LMU | Lincoln Memorial University

Data Classification Standard	
Version: 3	**Effective Date: 1/1/2017**

Data Classification Standard

Purpose:
The purpose of this standard is to define the data administration and classification responsibilities and requirements used by Lincoln Memorial University.

Definitions:

- **Data Owners** - University directors (typically at the level of Registrar, or Unit Director) who oversee data management functions related to the capture, maintenance, and dissemination of data for a particular operational area. They are responsible for decisions about the usage of University data under their purview.
- **Data Core Group (Core) -** The group is comprised of representatives of Data Owners and technical leads at the University who are responsible for the review and operational effectiveness of data management policies and procedures.
- **Data Users** - Individuals and organizations that access institutional data and Information in order to perform their assigned duties or to fulfill their role in the University community.
- **Institutional Data** - Recorded information that documents a University businessrelated transaction or activity by or with any appointed board member, officer, or employee of the University. Regardless of physical form, characteristic, or source, the recorded information is a University record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of University business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is a University record. University records include but are not limited to: personnel records, student records, academic records, financial records, patient records and administrative records. Record formats/media include but are not limited email, electronic databases, electronic files, paper, audio, video and images.

- **Third Party Email System and Messaging Services** - Any means or system for transmitting messages electronically (as between computers on a network) other than the University's official email or messaging systems.

Standards Statement:
Responsibility for Data Administration

All institutional data is owned by Lincoln Memorial University. As such, all members of the University community have the obligation to appropriately secure and protect the asset in all formats and in all locations. Roles and responsibilities for protecting and classifying the institutional data asset are defined in supporting IT Standards.

Data Classification Levels:

The data classification levels are defined as follows and are listed in order from the most secure to the least secure:

Restricted

- Data classified as *restricted* may be subject to disclosure laws and warrant careful management and protection to ensure its integrity, appropriate access, and availability. This information and must be guarded from disclosure. Unauthorized exposure of this information could contribute to identity theft, financial fraud, and violate state and/or federal laws. Unauthorized disclosure of this data could adversely affect the University or the interests of individuals and organizations associated with the University. Systems containing *restricted* data must be approved by the Chief Information Officer or Chief Data Officer.
- Special circumstances may require exceptional measures, such as encryption, two-factor authentication or added security protections that may be implemented to protect specific data elements.

- If a file which would otherwise be considered *confidential* contains any element of *restricted* data, the entire file is considered to be *restricted* information.
- ***Restricted - Special Circumstances*** - A subset of the University's restricted data classification comprised of highly sensitive data elements which require encryption and/or other protections.

Confidential

- Data classified as *confidential* includes all data that is not explicitly defined as *restricted* data and is not intended to be made publicly available. *Confidential* data is distributed on a need-to-know basis between members of the University staff, IT systems, and specific third parties when authorized. Unauthorized exposure of this information could violate state and federal laws and/or can adversely affect the University as a whole or in part or the interests of individuals associated with the University. *Confidential* data may only be disclosed to a third party with the permission of the Data Owner.
- If a file which would otherwise be considered *public* contains an element of c*onfidential,* the entire file may be considered to be c*onfidential* information.

Public

- Data classified as *public* includes all data that are published and broadly available, including student directory information. The types of data classified as *public* should be as broad as possible. Anyone may access *public* data. Care should be taken to use all University information appropriately and to respect all applicable laws. Information that is subject to copyright must only be distributed with the permission of the copyright holder.

Data Access:

Data Owners will establish standard rules, guidelines, and profiles for data access, and decide about individual requests to access data in compliance with local, state and federal laws and regulations.

Access to University data should be based on the business needs of the organization and should enhance the ability of the University to achieve its mission. Employees should have access to the data needed to perform their responsibilities, without regard to arbitrary barriers. Where necessary, Data Owners may specify some data as *restricted* or *confidential*, regardless of how it is made available. This data may only be used by those whose positions requiring such access and for the purpose authorized. When data is designated as *restricted* or *confidential*, the Data Owner will cite the specific legal, regulatory or other references and/or the descriptions of the users who are typically given access to the data and under what conditions the access is granted.

Data Classification, Transmittal and Storage: ○

Restricted Data

Industry encryption is required when transmitting *restricted* data through a network. Sending email to or from a third party email or messaging service is not appropriate for transmitting *restricted* data. Restricted numbers may be masked instead of encrypted. For storage, industry-standard encryption ***is recommended*** if data is not stored on secured servers in the University's administrative network. Third party processing or storage services are not appropriate for receiving or storing *restricted* data unless approved by the Data Owner and Information Security Officer. ○ **Restricted Data-Special Circumstances**

Industry encryption is required when transmitting "*restricted-special circumstances"* data through a network. Email or messaging services are prohibited for transmitting "r*estricted - special circumstances"* data, unless an encryption method is used that has been approved by the Information Security

Officer. For storage, industry-standard encryption ***is required*** if data is not stored on secured servers in the University's administrative network. Third party processing or storage services ***is prohibited*** for receiving or storing *restricted* data unless approved by the Data Owner and Chief Information Officer or Chief Data Officer.

- **Confidential Data**

  Industry encryption is recommended when transmitting *confidential* data through a network. Internal email services may be used between authorized employees to conduct University business. Sending email to or from a third party email or messaging service **is discouraged** for transmitting *confidential* data. For storage, industry-standard encryption ***is not required*** for storage. Third party processing or storage services are appropriate for receiving or storing *confidential* data with Data Owner approval.

- **Public Data**

  No encryption is required for *public* data. Care should still be taken to protect the integrity and availability of *public* information.

Inquiries:

Direct inquiries regarding this policy to:

Office Locations & Address

Lincoln Memorial University
Information Services, Duke Hall
6965 Cumberland Gap Parkway
Harrogate, TN 37752

Mailing Address:

Lincoln Memorial University

Information Services, Duke Hall
6965 Cumberland Gap Parkway Harrogate,
TN 37752

Last Reviewed: April 21, 2025