr>
<td>Tax Information</td>
<td>Veterans Information</td>
</tr>
<tr>
<td>Health Records</td>
<td>Emergency Contact</td>
</tr>
<tr>
<td>Credit Reports</td>
<td>Salary</td>
</tr>
<tr>
<td>Transcripts</td>
<td>Dates of Employment</td>
</tr>
<tr>
<td>Criminal Background Records</td>
<td></td>
</tr>
<tr>
<td>Permanent Address (Home)</td>
<td></td>
</tr>
<tr>
<td>Permanent Telephone Number</td>
<td></td>
</tr>
<tr>
<td>Cell Phone Number</td>
<td></td>
</tr>
<tr>
<td>Special Disabled Veteran</td>
<td></td>
</tr>
<tr>
<td>FMLA Information</td>
<td></td>
</tr>
<tr>
<td>Disability Information</td>
<td></td>
</tr>
<tr>
<td>International Information (Visa, Passport)</td>
<td></td>
</tr>
<tr>
<td>Payroll Records-Deductions</td>
<td></td>
</tr>
<tr>
<td>Retirement</td>
<td></td>
</tr>
<tr>
<td>Insurance</td>
<td></td>
</tr>
<tr>
<td>Garnishments</td>
<td></td>
</tr>
<tr>
<td>Tax-levies</td>
<td></td>
</tr>
<tr>
<td>Child-support</td>
<td></td>
</tr>
<tr>
<td>Charitable Contributions</td>
<td></td>
</tr>
</tbody>
</table>

### 7.0 REFERENCES

**National/Federal**

- Copyright Act of 1976
- Foreign Corrupt Practices Act of 1977
- Computer Fraud and Abuse Act of 1986

---

**10.02.03 DATA CLASSIFICATION POLICY**
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Gramm-Leach-Bliley Act of 1999
Sarbanes-Oxley Act of 2002
Family Education Rights and Privacy Act of 1974
Uniform Trade Secrets Act
Payment Card Industry Data Security Standard

Texas
Texas Administrative Code, Title 1, Part 10, Chapter 202 – Information Security Standards
Texas Business and Commerce Code, Chapter 48 – Consumer Protection Against Computer Spyware Act
Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information
Texas Government Code, Chapter 441 – Libraries and Archives
Texas Government Code, Chapter 552 – Public Information Act Texas
Texas Government Code, Chapter 2054 – Information Resources Management Act

8.0 REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every two years

Last Review Date: February 11, 2010

Next Review Date: February 11, 2012

9.0 APPROVAL

J. Simmons
President, Lamar University
February 11, 2010
Date of Approval

Priscilla Parsons
Chief Information Officer, Lamar University
February 11, 2010
Date of Approval

10.0 REVISION HISTORY

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Approved Date</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12/10/2009</td>
<td>Initial Version</td>
</tr>
<tr>
<td>2</td>
<td>06/30/2017</td>
<td>Amended Section 7.0 by removing the hyperlink to “Payment Card Industry Data Security Standard. Also removed “DIR Practices for Protecting Information Resources Assets”, and “DIR Standards Review and Recommendations Publications”.</td>
</tr>
</tbody>
</table>