COLORADO MESA UNIVERSITY	**Data Protection Policy**	
	Issued: October 20, 2023 **Revised:**	**Page: 1 of 7**

I. Purpose

Colorado Mesa University ("University") provides its employees access to information systems for academic and administrative objectives of the University. While utilizing University information systems, users may have access to data required to be accurately maintained and properly protected. A data protection policy establishes a data governance structure and security principles and is a key component of an information security program. The purpose of the University's Data Protection Policy is to 1) declare that all individuals that have been granted access to data have responsibility for the confidentiality, integrity, and availability of institutional data; 2) define roles and responsibilities for data stewardship; 3) classify institutional data based on levels of sensitivity; and 4) establish data protection principles for properly protecting institutional data.

The University's Information Security Program is strongest when all employees are aware and engage in information security. Data stewardship is essential for the implementation of an information security program and the protection of institutional data and the information systems that the data resides on. Data stewardship is equally important for maintaining the confidentiality, integrity, and availability of institutional data for the University to rely upon it as a resource. To support data stewardship, it is important that every individual understands the sensitivity of the data to which they may be exposed. This Policy classifies data in to three levels of sensitivity: Public, Sensitive and Confidential. Data sensitivity levels are designed to assist data stewards—trustees, managers, custodians, and users— in determining the necessary safeguards for the proper use and storage of institutional data and authorizing appropriate access to information. Further, by requiring all employees adhere to data protection principles for proper storage and handling of institutional data, the University is more likely to prevent a data breach from occurring that may negatively impact the University through financial loss or damage to its reputation.

The Data Protection Policy supports Colorado Mesa University’s Information Security Program and its requirements under Colorado Revised Statutes (C.R.S.) 24-37.5-404.5.

II. Scope

This policy applies to all Colorado Mesa University employees and information systems.

III. Definitions

“Cloud Service” refers to software applications, licensed or subscribed to by the University, that are run outside of the University’s data center.

“Computing device” refers to a desktop or laptop computer or mobile device (i.e., smartphone or tablet) that may reside on the University’s data network and/or communicate with Information Systems, to include personally owned devices used for University business but does not include removable media.

"Confidential" means a restriction placed on access to information by federal or state laws, court orders and rules, contracts, licenses, or University policies.

“Digital Authenticator” refers to something you know, such as a passcode; something you have, such as a smartphone; or something you are, like biometrics, that can be used to verify a digital identity.

"Employees" refers to all full and part-time, temporary, and regular University employees including faculty members, administrators, classified personnel, and student workers.

“FERPA” refers to Family Educational Rights and Privacy Act.

“GLBA” refers to the Gramm-Leach-Bliley Act which requires, in part, higher education institutions that administer student financial aid comply with federally required safeguards rule for financial institutions.

“HIPAA” refers to the Health Insurance Portability and Accountability Act which provides protection for individually identifiable health data.

“Information System” refers to a business application or system that provides discrete sets of computing, file storage, and electronic communication resources, organized for the collection, transmission, processing, storage, or sharing of institutional data. An Information System can run in the University’s data center or be a cloud-delivered platform.

“Institutional Data” refers to data owned by or placed in the trust of the University by its students, customers, and employees.

“PII” refers to personally identifiable information, such as social security number, government identification number, or driver's license number, that permits the identification of an individual to whom the information applies by either direct or indirect means.

“Removable Media” refers to digital media that may be removed from a computer system while its running such as portable hard drives and USB drives.

“Safeguard” refers to an information security measure, technical control, procedure, or a course of action implemented with the intention of protecting an information system and the data that resides on it.

“Student Identifier” refers to a number or alphanumeric string that is associated with a student such as the student’s 700 number or username.

IV. Policy

A. Data Stewardship

Data stewardship is essential for data governance, the implementation of an information security program, and the security of institutional data and information systems.

