Millersville University **Governance & Policies**

Effective: February 21, 2017

Information Technology Policy
ELECTRONIC DATA CLASSIFICATION AND HANDLING

Approved: February 21, 2017
President's Cabinet

Introduction

This policy governs the privacy, security, and integrity of Millersville University data, especially confidential data, and the responsibilities of institutional units and individuals for such data. The procedures provided herein apply to all Millersville University faculty, staff, students, visitors, and contractors.

Purpose

Millersville University maintains data essential to the performance of University business. The objective of this policy is to assist Millersville University employees and contractors in the assessment of data to determine the level of security, which must be implemented to protect that data, without restricting academic freedom or complicating access to data in which the University community has a legitimate or specific need.
Although a large portion of University data is available to the public, some data have restrictions due to privacy protections mandated by federal, state, or local regulations and laws. To comply with these mandates and protect the University community, Millersville University has the right and obligation to protect: the confidentiality, integrity, and availability of data under its purview. The classification level assigned to University data will provide guidance to data custodians and others who may collect, process, or store data.

Policy

All University data should be classified into three levels of security: Confidential, University-Restricted, and Public. Once data has been classified, appropriate safeguards should be implemented to protect data from theft, loss, and/or unauthorized disclosures, access, and/or destruction.

All members of the Millersville University community have a responsibility to protect University data from unauthorized generation, access, modification, disclosure, transmission, or destruction.

1. Data Management

A. All members of the Millersville University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed,

modified, transmitted, stored, or used by Millersville University, irrespective of the medium on which the data reside and regardless of format

B. Millersville University must classify data into the appropriate category according to the risks associated with the data being stored, accessed, or processed. Confidential data require the highest level of protection in order to prevent unauthorized disclosure or use. University-Restricted or public data may be given proportionately less protection. Data stored in collections (i.e., databases, files, tables, etc.) that do not segregate the more sensitive data elements from the less sensitive data, shall be classified according to the classification category assigned to the most sensitive data element.

a. Confidential Data:

i. Confidential data is personally identifiable information, requiring the highest level of protection due to its delicate nature. Confidential data includes data that Millersville University must keep private under federal, state, or local laws and regulations, or based on its proprietary nature.

ii. Confidential Data Includes, but is not limited to:

a) Medical Records
b) Disability Records
c) Student Records
d) Social Security Numbers (Including Partial Numbers)
e) Personnel and/or Payroll Records
f) Date of Birth
g) Driver's License Number
h) Privileged Legal Information
i) Credit Card Information
j) Passwords
k) Personal Financial Information

b. University-Restricted Data:

i. University-Restricted Data is private to Millersville University. Access is limited to University community members who have a legitimate and specific need, where law permits.

ii. University-Restricted Data Includes, but is not limited to:

a). University Partner or Sponsor Information, where no more restrictive confidentiality agreement exists
b) Detailed building plans that contain secure locations
c) Data Network Maps

c. Public Data:

i. Public data has no legal or other restrictions on access or usage and may be open to the University community and the general public
ii. Public Data Includes, but is not Limited to:

a) Millersville University's website
b) Approved official meeting minutes
c) Official policies and documents
d) Publicly-posted press releases
e) Publicly-posted schedules of classes or course catalog
f) Publicly-posted interactive maps, newsletters, newspapers, job announcements, and magazines

2. Data Safeguards

Millersville University entities must implement appropriate managerial, operational, physical, and technical safeguards for access to, use of, transmission of, and disposal of University data. If there is uncertainty regarding the category of the data, the higher level of classification should be applied.

A. General Safeguards for All Data

a) All University data will be classified as either Confidential, University-Restricted, or Public
b) Following initial classification, University data will remain classified at the initial level, or be reclassified as needed due to changes in usage, sensitivities, law or other relevant circumstances
c) Data will be protected in accordance with the security controls specified for the classification level assigned
d) The classification level and associated protection of replicated data will remain consistent with the original data [e.g. (i) confidential HR data copied to a backup storage device, or from one server to another, retains its confidential classification; (ii) printed copies of confidential data are also confidential]
e) Any physical or logical collection of data, stored, in transit, or during electronic transfer (e.g. file, database, emails and attachments, etc.) containing differing classification levels will be classified as a whole at the highest data classification level within the collection. Any data subset that has been separated from any such collection will be protected in accordance with the protection specified for the classification level of the data subset if assigned; otherwise, the data subset retains the classification level of the original collection and requires the same degree of protection
f) Destruction of data (electronic or physical) or systems storing data must be done in accordance with Records Retention and Disposition policies and guidelines

B. Safeguards for Confidential Data

a) Data will be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction
b) Should be labeled as Confidential Data
c) When stored in an electronic format it will be protected with strong passwords and stored on electronic devices that have protection measures

d) May only be disclosed on a strict need-to-know basis consistent with applicable policies and statutes
e) May be stored only in a locked room, or an area where access is controlled using sufficient physical access control measures to detect and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know
f) When sent via fax, may be sent only to a previously established and used address, or one that has been verified as using a secured location
g) May not be posted on any public website
h) Will be destroyed when no longer needed in accordance with Records Retention and Disposition policies, or applicable guidelines or statutes

C. Safeguards for University-Restricted Data

a) Data will be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction
b) Will be stored in a controlled environment when not in use
c) May not be posted on any public website unless prior approval is given by appropriate University legal council
d) Will be destroyed when no longer needed in accordance with Records Retention and Disposition policies, or applicable guidelines or statutes

D. Safeguards for Public Data

a) Protection considerations will be applied to maintain data integrity and prevent unauthorized modification of such data
   i. Storage on an appropriately secured host
   ii. Appropriate integrity protection
   iii. Redundant systems and an appropriate recovery plan to maintain availability as appropriate
b) Should be retained according to public record requirements