THE LeMoyne-Owen COLLEGE

LEADERSHIP. OPPORTUNITY. CHANGE.

LeMoyne-Owen College

AC3 - Access Control

March 16, 2020

AC3 - Access Control

The organization actively manages risks around user account management, access enforcement and monitoring, separation of duties, and remote access.

LeMoyne-Owen College Access Control Policy

1.0 Purpose

This policy establishes the Access Control Policy for managing risks around user account management, access enforcement and monitoring, separation of duties, and remote access through the establishment of an Access Control program. The access control program helps LeMoyne-Owen College implement security best practices with regard to logical security, account management, and remote access.

2.0 Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by LeMoyne-Owen College. Any information not specifically identified as the property of other parties, that is transmitted or stored on LeMoyne-Owen College IT resources (including e-mail, messages and files) is the property of LeMoyne-Owen College. All users (LeMoyne-Owen College employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3.0 Policy

The following subsections outline the Access Control standards that constitute the LeMoyne-Owen College policy. Each LeMoyne-Owen College Business System is then bound to this policy and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

All LeMoyne-Owen College Business Systems must develop, adopt or adhere to a formal, documented access control procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

3.1 Identification

Identification control should adhere to the following requirements:

- All users of information assets must only use the username assigned by the Identity Management System.
- Identity information shall be captured from authoritative institutional repositories of information.
- For users whose identity has not been created automatically:
    - Verification of identity must be conducted before identity information is entered into IAM system.
    - The request must be approved by the authorized individual directly responsible for supervising the requestor’s activities and then routed to IT department.
- Employees shall not have multiple identities.

3.2 Authentication

Authentication control should adhere to the following requirements:

- Use of central authentication based system of records, rather than separate authentication systems maintained by individual groups or departments.

- A role-based system should be implemented to manage authentication and access to systems.
- Authentication should be external to applications so that authentication mechanisms can be updated or changed to reflect changing requirements without significant application development.
- Use of appropriate encryption to protect the privacy of the exchange when electronic credentials are transmitted during authentication.
- Any applications required to use multi-factor authentication

3.3 Authorization

Authorization control should adhere to the following requirements:

- Separation of Duties: All LeMoyne-Owen College Business Systems that allow for privileged activities such as financial transactions or access to critical systems must:
  Separate duties of individuals as necessary, to prevent malicious activity without collusion. Document separation of duties.
  Implement separation of duties through assigned information asset access authorizations.
- Least Privilege: All LeMoyne-Owen College Business Systems must employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

3.4 Account Management

All LeMoyne-Owen College Business Systems must:

- Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated missions/business functions.
- Identify account types (i.e., individual, group, system, application, guest/anonymous, and temporary). Establish conditions for group membership.
- Identify authorized users of the information asset and specifying access privileges.
- Require appropriate approvals for requests to establish accounts. Access requests shall be limited to the systems and applications described on the work order.
- Applications shall only be used for the purpose stated on the request.
- Specifically authorize and monitor the use of guest/anonymous and temporary accounts.
- Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes.
- Deactivate temporary accounts that are no longer required and accounts of terminated or transferred users.
- A new request is required if there are changes in roles or access privilege to the stated application. Access to systems and applications is established or reviewed under the following conditions:A new user requires access for the purpose of fulfilling job responsibilities.
- An existing User has a change in job function requiring a change in role and privileges.
- A User is terminated or no longer needs access to the system or application.

  Annual review

3.5 System Use Notification

All LeMoyne-Owen College Systems should consider:

- Display an approved system use notification message or banner before granting access to the system

that provides privacy and security notices consistent with regulations, standards, and policies.

- Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information asset.

3.6 Access Security Mechanisms

LeMoyne-Owen College uses strong passwords, group policy, Single Sign On (SSO), and secure two-factor authentication wherever possible to determine a user's identity, ensure its correctness, and establish accountability.

- Concurrent Session Control: All LeMoyne-Owen College Business Systems should limit the number of concurrent sessions for each system account to ten for information assets, if possible.
- Session Lock: All LeMoyne-Owen College Business Systems must prevent further access to the information asset by initiating a session lock after 30 minutes of inactivity or upon receiving a request from a user.
- Publicly Accessible Content: All LeMoyne-Owen College Business Systems must:
- Designate individuals authorized to post information onto an organizational information system that is publicly accessible.
- Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
- Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.
- Review the content on the publicly accessible organizational information system for non-public information.
- Remove non-public information from the publicly accessible organizational information systems, if discovered.
- Use of External Information Systems: All LeMoyne-Owen College Business Systems must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information assets, allowing authorized individuals to:
- Access the information asset from the external information systems.
- Process, store, and/or transmit organization-controlled information using the external information systems.
- Permitted Actions without Identification or Authentication: All LeMoyne-Owen College Business Systems must identify specific user actions that can be performed on the information asset without identification or authentication. In addition, LeMoyne-Owen College Business Systems must document and provide supporting rationale in the security plan for the information asset, user actions not requiring identification and authentication.