1. Data Trustees

Data Trustees are senior University officers or their designee who have policy level and management responsibility for data within their areas of responsibility. Data Trustee responsibilities include:

- Assigning and overseeing Data Managers;
- Overseeing the adherence to data related policies in their areas;
- Determining legal and regulatory requirements for data in their areas; and
- Promoting appropriate use, quality, and security of data.

2. Data Managers

Data Managers are University officers having direct operational level responsibility for the management of data. Data Managers are assigned by Data Trustees and are generally directors or managers. Data Manager responsibilities include:

- The application of this and related policies to the information systems, data, and other information resources under their control including appropriate categorization of data using the University's data classification methodology;
- Coordinating education regarding the required minimum safeguards for protected data to authorized data users and data custodians;
- Establishing practices and procedures to ensure appropriate use, security of institutional data and maintain data quality;
- Adherence to access control protocols and procedures adopted by the University; and
- Oversee periodic audits in order to ensure compliance with data security requirements and classification standards.

In cases where multiple data managers collect and maintain the same confidential data elements, the data managers must work together to apply a common set of safeguards.

3. Data Custodians

Data Custodians are those responsible for the operation and management of information systems which collect, process, and provide access to institutional data. Data Custodian responsibilities include:

- Compliance with University information security standards and industry best practices;
- Implementation and maintenance of system security and safeguards appropriate to the classification level of the data under their care; and
- Managing Data User access as authorized by appropriate Data Managers.

4. Data Users

Data Users are the individual University employees who have been granted access to institutional data in order to perform assigned duties. This access is granted solely for the conduct of University business. Data User responsibilities include:

- Following the information security protocols and safeguards established by Information Technology and appropriate Data Managers;
- Compliance with federal and state laws, regulations, and University policies; and
- Immediate reporting of any unauthorized access or misuse of data to the appropriate Data Manager or Data Custodian for remediation.

B. Data Classification

A classification will be assigned to institutional data with respect to its level of sensitivity to guide data stewards, project teams, and others who may have access to stored or transmitted data in the security protection methods and access authorization mechanisms appropriate for that data. This classification generates discussion and consequent understanding of the nature of the data being displayed, manipulated, or transferred. Data is to be classified into one of the following three levels of sensitivity:

- ***Public* Data** (low level of sensitivity)
  Access to "Public Data" may be granted to any requester. Public Data is not considered confidential and is generally viewable by the public and does not include student directory information as defined by Colorado Mesa University's FERPA policy statement. Examples of Public Data include staff directories, athletic team rosters, and academic course descriptions. The integrity of Public Data must be protected and should not be modified without the consent of the author. Information generally released under State law, such as the Colorado Open Records Act, is not to be considered Public Data under this plan and shall only be released following University procedures.

- ***Sensitive* Data** (Default) (moderate level of sensitivity)
  Access to "Sensitive Data" must be requested from, and authorized by, the individual who is responsible for the data. Sensitive Data may be accessed by employees as part of their job responsibilities. The integrity of this data is of high importance, and the privacy of this data must be maintained. Examples of Sensitive Data include non-student financial transactions that do not include Confidential Data, information covered by non-disclosure agreements, purchasing data, student ethnicity, student date of birth, and library activity.

- ***Confidential* Data** (highest level of sensitivity)
  Access to "Confidential Data" must be controlled from establishment to destruction, and access will be granted only to those persons associated with the University who require such access to perform their job duties, or to those individuals permitted by law. Examples of Confidential Data include PII, student or parent income, and student financial award information. The confidentiality of data is of primary importance, although the integrity of the data must also be safeguarded. Access to Confidential Data must be requested from and authorized by an

individual with responsibility for the data. Confidential Data includes information protected by regulation or law and the improper disclosure or use could:

- Increase the risk of identity theft by the release of personally identifiable information;
- Negatively affect the University's ability to fulfill its mission due to brand tarnishment or loss of consumer confidence;
- Place the University into a state of non-compliance with contractual obligations; and
- Cause the University to fall into a state of non-compliance with state and federal regulations such as FERPA, HIPAA, and GLBA.

