Information Security Access Controls Policy

Department: Campus Technology	**Date Created:** 4/2/2025
Owner: IT Department	**Date Last Revised:** 6/30/2025

Printed copies of this document are for reference only.

1. Policy Statement

The purpose of the Access Controls Policy is to establish the standard for controlling access to college data and computer systems.

1.1 Scope

This policy is to be enforced and maintained by the Lewis & Clark Community College Information Technology department. The policy is applied to all Lewis & Clark Community College personnel, non-employees, students, or other individuals with a user account to campus systems to protect sensitive data.

1.2 Exceptions

Exceptions to this policy require explicit written permission from the Chief Data and Technology Officer and may be subject to approval by the applicable IT department leadership.

1.3 Access Controls Requirements

This section outlines the policy's requirements for user identifiers, authentication, privilege authorization, user logging and audit information, and how access control information will be provided to college personnel and the community.

1.3.1 User Identification

Each user who accesses campus technology will be assigned a unique identifier, which will be provided in the form of their username. This username (or an alias of it) will be used to identify an individual in all campus technology systems.

1.3.1.a – Other Users: On a case-by-case basis, guest, generic, and temporary users can be utilized for defined purposes. These external user accounts are created, modified, removed, and monitored by the IT department for security purposes.

1.3.1.b - Special Cases: Except in documented requests approved by IT, a user's unique identifier is not changed or reused.

1.3.2 User Authentication

For the protection of data, all users are required to authenticate to access any college systems before receiving access. The authentication requirements are based on the level of access the user is requesting. All authentication requests require at a minimum an alpha-numeric password, but other systems will require multi-factor authentication; below outlines each type of authentication level:

1.3.2.a – Password Authentication Requirements: For a password to be set and used to authenticate, it must meet the following requirements:

- All Passwords must contain at least:
  - Eight or more characters.
  - One or more uppercase letters.
  - One or more lowercase letters.
  - One or more numbers.
- Additional password constraints include:
  - Cannot contain the user's name.
  - Cannot be a previous password.
  - Cannot contain certain special/unique characters.

1.3.2.b – Password Lifespan requirements: Once a password is set, the password will be valid for a set length of time until it expires and needs to be reset. The lifespan of passwords is based on the type of user:

- Staff with PHI access: 60 days
- Team Members: 90 days
- Students: 180 days
- Special/ Other: 365 days maximum

1.3.2.c – Password Recovery Requirements: The college must provide a method for users to reset or update their own passwords to ensure the safety and availability of their accounts.

1.3.3 Multi-factor Authentication

To enhance the security of system & infrastructure access, Multi-Factor Authentication (MFA) is utilized by the college.

1.3.3.a – Multi-Factor Authentication Required Systems: MFA is required for the following systems, services, and infrastructure:

- Information systems containing or processing sensitive, confidential, or regulated information**.**
- Remote access to the college network.

- Administrative access to network servers
- College personnel & third-party assigned or shared workstations.
- Additional systems and services determined by IT leadership.

MFA may be added to protect additional systems and services, as determined by IT leadership, to enhance information security.

1.3.3.b – Approved Multi-Factor Authentication Factors: Authentication factors must include two or more of the following:

- Something you know: e.g., password, PIN.
- Something you have: e.g., hardware token, phone, platform authenticator.
- Something you are: e.g., biometric authentication.

1.3.3 User Access Authorization

Lewis and Clark Community College's Information Security program currently utilizes Role-based Access Control (RBAC) with elements of Discretionary Access Control (DAC) to assign user permissions. The following must describe all user access:

- A user must have enough access to complete their role's function.
- A user must not have more access than necessary.
- IT must be notified of any changes required regarding an individual's access.

All access requests are subject to review and periodic audits by IT leadership to prevent unauthorized data access.

1.3.3.a – Access Establishment:

A user's access is established when they are granted access to their account based on their role at the college (e.g., students, employees, third parties). When user access is established, they will receive access roles based on their position.

1.3.3.b – Access Modification:

At any time, a user, supervisor, or Human Resources may submit a written request to grant one or more users additional access, accompanied by a justification for the change. IT leadership will review all requests for access modification.

1.3.3.c – Access Suspension:

An individual's access may be disabled under specific circumstances to ensure the security, integrity, and compliance of the college's systems and policies. The following scenarios provide IT authorization to suspend access temporarily:

- An active security incident or hazard that involves one or more individuals or user accounts.
- Noncompliance with college codes or policies.
- Written consent from college leadership to IT leadership, provided with justification.

1.3.3.d – Access Termination:
Upon termination of an employee, Human Resources must inform the IT department by providing all required termination information to the helpdesk's ticketing system. The IT department must remove all user access to college information after the employee's final day of work.

In the event of an involuntary termination, access will be revoked on the designated date and time provided.

1.3.4 Access Logs
Access logs must be retained for the security of the college's information. Access logs are stored and accessed for security auditing (e.g., Threat hunting, intrusion detection, incident response), troubleshooting issues, and compliance. Access logs must be restricted to authorized personnel only.

1.4 Communication & Awareness
To ensure compliance and awareness of the policy, the following must occur:

- This policy must be provided to all new college hires as part of their cybersecurity new hire training.
- All college employees during their annual cybersecurity compliance training will be prompted to acknowledge this policy.
- This policy must be accessible for all college stakeholders for awareness and transparency initiatives.

1.5 Enforcement
Any violation of this policy will be reported directly to the infringers' supervisor and any applicable stakeholders in the event. Policy noncompliance will require an action plan and timeline within the IT department to ensure compliance.

1.6 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.

1.7 Revision history
Below is the recorded history of the policy. This must be updated each time the policy undergoes changes.

Date	Change Description	Author - Position	Approved By - Position
4-2-2025	Policy creation & Policy topics outlined	McLaughlin – Information Security Analyst	-
6-2-2025	Outline expanded and policy draft created	McLaughlin – Information Security Analyst	-
6-30-2025	Policy Revisions made from CDTO recommendations. Ready for signature	McLaughlin – Information Security Analyst	Ron Wall

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