3.6.1 Remote Access

Policy Condition: Organization allows remote access to systems.
All LeMoyne-Owen College Business Systems using remote services must follow the **Remote Access Policy**. Additionally, they must:

- Document allowed methods of remote access to the information assets.
- Establish usage restrictions and implementation guidance for each allowed remote access method.
- Monitor for unauthorized remote access to the information asset.
- Authorize remote access to the information asset prior to connection.
- Enforce requirements for remote connections to the information asset.

3.6.2 Wireless Access

All LeMoyne-Owen College Business Systems must follow the **Wireless Communication Policy** for usage restrictions and implementation guidance. Additionally, unauthorized access should be monitored and requirements for wireless connections to the information asset should be enforced.

3.6.3 Access Control for Mobile Devices

Policy Condition: Organization has corporate data on personal devices.

All LeMoyne-Owen College Business Systems should:

- Establish usage restrictions and implementation guidance for organization-controlled mobile devices.
- Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information assets.
- Monitor for unauthorized connections of mobile devices to organizational information assets. Enforce requirements for the connection of mobile devices to organizational information assets.
- Disable information asset functionality that provides the capability for automatic execution of code on mobile devices without user direction.
- Issue specially configured mobile devices to individuals traveling to locations (**China, Russia, Iran, North Korea** and international locations which are considered sensitive by the Department of State) that the organization deems to be of significant risk in accordance with organizational policies and procedures.

3.7 Administration and Management

Account creation and control shall be governed by this standard. The following processes are required:

- New hires will be given a temporary password to login.
- All default passwords are changed at first login. This includes vendor supplied default credentials, passwords used by operating systems, software that provides security services, application and system accounts, Simple Network Management Protocol ("SNMP") community strings, etc.
- Unnecessary default or generic accounts are changed before system on the network, including firewalls, routers, servers, storage devices, wireless devices, etc. are connected to sensitive data or used to transmit sensitive data.
- Default application, database, and system passwords shall be changed by systems personnel before moving into production.
- Default user accounts provided with purchased software must be disabled or the account names changed upon installation.
- Default accounts must be used only for designated maintenance tasks and must not be employed for daily use.
- Security mechanisms shall restrict access to credentials for the least privilege necessary to perform job responsibilities and such access is based on job classification role and function.
- Approvals are secured by authorized parties specifying necessary access control lists.
- Access control lists for systems components shall be set to deny all unless privilege to a particular function is explicitly allowed.
- Termination procedures exist for handling data and they are well known by support staff and the LeMoyne-Owen College Information Security Team.
- Procedures exist that assign responsibility for removing IT and/or physical access to facilities and collection of premise keys, cards, and other mechanisms for secure facility access.
- Regular reviews of Users with access to sensitive information shall be performed to ensure they are appropriate, necessary, and valid.
- Establish norms for accounts of individuals on extended leave, new user accounts that have not been accessed and accounts not access for a period of time.
- Inactive accounts shall be disabled or removed from account databases.
  All internal accounts shall be monitored. Admin accounts shall be tracked and monitored.
  Installation and use of network utility programs by users (non-admin) should be restricted in {{Organization. name}}. The use of utility programmes should be logged and monitored/reviewed periodically.

3.8 New User Accounts

When creating and granting access for a new user account:

System administrators shall establish a unique ID and unique password/phrase separate from their regular

user account.
End user passwords will be conveyed to staff and customers in a secure manner.
End users will be required to change their initial password/phrase to something that adheres to policy and is known only to that user.

- Restrictions on software installation by users shall be established and enforced.

4.0 Enforcement and Exceptions

Access Enforcement: All LeMoyne-Owen College Business Systems must enforce approved authorizations for logical access to the system in accordance with applicable policy.

Information Flow Enforcement: All LeMoyne-Owen College Business Systems must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Exceptions to this requirement must be approved by **Richard Berroa**. A list of such exceptions should be maintained.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Controls

AC3.0 - Internal Account Tracking

Internal users for all company accounts are documented and monitored.
To prevent an opportunity for collusion, error and fraud, separation of duties is enforced. This ensures that the same user is not in charge of completing multiple tasks that may be a conflict of interest.

AC3.1 - Manage Account Access

HR and People Management systems are used for both onboarding and off-boarding of organization members.

AC3.2 - Revoke Access on Termination

Access rights of employees and contractors to information and systems are revoked upon termination of their employment, contract or agreement.

AC3.3 - Adjust Access on Role Change

Access rights of employees and contractors to information and systems are adjusted relevant to the changes on their employment, contract or agreement.

AC3.4 - Privileged Access Management System

A Privileged Access Management Platform is implemented to restrict and audit access of privileged accounts to identified critical information assets.

AC3.5 - Production System Account Management

An account management process is being followed on all production systems.

AC3.6 - Roles-based Access

Role-based access system has been defined and implemented to manage authentication and access to production systems.

AC3.7 - User Account Reviews

User reviews are performed periodically to validate accounts that are assigned to authorized personnel.