Policy	Data Classification Policy
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	November 28, 2022
Reviewed	June 23, 2025
Approved by	VP for Finance and Administration
Version	25.1

DATA CLASSIFICATION POLICY

PURPOSE

Information assets and IT resources that contain, distribute, and store data are vital to the systems that support Shepherd University's ongoing mission of discovery, learning, and engagement. All information assets and IT resources, especially data, must be protected throughout various phases of their useful life, including when created, collected, stored, transferred, purged, and ultimately destroyed. To support its mission, Shepherd University classifies data into four categories: (1) restricted, (2) confidential, (3) sensitive, and (4) public.

POLICY

Shepherd University information assets and IT resources contain various types of data that is to be used holistically and individually in an approved, ethical, and lawful manner to avoid loss and/or damage to Shepherd University data, operations, image, or financial interest. All affiliated data should be considered confidential and proprietary, thus every effort to protect the integrity of all types of data must be made.

RESTRICTED DATA

Restricted data is highly confidential. Restricted data is protected by laws, statutes, regulations, guidelines, and contractual language, which if exposed could result in legal damages, fines, penalties, identify theft, and/or financial fraud.

Data examples/elements/fields exhibited as restricted include, but are not limited to:

- Personally identifiable information (Pii) of a user
- SSNs, Driver's License numbers, Federal ID numbers, taxpayer ID numbers, Passport numbers
- System account credentials
- Health records
- Financial data – credit/debit card numbers, tax return documents, bank account information

Collecting Restricted Data

- Restricted data may only be collected, maintained, used, or disseminated as necessary to accomplish/adhere to an academic or business purpose of the university or as required by law.

- Departmental units requesting or collecting restricted data must communicate why the data is being collected, how it will be used, and, if applicable, any consequences of not providing it.
- Individuals have the right to inspect and challenge, correct, or explain their personal information as protected by law.

Sending/Receiving Restricted Data

- Restricted data sent or received electronically must be secured using strong data-encryption technology, secure web transfer, or by utilizing the Secure File Transfer Protocol (SFTP). Other acceptable methods include transferring files between Shepherd University network drives on the university network or by leveraging the university's secure cloud/web file system.
- For releasing restricted data to an authorized third party, the sender must ensure that said third party is aware of the confidentiality obligations applicable and listed within this policy. Moreover, the third party is aware that Shepherd University reserves the right for a full security review of internal/external data/security/integrity practices of third party outlining how said data will be secured throughout all phases of transit and rest.
- Restricted data sent in physical form, such as inter-office mail, must be secured in a sealed envelope or by a similar method.
- Faxing restricted data is permissible provided that the recipient is notified in advance and is available to immediately retrieve the fax following transmission or be able to secure it upon receipt of delivery. All individuals receiving faxed documents containing restricted data are responsible for securing the document after receipt.

Storing Restricted Data

- Restricted data should only be stored on Shepherd University administered servers and approved cloud storage systems. If Restricted data must be stored on a computing device, the data must be encrypted in adherence with Shepherd University IT standards. Assisting with determining the best encryption options, users can contact the Information Privacy Officer.
- Restricted data being stored by a vendor/third party must adhere to the same standards/recommendations as if being stored on university information assets and/or IT resources.
- Restricted data saved in non-electronic forms must be protected from unauthorized access by being stored in a locked cabinet within a locked office.

CONFIDENTIAL DATA

Confidential data is information that is protected by laws, statutes, regulations, university policies, or other contractual language, but does not carry the same level of risk as restricted data. Confidential data may be disclosed to individuals on a strictly need-to-know basis only, where law permits.

Data examples/elements/fields exhibited as confidential include, but are not limited to:

- Student educational records protected by FERPA (i.e. grades, GPA, class lists, schedules, etc.)
- Student directory information (i.e. name, address, pronouns, gender, etc.)
- Job Application contact information
- Personal and/or payroll information
- Other data redacted for Right-to-Know requests

Sending/Receiving Confidential Data

- Confidential data may be sent/received via the Shepherd University e-mail system. Other acceptable methods include transferring files between network drives, using university cloud/web file system, or opting to leverage a secure file transfer or encryption service.
- Transmission of FERPA protected data using Shepherd University's e-mail systems must be restricted to recipients with a legitimate educational interest. E-mailing FERPA data to large groups of people is a violation of this restriction, unless it is verified that each recipient has a legitimate educational interest.
- For releasing confidential data to an authorized third party, the sender must ensure that said third party is aware of the confidentiality obligations applicable and listed within this policy. Moreover, the third party is aware that Shepherd University reserves the right for a full security review of internal/external data/security/integrity practices of third party outlining how said data will be secured throughout all phases of transit and rest.
- Confidential data sent in physical form must be secured in a sealed envelope or similar method.
- Faxing confidential data is permissible provided that the recipient is notified in advance and is available to immediately retrieve the fax following transmission or be able to secure it upon receipt of delivery. All individuals receiving faxed documents containing confidential data are responsible for securing the document after receipt.

