IT-0002 Storage and Handling of Data

Policy identification number: IT-0002

File: Information Technology Policies

Storage and Handling of Data

Policy Summary

This policy establishes the requirements and responsibilities regarding the storage and handling of classified data.

Policy Owner **Vice President, Finance & Administration**	Approval Date **January 30, 2019**	Effective Date **January 30, 2019**
Search Terms **storage, handling, data, s, vpfa**	Scheduled for Review **Spring 2024**	

I. General

Faculty, staff and employees of Fort Lewis College have the responsibility to protect information resources for which they are in care of. Each person and office is expected to:

- Review the “Classification of Data” policy and recognize the types of data that comprise the data classifications of: “Confidential Data”, “Internal Use Only Data”, and “Unrestricted Data”
- Protect Confidential and Internal Use Only data from unauthorized disclosure
- Handle, distribute, collect, and store data with discretion and the appropriate safeguards as outlined in this policy.
- Immediately report any accidental disclosure, unauthorized access, or unintended distribution of Confidential or Internal Use Only to the FLC IT Department.
- Review the guidelines in the “Disposal of Personally Identifiable Information” Policy, and delete files and emails that contain Confidential or Internal Use only data when no longer needed.
- Notify the Information Technology (IT) Department of business process requirements or technical barriers that may preclude a department’s ability to implement the data handling practices outlined in this policy.

II. Data Storage and Handling Requirements

1. The following types of information should not be sent or received via unencrypted email, or stored on unencrypted computers or mobile devices:
    A. Government Agency Issued ID Numbers
    B. Personally Identifiable Information
    C. Personal Health Information
2. Credit Card Data should not to be sent or received via email or stored in any digital format
3. Confidential or Internal Use Only should not be distributed or redistributed to those who are not authorized to view them.
4. Emails and other types of electronic documents containing Confidential data should not be stored on laptops, flash drives, or mobile devices unless properly encrypted.
5. Networked file shares, web sites, databases, or other networked applications, must be have appropriate file level or system access permissions applied to prevent unauthorized access or modification of Confidential or Internal Use data.
6. Paper files or documents that contain data classified as Confidential or Internal Use Only must be kept in a secure area when not in use and be protected from unauthorized viewing when in public areas.

III. Storage and Handling Best Practices

1. Regularly review processes or forms that collect Confidential data to ensure there is a legitimate business need. On forms, reports, and spreadsheets use redacted forms of identifiers where possible (i.e. last 4 digits of SSN or Student ID number).
2. Avoid using email to transfer, collect and distribute reports, documents, spreadsheets and files. The preferred method of collaboration involving is via FLC IT supported file shares or FLC IT supported collaborative web sites.
3. Safeguard information that is in your control. When possible, do not store digital copies of data that can be retrieved on-demand from a database or other mechanisms.

IV. Reason for Policy

Fort Lewis College is committed to protecting the reputation, safety, and privacy of the individuals that make up our community. Establishing best practices around the handling of data helps prevent the unauthorized disclosure of sensitive information and ensure compliance with data privacy laws and regulations.

V. 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

VI. Definitions

Electronic Documents: Electronic documents are created and stored on a computer system or application. Common types electronic documents include emails, database tables and reports, web pages, spreadsheets, text files, presentations, and digital images.

Mobile Devices: A portable computing device, such as laptops, tablets, smart phone.

Encryption: A technology that protects electronic documents and system drives by converting the data to a format that is unreadable to those with unauthorized access. Password protection of electronic documents is not an adequate substitute for encryption.

VII. Cross-Referenced Policies

Classification of Data Policy
Disposal of Personally Identifiable Information Policy

VIII. Consequences of Non-Compliance

Confidential data is protected by State, Federal, and International laws and regulations. Failure to properly manage data can result in disciplinary actions, penalties and other consequences for the individual and department. Violations shall be handled consistent with College disciplinary procedures. The College may refer suspected violations of applicable law to appropriate law enforcement agencies.

The College may suspend, block or restrict access to information and network resources if necessary to protect the integrity, availability, and/or confidentiality of College information or to protect the College from liability.

IX. Revision History

New policy January 2019