Data Classification Policy

NAME:	**Data Classification Policy**
ISSUING DEPARTMENT	**Campus Technologies**
ISSUED DATE:	**November 1, 2016**
REVIEWED DATE:	**November 25, 2019**
APPROVING AUTHORITY:	**Cabinet**
DATE REVISED:	**January 14, 2020**

DEFINITION

This policy governs the privacy, security, and integrity of Mansfield University data, especially confidential data and the responsibilities of institutional units and individuals employed by Mansfield University.

PURPOSE

Mansfield University maintains data essential to routine University business. All members of the University community have a responsibility to protect University data from unauthorized generation, access, modification, disclosure, transmission, or destruction. The objective of this policy is to assist Mansfield University employees and contractors in the assessment of data to determine the level of security, which must be implemented and adhered to, to protect that data. This applies to paper and electronic copy where the data is stored. All data should be classified into three levels of security: Confidential, Sensitive, and Public. Once data has been classified, appropriate safeguards should be implemented to protect data from theft, loss, and/or unauthorized disclosure, use, access, and/or destruction. Appropriate safeguards, including encryption, are found in related guidelines.

Although a large portion of University data is available for the public, some data have restrictions due to privacy protections mandated by federal, state, or local regulations and laws, ethical considerations, and proprietary worth. To comply with these mandates and protect the University community, Mansfield University has the right and obligation to protect the confidentiality, integrity, and availability of data under its purview. Data can also be classified based on the application of the Right to Know Law. The classification level assigned to data will provide guidance to data custodians and others who may collect, process, or store data.

SCOPE

The procedures provided herein apply to all Mansfield University faculty, staff, students, visitors, and contractors.

FORMS

N\A

PROCEDURE

I. DATA MANAGEMENT

    a.   General. All members of the Mansfield University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by Mansfield University, irrespective of the medium on which the data reside and regardless of format (such as in electronic, paper, or other physical form).

    b.   Data Classification. The University must classify data into the appropriate category. Data are assets belonging to the University and should be classified according to the risks associated with the data being stored or processed. Confidential data require the highest level of protection to prevent unauthorized disclosure or use. Data, which are sensitive or public, may be given proportionately less protection. Data are generally stored in collections (i.e., databases, files, tables, etc.) Often these collections do not segregate the more sensitive data elements of a collection from the less sensitive data. Therefore, in determining the classification category, the most sensitive data element in the collection should be used to classify the entire collection.

Examples of Confidential Data include:
1)   Medical Records
2)   Disability Records
3)   Student Records
4)   Social Security Numbers or Partial Social Security Numbers
5)   Personnel and/or Payroll Records
6)   Specific Donor Information
7)   Date of Birth
8)   Driver's License Number
9)   Privileged Legal Information
10)   Credit Card Information
11)   Passwords
12)   Personal Financial Information

Examples of Sensitive Data include:
1)   University Partner or Sponsor Information, where no more restrictive confidentiality agreement exists
2)   Certain Research Records
3)   Library and archive circulation and order transactions.

Examples of Public Data include:
1)   Mansfield University's website
2)   Financial transactions
3)   Approved official meeting minutes
4)   Official policies and documents
5)   Publicly posted press releases
6)   Publicly posted schedules of classes or course catalog
7)   Publicly posted interactive maps, newsletters, newspapers, job announcements, and magazines.

II. DATA SAFEGUARDS

Mansfield University entities must implement appropriate managerial, operational, physical, and technical safeguards for access to, use of, transmission of, and disposal of University data. Confidential Data require the highest level of protection. If there is uncertainty regarding the category of the data, the higher level of safeguards should be applied. This policy provides examples of safeguards.

a. General Safeguards for All Data
1) Using the categories Confidential, Sensitive, or Public, all University data must be classified.
2) Following initial classification, University data should remain classified at the initial level or reclassified as needed due to changes in usage, sensitivities, law or other relevant circumstances.
3) Data should be protected in accordance with the security controls specified for the classification level that it is assigned.
4) The classification level and associated protection of replicated data should remain consistent with the original data [e.g., (i) confidential HR data copied to a CD-ROM, or other removable media (e.g. flash drive), or from one server to another, retains its confidential classification; (ii) printed copies of Confidential Data are also confidential].
5) Any physical or logical collection of data, stored, in transit, or during electronic transfer (e.g. file, database, emails and attachments, filing cabinet, backup media, electronic memory devices, sensitive operation logs or configuration files) containing differing classification levels should 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 should 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.
6) Destruction of data (electronic or physical) or systems storing data should be done in accordance with Records Retention and Asset Management policies and guidelines.
7) Before systems or media are reused they should be wiped according to Department of Defense standards to ensure no residual data.

b. Safeguards for Confidential Data
1) Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
2) Should be labeled Confidential Data.
3) When stored in an electronic format should be protected with strong passwords and stored on electronic devices that have protection and encryption measures.
4) May only be disclosed on a strict need-to-know basis and consistent with applicable policies and statutes.

5) Should be stored only in a locked drawer or 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.
6) When sent via fax, should be sent only to a previously established and used address or one that has been verified as using a secured location.
7) Must not be posted on any public website.
8) Should be destroyed when no longer needed in accordance with System policies, guidelines or statutes.

c.   Safeguards for Credit Card Data
1) All divisions that process or store cardholder data and have access to the information as a result of Internet, mail, fax, or telephone acceptance of credit card account information are required to comply with the American Express, Discover, VISA USA, and Master Card International operating regulations and the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is intended to protect cardholder data in the card-not-present industry. A card-not-present transaction can include Internet, mail, fax or telephone acceptance of credit card account information.
2) Comprehensive information on PC/ requirements and merchant levels may be found on the PCI Security Standards Council Web site at the following link:
https://www.pcisecuritystandards.org/

d.   Safeguards for Sensitive Data

1) Should be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
2) Should be stored in a controlled environment (i.e. File cabinet or office where physical controls are in place to prevent disclosure) when not in use.
3) Should not be posted on any public website unless external affairs and Office of Legal Counsel give prior approval.
4) Should be destroyed when no longer needed in accordance with the Records Retention and Asset Management policies and guidelines.

e.   Safeguards for Public Data available to the public. Protection considerations should be applied to maintain data integrity and prevent unauthorized modification of such data. Safeguards for Public Data may include:
1) Storage on an appropriately secured host.
2) Appropriate integrity protection.
3) Redundant systems to maintain availability as appropriate.
4) Retention according to public record requirements.
5) Appropriate recovery plan.

III. CLOUD STORAGE

Cloud storage services are readily available tools used for accessing, storing, processing or transmitting University related data. These tools, regardless of whether they are personally or University owned, are governed by the procedures provided herein if they are used in conjunction with University Confidential or Sensitive data.

The use of the cloud services must comply with applicable System and University policies. Mansfield University will only allow University data to be stored on cloud services where the approved service contract expressly guarantees the encryption of data in transit and at rest. No University data can reside on any cloud service that does not provide strong encryption nor be able to be transmitted or received without strong encryption.

Requests for non-supported cloud services must be routed to Mansfield University's Information Security Officer. If you use cloud services that are not approved, you are responsible for any and all implications that result and you will not be represented or indemnified by the University. Any decision to use cloud services for the storage of University data in the cloud should take into account the risks and liabilities related to its security, privacy, retention, access and compliance.

RESPONSIBILITY
It is the responsibility of the office of Campus Technologies to update and implement the policy, as needed.

DISTRIBUTION
This policy will be posted to the Policies and Procedures web page.