DATA CLASSIFICATION

POLICY

All Sherman College employees and other covered individuals are responsible for:

A. Understanding what constitutes Private or Public Sherman College information; and

B. Managing Private or Public Sherman College information in a manner consistent with the criticality of and the requirements for confidentiality associated with the data in any form (electronic, documentary, audio, video, etc.) throughout the entire information lifecycle (from creation through preservation or disposal).

All Sherman College information whether **at rest** (i.e., stored in databases, tables, email systems, file cabinets, desk drawers, etc.) or **in use** (i.e., being processed by application systems, electronically transmitted, used in spreadsheets, or manually manipulated, etc.) **must be classified into one of the three data classification levels described in this policy.**

Determining classification level should be done according to an assessment of the need for **Confidentiality** of the information.

Confidentiality: *Access to information must be strictly limited to protect the college and individuals from loss.*

Limiting access to authorized individuals/entities/devices ensures legal obligations are fulfilled and/or protects Sherman College and its stakeholders from the disclosure of data which is sensitive in nature.

Note: The appropriate classification of each data set is based on the classification of the most confidential data stored in the data set (e.g., the database, table, file, etc.), or accessed by systems or people. This is true even if the data set contains other information that would qualify for a lower level of protection if it were stored separately.

The table below summarizes the Data Classification process.

Level I – Confidential Protection	**STOP! SPECIAL CARE IS REQUIRED**
Level II – Sensitive Protection	**BE VERY CAUTIOUS**
Level III – Public Protection	**PROCEED WITH AWARENESS**

DATA CLASSIFICATION

Level I – Confidential Information: High risk of significant financial loss, legal liability, public distrust, or harm if this data is disclosed. (Examples provided in Appendix 1: Data Classifications Levels I, II, and III, shown below).

Level II – Sensitive Information: Moderate requirement for Confidentiality and/or moderate or limited risk of financial loss, legal liability, public distrust, or harm if this data is disclosed. (Examples provided in Appendix 1: Data Classifications Levels I, II, and III, shown below)

Level III – Public Information: Low requirement for Confidentiality [information is public] and/or low or insignificant risk of financial loss, legal liability, public distrust, or harm if this data is disclosed. (Examples provided in Appendix 1: Data Classifications Levels I, II, and III, shown below)

Exclusions or Special Circumstances
Exceptions to this Policy shall only be allowed if previously approved by the director of information technology and this approval is documented and verified.

Consequences
Use of Sherman College electronic information resources contrary to this policy or applicable federal, state, or local law is prohibited and may subject the user to disciplinary action including, but not limited to, suspension of the user's access to the electronic information resources. Users also should be aware of other possible consequences under College policies and federal, state, or local laws, particularly those related to computer crime and copyright violation.

Recourse/Appeals
If a department or individual feels that actions taken under this policy have been inappropriate, a review of the decision may be requested. The review will be conducted by the provost and executive vice president. If, after the review, there is still a disagreement with the decision, appeals should be directed through the existing procedures established for employees and students.

DATA CLASSIFICATION

APPENDIX 1: Data Classification Levels I, II and III

Level I – Confidential Information examples include:

- Data protected by HIPAA (health information)
- Data protected by FERPA (student information including grades, exams, rosters, official correspondence, financial aid, scholarship records, etc.)
- Data protected by GLB (financial information)
- Data subject to PCI (credit or payment card industry) standards
- Data subject to other Federal or state confidentiality laws
- Donor or prospect information
- Passwords and PINs
- Personally Identifiable Information ("PII")
- Personnel data
- Individually identifiable information created and collected by research projects
- Data subject to protection pursuant to non-disclosure agreements
- Audit working papers
- Data protected by attorney/client privilege
- Email covering topics listed above

Level II – Sensitive Information examples include:

- Audit reports
- Email addresses that are not a public record
- Other grants and contracts (not included above)
- Competitive business information
- System security information such as firewall rules and hardening procedures
- Security incident information

Level III – Public Information examples include:

- College directory information
- Blogs
- Web pages
- Course offerings
- Annual reports, etc.