EDINBORO UNIVERSITY OF PENNSYLVANIA

INFORMATION SECURITY AND DATA CLASSIFICATION POLICY
Policy No. C056

Supersedes Policy No. C056 dated September 12, 2003 and Guidelines on Data Classification dated February 2, 2015

Recommended for Approval by Mr. Guilbert Brown, Vice President Finance and Administration

Approved by Dr. David Werner, Interim President on February 2, 2016

Review Date: As Required

INTRODUCTION

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

PURPOSE

Edinboro University maintains data essential to the performance of 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 Edinboro University employees and contractors in the assessment of data to determine the level of security, which must be implemented 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, Edinboro 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.

POLICY

A. Data Management

1. General. All members of the Edinboro University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by Edinboro University, irrespective of the medium on which the data reside and regardless of format (such as in electronic, paper, or other physical form).
2. 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:

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

   Examples of Sensitive Data include:

   a) University Partner or Sponsor Information, where no more restrictive confidentiality agreement exists
   b) Certain Research Records
   c) Library and archive circulation and order transactions

   Examples of Public Data include:

   a) Edinboro University's website

b) Financial transactions
c) Approved official meeting minutes
d) Official policies and documents
e) Employment data to include name, position, compensation, employment contractor agreement and length of service
f) Publicly posted press releases
g) Publicly posted schedules of classes or course catalog
h) Publicly posted interactive maps, newsletters, newspapers, job announcements, and magazines

B. DATA SAFEGUARDS. Edinboro 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.

1. General Safeguards for All Data
    a) Using the categories Confidential, Sensitive, or Public, all University data must be classified.
    b) 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.
    c) Data should be protected in accordance with the security controls specified for the classification level that it is assigned.
    d) 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].
    e) 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.
    f) Destruction of data (electronic or physical) or systems storing data should be done in accordance with Records Retention and Asset Management policies and guidelines.

g) Before systems or media are reused they should be wiped according to Department of Defense standards to ensure no residual data.

2. Safeguards for Confidential Data
    a) Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
    b) Should be labeled Confidential Data.
    c) When stored in an electronic format should be protected with strong passwords and stored on electronic devices that have protection and encryption measures.
    d) May only be disclosed on a strict need-to-know basis and consistent with applicable policies and statutes.
    e) 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.
    f) 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.
    g) Must not be posted on any public website.
    h) Should be destroyed when no longer needed in accordance with System policies, guidelines or statutes.

3. Safeguards for Credit Card Data
    a) 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.
    b) Comprehensive information on PCI requirements and merchant levels may be found on the PCI Security Standards Council Web site at the following link : https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
    c) All third party vendors that divisions use to fulfill PCI compliance will be retained at the division's expense.

4. Safeguards for Sensitive Data
    a) Should be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.

b) 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.
c) Should not be posted on any public website unless prior approval is given by external affairs and Office of Legal Council.
d) Should be destroyed when no longer needed in accordance with the Records Retention and Asset Management policies and guidelines.

5. Safeguards for Public Data
   Public data are 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:
   a) Storage on an appropriately secured host.
   b) Appropriate integrity protection.
   c) Redundant systems to maintain availability as appropriate.
   d) Retention according to public record requirements.
   e) Appropriate recovery plan.

DEFINITIONS

A. **Confidential Data:** Confidential data are considered the most sensitive and require the highest level of protection. Confidential data include data that the University must keep private under federal, state, or local laws and regulations, or based on its proprietary worth. Confidential data may be disclosed to individuals on a strict need-to-know basis only, where law permits.
B. **Sensitive Data:** Sensitive data are generally private to Edinboro University. Access is limited to University community members on a need-to-know basis and these data are not generally available to external parties.
C. **Public Data:** Public Data have no legal or other restrictions on access or usage and may be open to the University community and the general public.

RELATED POLICIES AND GUIDELINES

Policy No. C065 Cloud Storage Policy
Mobile Device Guidelines

CONTACT INFORMATION:

Vice President Finance and Administration
219 Meadville Street
Edinboro, PA 16444
814-732-2585