Kutztown University Policy GEN-010

Data Classification

A. Purpose

All members of the Kutztown University community have a responsibility to protect Institutional Data from unauthorized access, modification, or disclosure and are expected to understand and comply with this policy. Data Classification is an established framework for classifying Institutional Data based on its level of sensitivity, value, and criticality to the University. The classification of data will aid in determining the baseline security controls for the protection of data.

All data must be classified into three (3) levels of security: Confidential, Sensitive, and Public. Once data has been classified, appropriate safeguards must be implemented to protect data from theft, loss, and/or unauthorized disclosure, use, access, and/ or destruction.

Although a large portion of Kutztown University's data is available to the public, some data have restrictions. Restrictions include, but are not limited 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, Kutztown 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.

B. Scope

This policy applies to all faculty, staff, students, student employees, volunteers, and contractors who have access to Institutional Data. This policy covers data that is stored, accessed, or transmitted in all formats, including electronic, magnetic, optical, paper, or other non-digital formats. Except for those classes of data expressly protected by statute, contract, or industry regulation, the data classification examples presented below are guidelines. The data owner and data stewards are ultimately responsible for the classification of data under their management. Classifications for data sets may be adjusted based on risk assessment or documented business need.

C. Definition(s)

Confidentiality: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.

Integrity: "Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.

Availability: "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to or use of information or an information system.

Data Owner: The person who is ultimately responsible for the data and information being collected and maintained by their department or division, usually a member of senior management.

Data Custodians: Technicians from the Office of Information Technology or, in larger organizations, the Information Security office. Data custodians are responsible for maintaining and backing up the systems, databases and servers that store the organization's data. In addition, this role is responsible for the technical deployment of all the rules set forth by data owners and for ensuring that the rules applied within systems are working.

Data User: A person, organization or entity that interacts with, accesses, uses, or updates data for the purpose of performing a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended and comply with this policy and all policies applicable to data use.

Authorized User: Person that has been authorized by the university to use Kutztown University Information Systems.

Student Record\Education Record: Those records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution, or by a party acting for the agency or institution.

Institutional Data:

Confidential: Considered the most sensitive and requiring the highest level of security. Confidential data includes, but is not limited to, data that Kutztown University must keep private under federal, state, or local laws and regulations, or based on its proprietary worth subject to legal review and Right-to-Know redaction. Confidential data may be disclosed to individuals on a strict need-to-know basis only, where the law permits. The risk of impact of exposure of this type of data would generally be considered high.

Sensitive: Generally private to Kutztown University. Access is limited to Kutztown University community members on a need-to-know basis and these data are not generally available to external parties. The risk of impact of exposure of this type of data would generally be considered moderate.

Public: Have no legal or other restrictions on access or usage and must be open to the university community and the general public and provided if properly requested under the Pennsylvania Right-to-Know Law.

Personally Identifiable Information (PII) definition: Information maintained by the University that can be used to distinguish or trace an individual's identity that specifically includes Social Security Numbers (SSNs), credit card numbers, bank account numbers, Driver's License numbers, state ID numbers, passport numbers, biometric data (including fingerprints, retina/facial images, and DNA profile), or protected health information. These data elements are defined by the University as personally identifiable information. PII is considered confidential information.

Full Disk Encryption: A computer security technique that encrypts data stored on a computer's mass storage and automatically decrypts the information when an authorized user requests it. Full disk encryption is often used to signify that everything on a disk, including the operating system and other executables, is encrypted.

D. Policy

Data Management

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

2. Kutztown University shall classify data into the appropriate category. Data are assets belonging to Kutztown University and must 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 that are Sensitive may be given proportionately less protection.

3. Data are generally stored in collections (e.g., 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 must be used to classify the entire collection.

4. Requests for Confidential Data must be approved by the Data Owner. Transmissions and use of this data must be handed with relevant security controls.

Examples of Confidential Data:

- Medical records
- Disability records
- Student conduct records
- Student records
- Social security numbers or partial social security numbers
- Personnel records
- Specific donor information
- Date of birth
- Driver’s license number
- Privileged legal information
- Credit card information
- Passwords
- Personal financial information

Examples of Sensitive Data:

- University partner or sponsor information
- Certain research records
- Library and archive circulation and order transactions

- Employee ID and Student ID Numbers
- Anonymized data provided for data analysis

Examples of Public Data:

- Kutztown University's public website
- Financial transactions
- Approved official meeting minutes
- Official policies and documents
- Information required to be shared per state law or policy
- Press releases
- Schedule of classes or course catalogs
- Interactive maps, newsletters, newspapers, job announcements, and magazines

Data Safeguards

Kutztown University must implement appropriate managerial, operational, physical, and technical safeguards for access to, use of, transmission of, and disposal of Kutztown University data. Confidential data require the highest level of security. If there is uncertainty regarding the category of the data, the higher level of safeguards must be applied, subject to Right-to-Know redaction. This policy provides examples of safeguards; however, policies may be more restrictive than the ones identified.