Student Identifiers: The use of a Student Identifier by itself is not confidential data, however, it shall be considered confidential when provided in combination with other PII that permits the identification of an individual to whom the information refers by direct or indirect means. Data sets or files that contain a significant amount of Student Identifiers, whether in combination with PII or not, shall be protected as if the file or data set includes Confidential Information.

C. Data Protection

The following data protection principles are established to ensure the proper storage and handling of institutional data.

1. Identity and Access Management

The University shall maintain identity and access management (IAM) protocols and safeguards that ensure data is only accessed by appropriate individuals and in a controlled manner to protect institutional data and information systems. IAM protocols and safeguards include account management procedures for the identification, authentication, and authorization of users of information systems. Data Managers and Data Custodians must be vigilant when assigning access privileges to data and information systems they manage.

The following data protection principles shall apply:

- Individuals shall be identified and assigned the minimum necessary access to each information system required to perform their job duties assigned.
- Role-based access controls will be used wherever possible to manage user account creation and minimize risk to the University.
- Digital authenticators of sufficient complexity, combination (multifactor), and security will be implemented to protect institutional data and information systems based on risk.

2. Risk Management

The predominance of mobile computing and cloud services requires the University to take a risk-based approach to protecting institutional data. With every data source, software application licensed or subscribed, and individual with access to sensitive and confidential information; the University's risk of unauthorized disclosure of institutional data increases. Assessing information security risks from a business perspective and not purely from a technological viewpoint requires Data Trustee and Data Manager involvement.

The following data protection principles shall apply:

- Identify, assess, and address information security risks at the onset of each technology project that includes a full scope of institutional data involved.
- Institutional data entrusted to information systems or cloud service provider will be kept to the minimum necessary required for the intended use of the application.
- Information systems and cloud services that transmit, process, and store institutional data shall comply with legal, regulatory, and privacy requirements.

3. Data Management

The University shall maintain data management protocols that ensure necessary safeguards are in place to protect institutional data that may be accessed on or through information systems, cloud services, and computing devices. All employees are responsible for the security of institutional data they have access to and have a responsibility to report conditions that place the University at risk.

The following data protection principles shall apply:

- Protocols, safeguards, and audit mechanisms shall be implemented so no single individual can access, modify, or use institutional data without authorization or detection.
- Sensitive and confidential information transmitted or stored shall always be the minimum necessary required for each business process or business need.
- Computing devices and removable media will be properly protected by appropriate safeguards (i.e., encryption) to prevent the unauthorized disclosure of information.
- Confidential information shall not be retained in information systems when it is no longer necessary for business operations or otherwise required by law or regulation.

V. Information Security Program

The University shall maintain an Information Security Program that continually improves user awareness of cyberthreats and how to protect institutional data; properly protects institutional data and the information systems and computing devices that the data resides; and properly prepares the University for adverse impacts on information systems resulting from a security incident. The University's Information Security Program shall be based on an industry recognized information security framework and controls and reviewed on at least an annual basis.

The Information Security Program shall include:

- Information Security and Incident Response Plan
- Information Security Awareness Program
- Business Continuity and Disaster Recovery Plan
- Annual Risk Assessment
- Annual report to the CMU Board of Trustees

VI. Responsibilities

Colorado Mesa University's Data Protection Policy and Information Security Program is managed by Information Technology and is fully supported by University administration and the Board of Trustees. Proper education regarding data classification levels and the necessary safeguards will be provided by Information Technology staff and Data Managers as part of the University's Information Security Awareness Program. Each employee of the University is individually responsible for maintaining a proper understanding of the classification model of the data that they have access to in performing their job duties.

Employees are responsible for reporting inappropriate use or disclosure of institutional data to the appropriate Data Manager, Data Custodian, and Information Technology immediately upon discovery so steps may be taken to address the incident as soon as possible.

VII. Related Policies

This Policy supplements and does not supersede other University policies governing the appropriate or acceptable use of computing and network facilities:

- Electronic Communications Policy
- Computer Use Policy