Campus Technology Services
Juniata College
814.641.3619
help@juniata.edu
https://www.juniata.edu/offices/campus-technology-services/

Data Protection Policy

PREAMBLE

Juniata College is strongly committed to maintaining the security of sensitive institutional data that it collects and creates. Juniata expects all those who have access to such data to treat this data with the utmost care. The purpose of this policy is to highlight specific requirements that must be met by all who collect, transfer, access, and store sensitive institutional data on electronic devices, electronic media, or cloud storage regardless of whether those are owned by the College or the individual.

DEFINITIONS

Data Classification Definitions

NOTE: The Data Classification Matrix shares examples and additional guidance and is available at http://help.juniata.edu/pdfs/data-classification.php.

- High Risk Data**:** Data should be classified as high risk when the unauthorized disclosure, alteration or destruction of that data could cause a **significant** level of risk to the College or its affiliates. Restricted data include data protected by state or federal privacy regulations that have associated breach notification requirements. The highest level of security controls should be applied to high risk data.
- Moderate Risk Data: Data should be classified as moderate risk when the unauthorized disclosure, alteration or destruction of that data could result in a **moderate** level of risk to the College or its affiliates. This includes data protected by state and federation privacy regulations that does not have an associated breach notification requirement and other personal private information that should be treated as confidential.
- Low Risk Data: Data should be classified as low risk when the unauthorized disclosure, alteration or destruction of that data could result in a **low** level of risk to the College or its affiliates. This includes institutional information that is meant for internal audiences only.
- Public Data: Data should be classified as public when the unauthorized disclosure, alteration or destruction of that data would result in little or **no** risk to the College and its affiliates. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data.

Types of Devices and Storage

- Individual-Use Devices**:** Computer equipment, whether owned by the College or an individual, that has a storage device or persistent memory, such as but not limited to desktop computers, laptops, tablet PCs, and smartphones.
- Individual-Use Media**:** All media, whether owned by the College or an individual, on which electronic data can be stored, including but not limited to external hard drives, magnetic tapes, diskettes, CDs, DVDs, and USB storage devices (e.g., thumb drives).
- Cloud Storage**:** Any electronic storage repository or mobile application, which is not centrally located in the on-premise data centers and file servers at Juniata College.
- On-Premise Servers: All college-owned servers centrally managed by Campus Technology Services and secured in the college's data centers.
- Paper: Non-electronic paper based records and data.

REQUIREMENTS

It is the responsibility of each employee to determine if they will be or have collected, transferred, and/or stored any high or moderate risk data on any device(s), media, or cloud storage and to ensure compliance with this policy. During the onboarding process, all employees agree to the Data Confidentiality Agreement which ensures understanding and agreement to this policy.

Data Protection & Governance

Juniata College will appropriately protect all data that it collects or processes for a lawful basis. This data shall be:

- Processed lawfully, fairly, and in a transparent manner;
- Collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;
- Limited to what is necessary in relation to the purposes for which they are collected and processed;
- Accurate and kept up to date;
- Retained only as long as necessary;
- Securely stored and transmitted.

Collection

Juniata College employees who collect or process data must ensure we have a lawful basis for the collection and processing of this data. Most of Juniata College's collection and processing of confidential and/or restricted data will fall under the following categories:

- Processing is necessary for the purposes of the legitimate interests pursued by Juniata College or by a third party.
- Processing is necessary for the performance of a contract to which the data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which Juniata College is subject.
- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Storage

- All **high risk** data must be stored in a secured location, on designated on-premise servers, or in institutionally approved cloud storage solutions.
- All **moderate risk** data should be stored in a secure location, on on-premise servers, in institutionally approved cloud storage solutions, or on encrypted individual-use devices/media.
    - **Moderate risk** data may be stored in Juniata Email accounts that have 2-Factor Authentication enabled.
    - If there is a legitimate business need to store **moderate risk** data on personally owned individual-use devices/media, it must be stored on encrypted devices/media.
- All cloud storage vendors must be approved by Campus Technology Services. They must guarantee by contract and/or data security policy to encrypt **high and moderate risk** data according to approved methods.
- All electronic **high and moderate risk** data must be stored securely behind a login password/passcode and password-protected screen saver.

Sharing/Transferring

- Transferring management or ownership of any storage device containing **high or moderate risk** data to any 3rd party must be documented by the supervisor and approved by Campus Technology Services.
- Sharing of **high or moderate risk** data must be done in a secure manner using approved solutions. Examples of approved solutions are provided in the Data Classification Matrix.

Retention/Deletion

- Data must only be retained for as long as necessary to support legitimate business purposes and to be in compliance with state and federal regulations.
- **High and moderate risk** data must be deleted using secure methods from the approved individual-use device or media, cloud storage, or other electronic storage solution as soon as there

is no legal, business, or other legitimate reason to store it. Paper records must be shredded.

