COLORADO MESA UNIVERSITY	**Data Protection Plan**	
	Issued: March 21, 2017 **Revised: November 5, 2018**	**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. The purpose of the Data Protection Plan is to establish a data governance structure for the University by 1) defining roles and responsibilities for data stewardship; 2) defining classifications for University data based on levels of sensitivity; and 3) outlining guiding principles for properly protecting University data.

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 quality data and its integrity in order for the University to rely upon it as a resource. To support data stewardship, it is important that every individual understand the sensitivity of the data to which they may be exposed. This plan 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 security precautions and controls for the proper use and storage of University-owned data and determining appropriate access to information. Further, by establishing and communicating to employees data protection guidelines 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 Plan supports Colorado Mesa University's information security program and its requirements under Colorado Revised Statutes (C.R.S.) 24-37.5-404.5.

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

II. Definitions (sort definitions)

"Cloud Service" refers to software applications, licensed or subscribed to by the institution, that are run outside of the University's data center.

“Computing device” refers to a desktop or laptop computer that may reside on the University data network and/or communicate with Information Systems. Computing devices do not include mobile devices and 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.

"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, financial institutions to provide information regarding information sharing and security practices.

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

“Identity and Access Management” refers to the processes that ensure data is only accessed by appropriate individuals in the performance of their job duties in a controlled manner.

“Information System” refers to a discrete set of computing, file storage, and electronic communication resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of institutional data.

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

“Mobile device” refers to a portable computing technology that may be carried and used as a hand held device and does not run a full desktop/laptop operating system such as Windows or Mac OS. Smartphones and tablets fit into this category.

“PCI-DSS” refers to Payment Card Industry—Data Security Standard which is a framework for the development of a comprehensive payment card data security process. This includes appropriate prevention and detection of security incidents.

“Remote Access” refers to accessing information systems from a separate device or location off the University’s network.

“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 a measure, procedure or a course of action implemented with the intention of protecting an information system and the data that resides on it.

III. Plan

A. Data Stewardship

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

1. Data Trustees

Data Trustees are senior University officers or their designees 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
- Promoting appropriate use and quality 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 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 of institutional data and maintain data quality.
- Adherence to access control protocols and procedures adopted by the University
- 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 and servers which collect, manage, and provide access to institutional data. Data Custodian responsibilities include:

- Compliance with University information security standards and best practices

- Implementation and maintenance of system security and safeguards appropriate to the classification level of the data under their care
- 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 procedures established by the University and appropriate Data Managers
- Compliance with federal and state laws, regulations, and policies
- 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 in order 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 the 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 persons 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 in order to perform their job duties, or to those individuals permitted by law. Examples of Confidential Data include bank account numbers, social security numbers, 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 information. 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
  - Cause the University to fall into a state of non-compliance with state and federal regulations such as FERPA, HIPAA, and GLBA

  The classification of data as confidential should include references to related legal or externally imposed constraints that require the restriction, the groups of users typically given access to the information, and under what conditions or restrictions access is typically given.

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 control protocols and procedures that ensure necessary technological and administrative safeguards are in place to protect institutional data and information systems. Access control safeguards shall include account management procedures related to the identification, authentication, authorization, and access privileges for users of information systems and University-owned computing devices. Identity and Access Management controls, protocols and procedures shall be identified and implemented as part of the University's Information Security and Incident Response plan and shall be reviewed on at least an annually basis.

The following data protection principles shall apply:

- Employees shall be assigned minimum necessary access to each information system required to perform their job duties assigned.
- The concept of role based access will be used wherever possible in order to manage user account creation.

- Audits of an employee's access to data will occur with changes in employee position/duties or employment status.

2. Risk Assessment

The University shall maintain a process to assess the risks to security and integrity of institutional data at the onset of technology projects and upgrades to verify required information security controls are in place. This includes an approval process for identifying and assessing the risks associated with technology purchases.

The following data protection principles shall apply:

- Ensure that institutional data is properly protected by defining the appropriate scope of involved data.
- Balance the benefits of the project with the inherent risks while focusing on risk identification
- Identified risks will be managed properly and addressed by appropriate University security controls.

3. Mobile Data Management

The University shall maintain mobile data management controls, protocols and procedures that ensure necessary technological safeguards are in place to protect institutional data that may be stored, processed or accessed on or through mobile devices, laptops and removable media based on data protection levels identified. Special consideration shall be given to remote access to information systems and the establishment of usage restrictions and configuration requirements from mobile devices.

The following data protection principles shall apply:

- No confidential information may be stored on mobile devices or removable media.
- Mobile device management standards and safeguards must be in place in order for authorized institutional data to reside on the device.
- University-owned computing devices will be properly protected by reasonable and appropriate safeguards in order to protect sensitive or confidential information.
- University data may only be stored on authorized devices and storage configurations authorized by the Information Technology department

4. Cloud Services Management

The University shall maintain cloud services management controls, protocols and procedures that ensure necessary technological safeguards and contractual agreements are in place to protect institutional data that may reside outside the University's data center. Protecting institutional data stored with cloud services will place increasingly more responsibility on data stewards.

The following data protection principles shall apply:

- A process for evaluating cloud service contracts will be maintained to protect institutional data and mitigate risk to the University.
- Minimize the amount of confidential information exposed and require the service provider commit to industry standard data security safeguards and controls as part of the contract review process.
- Institutional data transmitted or stored with the cloud service provider will be kept to the minimum necessary required for the intended use of the application.

D. Information Security Awareness Program

The University shall maintain an information security awareness program providing guidance on adhering to information security policies and best practices, avoiding cyber threats, protecting personal and institutional data, and the proper use of computing systems. The University's Information Security Awareness program shall be reviewed on at least an annual basis with the Information Security and Incident Response Plan.

IV. Responsibilities

Colorado Mesa University's Data Security Plan is managed by the department of Information Technology and is fully supported by University Administration and the Board of Trustees. Proper education regarding data classification levels and the associated protection measures will be provided by Information Technology staff and other designated individuals. 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.

V. Related Policies

Electronic Communication Policy

Computer Use Policy