LeMoyne-Owen COLLEGE

LEADERSHIP. OPPORTUNITY. CHANGE.

SUBJECT:	**Effective Date:**	**Policy Number:**
Access Control Policy	September 2024	05-1-014
	Supersedes:	**Page 1 Of 4**
	Policy:	
	Date:	
	Responsible Authority: VP of IT & CIO	

I. Purpose and statement of operational policy underlying the procedure.

The purpose of this Access Control Policy is to establish guidelines for managing access to the college's information systems, ensuring that only authorized users have access to specific resources, data, and information technology infrastructure. This policy aims to protect the confidentiality, integrity, and availability of the college's systems and data.

II. Applicability/Scope

This policy applies to all students, faculty, staff, contractors, third-party vendors, and anyone with access to LeMoyne-Owen College's information systems, data, or technology resources. It includes, but is not limited to, the following systems:
College networks (wired and wireless)
Administrative systems
Academic systems
Servers, databases, and storage systems
End-user devices (desktops, laptops, tablets, smartphones)
Cloud services used by the institution

Access Control Principles
Access to LeMoyne-Owen College's systems will be controlled based on the following principles:

Need to Know: Access to information and resources will be granted based on the user's role and responsibilities.

Least Privilege: Users will only be given the minimum, yet most properly needed and effective access necessary to perform their duties.

Role-Based Access Control (RBAC): Access rights will be assigned according to the user's role within the institution or otherwise given after Department Head of area approval or request.

Separation of Duties: Critical duties will be separated to prevent conflicts of interest or unauthorized actions by a single individual.

User Access Management

User Identification and Authentication
All users must have a unique user ID for accessing LeMoyne-Owen systems.

Multi-factor authentication (MFA) will be required for access to sensitive systems, such as financial records and student data.

Passwords must adhere to the college's password policy, which includes complex requirements and regular updates.

Account Creation and Deactivation
Accounts will be created based on approval from department heads or supervisors and will align with the user’s role within the institution.

User access will be promptly disabled upon termination or role changes within the college.

Dormant or inactive accounts will be reviewed and disabled after 90 days of inactivity unless special approval is granted.

Physical Access Control
Facility Security
Physical access to data centers, server rooms, and other critical infrastructure will be restricted to authorized personnel only.

Regular audits of physical access logs will be conducted to ensure only authorized personnel are accessing secure areas.

Device Security
All college-issued devices must be secured with password protection and encryption.

Remote access to systems (e.g., VPN) will require secure authentication, and the college's VPN policy must be followed.

Portable devices, such as laptops and smartphones, must be secured with encryption and locked when not in use.

Network Access Control
Access to the college network (wired and wireless) will be restricted to authorized devices.

Guests and third-party vendors will be provided with limited, temporary access to the network, separate from internal systems.

Network segmentation will be implemented to restrict access to sensitive systems (e.g., student records, financial systems).

Access Reviews and Audits
Regular audits of user access rights will be conducted at least annually to ensure access is aligned with users' roles and responsibilities.

Privileged accounts (e.g., system administrators) will be reviewed more frequently, with access logs monitored for any unusual activity.

Third-party access will be regularly reviewed and revoked when no longer necessary.

Incident Response
Any unauthorized access or security breaches must be reported immediately to the IT department. The college's incident response plan will be followed to investigate and mitigate unauthorized access incidents.

III. Process for Implementing Procedure

Responsibility	Action	Timeline
IT Department	Responsible for implementing and managing access controls, conducting audits, and responding to security incidents.	Ongoing
Department Heads	Approve access requests for their team members and ensure access is appropriate for the individual's role.	Ongoing
Users	Responsible for complying with access control policies, safeguarding credentials, and reporting suspicious activity.	Ongoing
Authorizing Official	This Access Control Policy will be reviewed annually and updated as necessary to reflect changes in technology, risks, and regulatory requirements.	Annually

IV. Related policies/References for more information

- Identification and Authorization Policy
- Incident Response Policy
- IT Risk Assessment Policy

Authorizing Official: _____ Authorization Date: _____

Title: _ _____