


IT-0001 Classification of Data

	Policy identification number: IT-0001	
	File: Information Technology Policies	
	Classification of Data	
	Policy Summary This policy classifies the types of information used at Fort Lewis College.	
Policy Owner	Approval Date	Effective Date
Vice President, Finance & Administration	January 30, 2019	January 30, 2019
Search Terms	Scheduled for Review	
classification, data, c	Spring 2024	

I. General

This policy applies to:

- Information produced, stored, and collected by Fort Lewis College.
- Information stored and collected by third parties on the behalf of Fort Lewis College.
- Data transmitted, communicated, recorded or handled by any means. This includes but is not limited to electronic, digital, fax, paper, email, posted mail, voice, telephone, answering machines, voice mail, or other photographic, video, and audio mechanisms and technologies.
- Data associated with current, former, and prospective students, faculty, staff, alumni, executives, vendors, and third parties.

Data is classified into one of the following three categories:

- **Confidential Data:**
Data under this classification may be protected by State, Federal, International statutes and laws. Unauthorized or improper disclosure of confidential data can harm the reputation, well-being and safety of the Fort Lewis College community

- **Internal Use Only Data:**
Internal Use Only Data is information that is intended for limited distribution to some or all members of the Fort Lewis College community
- **Unrestricted Data:**
This type of data is intended for public distribution. It will not contain “Confidential Data” or “Internal Use Only Data”

II. Confidential Data

Confidential data is associated with one or more of the following nine main categories:

- Government Agency Issued ID Numbers
- Credit Card Data
- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Personally Identifiable Demographic Data
- Confidential College Business
- Human Subjects Research: Sensitive Personally Identifiable Data
- FERPA – Educational Records

1. Government Agency Issued ID Numbers

Government Agency Issued ID numbers can be used to directly identify an individual. These include:

1. Social Security Number
2. Driver license Number
3. State identification Number
4. Tribal identification Number
5. Passport Number
6. Alien Registration Number
7. Foreign Government Agency Issued ID numbers
8. Military ID Number

2. Credit Card Data

1. Credit card data is comprised of two components, “cardholder data” and “sensitive authentication data”.
2. Cardholder Data consists of:
 1. Primary Account Number (PAN)
 2. Cardholder Name
 3. Expiration date Sensitive
3. Authentication Data consists of:
 1. Magnetic Stripe Data
 2. CVC2 / CVV2 / CID / CVD
 3. EMV or Chip or IC
 4. PIN

3. Personally Identifiable Information (PII)

Information that can be used on its own or in context with other information to identify

an individual. PII is defined as an individual's first name or first initial and last name in combination with one or more of the following data types:

1. Social Security number
 2. Government issued Driver's license or identification card number
 3. Bank/financial account number or credit/debit card number
 4. Date and Place of Birth
 5. Mother's Maiden Name
 6. Security or access codes
 7. Passwords or passcodes
 8. Personal Identification Number (PIN)
 9. Security Question/Answer pairs
 10. Law enforcement information
 11. Military Records
 12. Spouse, child or emergency contact information
 13. Biometric data
 14. Address and Names of student's family member
 15. Student identification number
4. **Personal Health Information (PHI)**
1. Personal Health Information is broadly defined as information about the health status, health care or payment for health care that can be linked to a specific individual. This includes demographic and specific data that relates to:
 1. the individual's past, present or future physical or mental health or condition
 2. information related to the provisioning of health care to the individual
 3. the past, present, or future payment for the provision of health care to the individual
 2. More specifically, the following information are classified under the context of PHI:
 1. Name
 2. Address (including street address, city, county, or ZIP code)
 3. All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
 4. Telephone numbers
 5. FAX number
 6. Email address
 7. Social Security number
 8. Medical record number
 9. Health plan beneficiary number
 10. Account number
 11. Certificate/license number
 12. Vehicle identifiers and serial numbers, including license plate numbers
 13. Device identifiers or serial numbers
 14. Web URLs
 15. IP address
 16. Biometric identifiers, including finger or voice prints