Lost or Stolen Information

- All lost or stolen college-owned devices/media must be reported immediately to the Help Desk: **(814) 641-3619**. When so notified, CTS will attempt to remotely delete the data to prevent a compromise of **high and moderate risk** data. If the college-owned device is a cellular phone, Campus Technology will also contact the wireless service provider to deactivate the cellular voice capability to minimize responsibility for unauthorized use.
    - For personally owned mobile devices, we suggest that you subscribe to a tracking service such as ***Find My iPhone***. Services like this allow you to remotely find your device and to delete data if necessary. Employees will be held accountable for any approved or unapproved restricted or confidential data that is potentially lost due to a lost or stolen personal device/media.
    - CTS will replace a lost college-owned device, with cost to be borne by the employee or employee's department as directed by the supervisor.
- Any Juniata College department that suspects that a breach or disclosure of **high or moderate risk** data has occurred must **immediately** report this to the Help Desk: **(814) 641-3619**.

Return of College Assets

- All transferred or retired college-owned individual-use devices/media must be returned to Campus Technology for data destruction and redeployment.
    - The supervisor is responsible for returning college owned devices to CTS. In the event of employee reassignment/departure/termination, all Juniata data will be removed from the device/media after the last day of employment.
    - The supervisor is responsible for ensuring Juniata data has been removed from personal devices.
- It is the supervisor's responsibility to inform HR of an employee reassignment/departure/termination, which initiates the process of network account and data access termination.

General Guidelines

- Do not collect and/or store SSNs unless it is required by a federal or state agency and there is no other option in terms of unique identifier. If collection and storage of SSNs are required for operations in a given unit, register this by sending an email to ITSecurity@juniata.edu explaining why the SSNs must be utilized and how and where they are being collected/stored.
- Use the Colleague ID assigned to all individuals as the unique identifier for all Juniata entities. If the Colleague ID is not available or does not exist for certain populations, use a non-SSN type of ID.
- Data should be stored in as few places as possible and duplicated only when necessary. Authorized locations for data storage are included in the Data Protection Matrix.
- Inventory and identify the data under your control that is external to central administrative systems. Know where you have data and in what form (electronic, paper, etc.). Purge or delete data files in a timely manner to minimize risk. The owners of data stored on network accessible systems are responsible for managing and determining the appropriateness of information stored on these systems. This includes both private storage areas and "shared" folder areas.
- It is your responsibility to secure your workstation and/or ensure that only authorized individuals have access.
- Know and understand your environment technically. Understand who has access to areas to which you send, receive, store, or transmit data.
- Transmission of any sensitive data should be encrypted. Websites should use HTTPS encryption if they collect data. Unencrypted protocols should be abandoned in favor of their encrypted counterparts (i.e. abandon Telnet in favor of SSH, or abandon FTP in favor of SFTP).
- Do not release College data of any kind to 3rd party, non-Juniata entities for any reason, unless such entities have been vetted by CTS and agreed in writing to restrict the use of such data to the specific and intended purposes authorized. Any Juniata department or unit releasing data to a non-Juniata 3rd party entity is responsible for how the data are used (misused).

- Report any breaches, compromises, or unauthorized/unexplained access of sensitive data immediately to the CTS Help Desk at (814) 641-3619.
- Confidential information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents must be shredded.

Institutional Data Security Measures

- Campus Technology Services implements appropriate technical and organizational security measures designed to protect institutional information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access, and other unlawful or unauthorized forms of processing, in accordance with applicable law. This includes password-controlled servers in a secured physical location with limited access, hard drive encryption on college-owned laptops, SSL to encrypt information before it's sent over any network, layered security through anti-malware software, firewalls, multi-factor email authentication, intrusion prevention systems, campus wide paper shredding, and training for all employees who have access to sensitive data maintained by Juniata College.
- The College will not process information in any way that is inconsistent with the purpose for which such information was initially collected.
- The College reviews all new 3rd party agreements and contracts to ensure they have the appropriate technical and organizational security measures in place to protect any information we transfer or store with those 3rd parties. We cannot guarantee there will not be a breach, however, we do ensure that we and our 3rd party vendor have breach notification procedures in place.
- Because the Internet is an open system, the transmission of information via the Internet is not completely secure. Although we implement reasonable measures to protect information, we cannot guarantee the security of all data transmitted to us using the Internet.

For more information, please read our Privacy Policy. If you have any other questions or concerns, email us at privacy@juniata.edu.

Revisions:
01/27/20: Revised to add general guidelines.
02/03/20: Revised to add paper documents.