1. **General Safeguards for All Data**
   - Using the categories Confidential, Sensitive, or Public, all Kutztown University data must be classified.
   - Following initial classification, Kutztown University data must remain classified at the initial level or reclassified as needed due to changes in usage, sensitivities, law, or other relevant circumstances.
   - Data must be protected in accordance with the security controls specified for the classification level that it is assigned.
   - The classification level and associated protection of replicated data must remain consistent with the original data [e.g., (1) confidential Human Resources data copied to other removable media (e.g., flash drive), or from one server to another, retains its confidential or sensitive classification; (2) printed copies of data are also retain their original classification].
   - 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 must be classified as a whole at the highest data classification level within the collection, subject to legal review for Right-to-Know requirements. Any data subset that has been separated from any such collection must 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.
   - Destruction of data (electronic or physical) or systems storing data must be done in accordance with the Kutztown University Policy on Records Retention and Disposition, and the Policy on Information Technology Asset Management.
   - Before systems or media are reused, they must be wiped according to Department of Defense standards to ensure no residual data remains.
   - Full disk encryption must be implemented on all Kutztown University assets.

- The use of removable media containing confidential or sensitive electronic information, which serves as the primary storage device for the information, is strongly discouraged. If it is used, the removable media must be encrypted using content encryption or full disk encryption and stored in a secure, locked location. This policy does not apply to entities using tape media to store non-public or sensitive electronic information.
- A laptop computer with full disk encryption and removable storage media encrypted with either content encryption or full disk encryption must use passwords in accordance with the Kutztown University Policy on Passwords.

2. Safeguards for Confidential Data

- Must be labeled Confidential data.
- Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
- Confidential Data, including but not limited to credit card, social security, or driver's license information, should not be stored on a PC, Laptop, or Mobile Device such as an iPad, or Smartphone or sent via email without appropriate security protections.
- Confidential Data must use encryption in transit and at rest. When application restrictions prevent it, other compensating controls must be evaluated and implemented.
- When stored in an electronic format, must be protected with strong passwords, and stored on electronic devices that have protection and encryption measures.
- May be disclosed only on a strict need-to-know basis and consistent with applicable policies and statutes.
- Must only be stored 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.
- When sent via fax, it must be sent only to a previously established and used address or one that has been verified as using a secure location.
- Must not be posted on any public website.
- Must be destroyed when no longer needed in accordance with Kutztown University policies or statutes.
- When standard protections for Confidential data cannot be implemented compensating controls must be evaluated and implemented.

3. Safeguards for Credit Card Data

- 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.
- All third-party vendors that divisions use to fulfill PCI compliance will be retained at the division's expense.
- Primary Account Numbers may not be sent via messaging technologies such as email, instant messaging, chat, text messaging, etc.

4. Safeguards for Sensitive Data

- Must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
- Must be stored in a controlled environment (e.g., file cabinet or office where physical controls are in place to prevent disclosure) when not in use.
- Must not be posted on any public website unless prior approval is given by External Affairs and the Office of General Counsel.
- Must be destroyed when no longer needed in accordance with the Kutztown University Policy on Records Retention and Disposition, and the Policy on Information Technology Asset Management.
- Sensitive data may be sent by secure university provided email.

5. **Safeguards for Public Data**
   Public data is available to the public. Protection considerations must be applied to maintain data integrity and prevent unauthorized modification of such data. Safeguards for Public Data may include:
   - Storage on an appropriately secured host
   - Appropriate integrity protection
   - Redundant systems to maintain availability as appropriate
   - Retention according to public record requirements and Kutztown University policies
   - Appropriate recovery plan

6. **Provision for 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 confidential or sensitive university data. The use of cloud services must comply with applicable system and university policies. Kutztown 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 Kutztown University's Chief Information Officer. Users who utilize unapproved cloud services are responsible for all resulting implications and 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 consider the risks and liabilities related to its security, privacy, retention, access, and compliance.

E. Approved By

- Administrative Council – 2/20/25
- President – 3/11/25

F. Effective Date

- 3/11/25