Device Encryption Policy

Department: Campus Technology	**Date Created:** 2/11/2025
Owner: IT Department	**Date Last Revised:** 3/18/2025

Printed copies of this document are for reference only.

1. Policy Statement

It is the policy of Lewis and Clark Community College to enforce encryption on all employee-assigned laptops, desktops, and certain servers to protect sensitive information and maintain the confidentiality of data. Encryption is a critical security measure that helps safeguard against unauthorized access, data breaches, and theft of sensitive information. This policy outlines the requirements for encryption on systems and the procedures for implementing and enforcing encryption.

1.1 Scope

This policy applies to all information systems of Lewis and Clark Community College that contain personally identifiable information (PII), or any employee computers owned by the college. This policy covers all laptops, employee desktops, and certain servers.

1.2 Exceptions

Exceptions include systems owned by the college that have not yet been issued or imaged, any servers not containing PII, any system not on the college's domain, or a system in-service that requires encryption to be disable for troubleshooting purposes. Systems may also be exempt from the policy if a risk acceptance document is approved, indicating a business operation that cannot function with encryption.

1.3 Encryption Requirements

All systems that contain or process personally identifiable information must have hard drive encryption enabled. The encryption must meet the Advanced Encryption Standard (AES). This includes any applicable servers and all employee systems, such as desktops and/or laptops.

1.4 Encryption Implementation

The Lewis and Clark Community College IT Department shall be responsible for implementing and managing encryption on all employee laptops, desktops, and all servers

to protect any Personal Identifiable Information (PII) that could be on them. The following procedures shall be followed:

a. **1.4.1 Encryption Setup**: All systems deployed by the college must be encrypted before they are issued to employees. All servers processing or containing PII will be encrypted prior to use. The IT department shall use an approved encryption solution to configure and enable encryption on systems.

b. **1.4.2 Encryption Enforcement**: The IT department shall regularly monitor and enforce compliance with the encryption policy. This includes conducting regular audits to ensure that all required systems are encrypted as per the policy requirements. Non-compliant laptops and servers shall be identified, documented to the risk register, and brought into compliance within an appropriate time.

c. **1.4.3 Encryption Key Management**: The IT department shall implement proper encryption key management practices, including securely storing encryption keys and providing authorized access only to authorized personnel. Lost or compromised encryption keys must be reported immediately to the IT department.

1.5 Employee Responsibilities

All employees of Lewis and Clark Community College are responsible for complying with this policy. This includes the following:

a. **1.5.1 Encryption Activation:** Employees must not disable or circumvent encryption on college computers, unless for troubleshooting purposes by IT. If an employee suspects encryption is not enabled on their system, they must report it immediately to the IT department.

b. **1.5.2 Encryption Usage:** Employees must use encryption in accordance with the policy requirements. This includes storing sensitive information only on encrypted systems and devices as per the policy.

c. **1.5.3 Encryption Key Protection:** IT employees are to protect each individual encryption key with the same care as a privileged password. IT cannot give out encryption keys to non-IT personnel. Encryption keys are not allowed to be recorded or transmitted, this includes but is not limited to SMS messages, phone calls, emails, written notes, and any file transfer system.

1.6 Enforcement

Any violation of this policy will be reported directly to the infringers' supervisor, and any applicable stakeholders.

1.7 Policy Review

This policy shall be reviewed and updated periodically by the IT department to ensure its effectiveness and compliance with relevant laws, regulations, and industry standards.

Date	Change Description	Author - Position	Approved By - Position
2-11-2025	Policy creation	McLaughlin – Information Security Analyst	-
2-21-2025	Policy revision based on 2-13-2025 meeting. Created policy template.	McLaughlin – Information Security Analyst	-
3-18-2025	Watermark removed. Revised the policy statement to include desktops. Ready for Approval	McLaughlin – Information Security Analyst	Ron Wall

-----END OF DOCUMENT-----