Storing Confidential Data

- Confidential data should only be stored on Shepherd University administered servers and approved cloud storage systems. If confidential data must be stored on a computing device, the data must be encrypted in adherence with Shepherd University IT standards. Assisting with determining the best encryption options, users can contact the Information Privacy Officer.
- Confidential data being stored by a vendor/third party must adhere to the same standards/recommendations as if being stored on university information assets and/or IT resources.
- Confidential data saved in non-electronic forms must be protected from unauthorized access in a locked cabinet within a locked office.

SENSITIVE DATA

Sensitive data is information that is protected by laws, statutes, regulations, university policies, or other contractual language, but does not carry the same level of risk as restricted or confidential data. Sensitive data should be perceived as data that can be shared internally but generally not to external parties.

Data examples/elements/fields exhibited as sensitive include, but are not limited to:

- Student ID numbers
- Faculty workload
- Event participation/forms (i.e. travel, training, reimbursement, etc.)
- Research work in progress
- Library archive

Sending/Receiving Confidential Data

- Sensitive data may be sent/received via the Shepherd University e-mail system. Other acceptable methods include transferring files between network drives, using university cloud/web file system, or opting to leverage a secure file transfer or encryption service.
- Sensitive data sent in physical form must be secured in a sealed envelope or similar method.
- Faxing Sensitive data is permissible provided that the recipient is notified in advance and is available to immediately retrieve the fax following transmission or be able to secure it upon receipt of delivery. All individuals receiving faxed documents containing sensitive data are responsible for securing the document after receipt.

Storing Sensitive Data

- Sensitive data should only be stored on Shepherd University administered servers and approved cloud storage systems. If confidential data must be stored on a computing device, the data must be encrypted in adherence with Shepherd University IT standards. Assisting with determining the best encryption options, users can contact the Information Privacy Officer.
- Sensitive data saved in non-electronic forms must be protected from unauthorized access in a locked cabinet within a locked office.

PUBLIC DATA

Public data is information that may be available to the general public and is defined with no existing local, national, or international legal restrictions on access or usage.

Data examples/elements/fields exhibited as public include, but are not limited to:

- Publicly posted press releases
- Publicly posted catalogs, class listings, or schedules
- Public announcements, advertisements, directory information, and other freely available data accessible on university websites

PRIVACY, OPERATIONS, and MONITORING

Shepherd University seeks to maintain its IT environment and manage all information assets including data, computing devices, systems technology, telephony, and IT resources in a manner that respects individual privacy and promotes user trust. However, the use of Shepherd University IT resources is not completely private, and users should have no expectation of privacy in connection with the use of any information asset or IT resource.

Shepherd University has the legal right to access, preserve, and review all information stored on or transmitted through any information asset or IT resource, including the inspection of e-mail messages, logging of activities, monitoring usage patterns, and data audits/integrity checks. IT Services may, with or without notice to users, take any other action it deems necessary to preserve, secure, and protect systems, information assets, or IT resources for the betterment of Shepherd University. Without limiting its right to take action, Shepherd University may, at its sole discretion, disclose the results of any general or individual monitoring or access permitted by this policy, including the contents and records of individual communications, to appropriate Shepherd University personnel and/or law enforcement agencies.

SCOPE of AFFECTED PARTIES

This policy applies to all users, such as students, faculty, and staff of Shepherd University and to other persons accessing Shepherd University information assets and/or IT resources including but not limited to authorized agents or community members, regardless of whether such information asset or IT resource is accessed from on-campus or off-campus.

ROLES & RESPONSIBILITIES

All Shepherd University students, faculty, staff, and other parties with access to Shepherd University information assets and IT resources shall be responsible for:

USERS

- Understand and comply with the guidance provided by this policy, as well as applicable compliance programs and affiliated awareness training with all applicable laws, standards, procedures, and university protocols.
- Physically secure and safeguard information assets and IT resources, within the user's possession and control, including abiding with the safe handling of data.
- Promptly report any suspected violation of this policy, any security events, and/or incidents involving a suspected compromise of a user's account or IT resource to itworkorder@shepherd.edu.

CIO/CISO - INFORMATION PRIVACY OFFICER

- Oversee and administer this policy.
- Provide authorization and direction to IT Services staff in accordance with this policy.
- Develop awareness and necessary training materials as it pertains to this policy.

IT SERVICES STAFF

- With appropriate authorization, take directed action in accordance with this policy to preserve, secure, and protect the interests of Shepherd University.
- Ensure all associated procedures are followed and documented accordingly when taking any actions outlined in this policy.

RELATED TOOLS

RELATED POLICIES & GUIDELINES

- BOG#35: Information Technology Security
- Acceptable Use Policy
- Information Security & Privacy Policy
- Data Notification Policy
- Password Guidelines
- Social Security Number Guidelines
- Work from Home / Remote Access Guidelines
- Information Security Program
- Access Control Procedures