17. Full-face photographic images and any comparable images
 18. Any other unique identifying number, characteristic, or code
5. **Personally Identifiable Demographic Data:**
 Personally Identifiable Demographic data is information concerning an individual's: racial or ethnic origin, political opinions or affiliations, religious or philosophical beliefs, trade-union membership, sexual orientation, and citizenship or immigration status.
 6. **Confidential College Business**
 Confidential College Business data consists of information protected by contract, binding agreement or industry requirements. It may include any information regarding College Business that is intended for a very limited distribution or need-to-know basis. This may include information concerning legal sanctions, criminal investigations, fines and penalties; violations of personal privacy; financial and/or reputational loss; potential lawsuits; and access to critical data sources or funding. Other types of information that might be considered as Confidential College Business data include:
 1. Financial Statements and Accounting Information
 2. Unit Budgets
 3. Purchase Orders
 4. Internal Memos and Emails
 5. Planning Documents
 6. Meeting Minutes
 7. Donor contact Information and non-public gift amounts
 8. Non-public policies
 9. Non-public contracts
 10. Administrative or technical information regarding information systems that could jeopardize system security
 11. Sexual harassment complaints and investigations
 12. Grievances filed
 13. Emergency or security information regarding any building the could jeopardize safety and security of the building or persons within.
 14. Criminal investigations and campus police records
 15. Information that would give an advantage to competitors or bidders
 7. **Human Subjects Research: Personally Identifiable Data**
 Human Subjects Research is any research or clinical investigation that involves human subjects. Research and investigation may include; surveys and questionnaires, interviews and focus groups, analyses of existing data or biological specimens, epidemiological studies, evaluations of social or educational programs, cognitive and perceptual experiments and medical chart review studies. Personally Identifiable data in this context is information that contains one or more elements that can be combined with other reasonably available information to identify an individual.
 8. **FERPA – Educational Records:**
 The definition of an educational record, and the requirements concerning the access and handling of educational records are defined in the FERPA statement found in the Policy Library.

III. Internal Use Only Data

“Internal Use Only” Data is information that is intended for limited distribution to some or all members of the Fort Lewis College community. This information may include routine operational information, meeting minutes, internal emails, and other documents.

IV. Unrestricted Data

This type of data is intended for public distribution. It will not contain “Confidential Data” or “Internal Use Only Data” as defined earlier in this policy. Publicly posted information must not adversely impact the College, its students, staff or faculty, the state, or the public. Materials should be checked for accuracy and content to avoid damage to reputation and/or operational effectiveness. Unrestricted Data can include:

1. Approved press releases and publications
2. Information approved for posting on open websites and social media
3. Course Catalogs
4. Email sent to campus wide distribution lists

V. Reason for Policy

To enable the prioritization of appropriate security and handling requirements and ensure compliance with laws and regulations applicable to data privacy and usage.

VI. Responsibilities

For following the policy: All employees and contracted vendors

For enforcement of the policy: Information Security Officer

For oversight of the policy: Vice President for Finance & Administration

For notification of policy: Policy Librarian

VII. Definitions

Biometric data: These are identifiers derived from body characteristics, measurements and calculations that can be used to uniquely identify an individual.

Cardholder Name: This is the name of the owner of the card

CVC2 / CVV2 / CID / CVD: The 3 or 4 digit codes found on the back of the credit card.

EMV or Chip or IC: Authentication data is stored in the integrated circuit (IC) chip that is embedded in the credit card that can be used with a PIN to increase the security of a transaction.

Expiration date: The expiration date printed on the credit card data

Foreign Government Agency Issued ID Number: These include national or social identification numbers, national or social insurance numbers, or other personal identifiers that are issued by foreign government agencies.

Financial transaction device: Any instrument or device such as a credit card, banking card, debit card, electronic funds transfer or stored value card, or account number representing a financial account.

Magnetic stripe: Stores PAN, EXP date, credit limit and other highly confidential data on the credit card.

Password or passcode: A string of alpha-numeric characters that is used to prove identity or gain access to a resource

Personal Identification Number (PIN): a numeric number used in the process of authenticating or identifying an individual or entity to a system or account.

Primary Account Number (PAN): The 15 or 16-digit number found on the front of a credit card.

Security Question/Answer pairs: These are questions that are used to verify account ownership.

Social Security Number: A nine-digit number issued to U.S. citizens, permanent residents and temporary residents under section 205(c)(2) of the Social Security Act.

VIII. Cross-Referenced Policies

[1-20: Accounts Receivable: Disclosure of Student Records](#)

[6-10: Acceptable Use of Information Technology](#)

[Family Educational Rights and Privacy Act \(FERPA\)](#)

[6-1: Privacy Statement](#)

IX. Revision History

New policy - January 2019