
**LeMoyne-Owen College**

# AC9 - Server Security

***March 16, 2020***

# AC9 - Server Security

*The organization manages, configures and protects organization servers and hosts based on industry best practices.*

# LeMoyne-Owen College Server Security Policy

## 1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by LeMoyne-Owen College. Effective implementation of this policy will minimize unauthorized access to LeMoyne-Owen College proprietary information and technology.

## 2.0 Scope

This policy applies to server equipment owned and/or operated by LeMoyne-Owen College, and to servers registered under any LeMoyne-Owen College-owned internal network domain.

Based on the type of servers, such as Cloud Managed Systems, Cloud Managed Instances or Physical Servers, the policy for handling patching, configuration, backups and monitoring shall vary. See table below.

| | Cloud Managed System | Cloud Managed Instance | Physical Servers |
|---|---|---|---|
| **Infrastructure Ownership** | Service Provider | Service Provider | LeMoyne-Owen College |
| **Configuration & Backup** | Managed by Provider | Managed by LeMoyne-Owen College | Managed by LeMoyne-Owen College |
| **Monitoring** | Managed by Provider | Managed by LeMoyne-Owen College | Managed by LeMoyne-Owen College |
| **Patch Management** | Managed by Provider | Managed by LeMoyne-Owen College | Managed by LeMoyne-Owen College |
| **Decommissioning** | Not Applicable | Not Applicable | Applicable |

## 3.0 Definitions

**Demilitarized Zone (DMZ):** A network segment external to the corporate production network. Server For purposes of this policy, a Server is defined as an internal LeMoyne-Owen College Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

**Intrusion Detection System (IDS):** A system that monitors network traffic for malicious activity.

**Intrusion Prevention System (IPS):** A network security prevention technology that examines network traffic flow to detect and prevent vulnerability exploits.

**SSH (Secure Shell):** SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

**IPSec (Internet Protocol Security):** IPSec is a suite of protocols for securing IP communications by authenticating and encrypting each IP packet of a data stream.

# 4.0 Policy

## 4.1 Ownership and Responsibilities

All servers deployed at LeMoyne-Owen College must be the responsibility of corporate IT. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by LeMoyne-Owen College IT. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by LeMoyne-Owen College IT.

Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact.
- Hardware and Operating System/Version.
- Main functions and applications, if applicable.
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

*Policy Conditions:*

- Physical security and maintenance of the infrastructure (hardware, software, networking, and facilities that run the Cloud services) is the responsibility of the Provider in case of Cloud Managed Systems and Cloud Managed Instances.
- Physical security and maintenance of the infrastructure (hardware, software, networking, and facilities that run server) is the responsibility of LeMoyne-Owen College in the case of Physical servers being used.

## 4.2 General Configuration and Backup Guidelines

Operating System configuration should be in accordance with approved LeMoyne-Owen College IT guidelines. Services and applications that will not be used must be disabled where practical.

- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account is acceptable.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- The production servers shall be backed up once a day.
- There might be other servers that may require fewer backups. Define the frequency for regular backups of such servers.

*Policy Conditions:*

- Configurations and backups for Cloud Managed Systems shall be managed by the provider.

- Configurations and backups for Cloud Managed Instances and Physical Servers shall be managed by LeMoyne-Owen College in accordance with the Server Security Policy.

## 4.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- Logs are accessible only to appropriate applications and trusted users (via sudo or similar access control).
- Review of logs will only be done with read-only access tools (e.g., view, more, less, graphical web tools for

accessing/filtering logs, etc.).
- All security related logs will be kept online for a minimum of 1 week.
- Security-related events will be reported to LeMoyne-Owen College IT, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.
  - Loss or breach of sensitive data.
- The server shall also be monitored for capacity requirements.

*Policy Conditions:*

- Logging and monitoring for Cloud Managed Systems shall be managed by the provider.
- Logging and monitoring for Cloud Managed Instances and Physical Servers shall be managed by LeMoyne-Owen College in accordance with the Server Security Policy.

## 4.4 Patch Management

All servers under LeMoyne-Owen College will be maintained with the latest security patches to their operating systems and key applications.

Each Department is responsible for servers under their control. When a patch is announced, an authorized system administrator must enter a change ticket according to the change management policy. A criticality rating of high or normal must be assigned. All high/critical patches must be applied as soon as practically possible, but not longer than thirty (30) calendar days after public release for any critical production server. All patches that are medium/high severity or for non-critical systems must be rolled out within ninety (90) calendar days. Any low priority patches will be installed on a case-by-case basis. All patches should be tested on development systems before being rolled out to production, where possible.

In case the patches cannot follow the aforementioned schedule, a document must be produced explaining why the patch must be deferred. Permissible deferrals may include a lack of appropriate change windows within the appropriate timeframe or a conflict with other critical changes scheduled at that time. Approvals shall be granted by CTO.

IT/Information Security is responsible for performing a vulnerability scan on their systems after each patch window to show that the patches were installed correctly. Clean vulnerability scan reports should be reviewed periodically.

*Policy Conditions:*

- Patch Management for Cloud Managed Systems shall be managed by the provider.
- Patch Management for Cloud Managed Instances and Physical Servers shall be managed by LeMoyne-Owen College in accordance with the Server Security Policy.

## 4.5 Decommissioning a Server

*Policy Condition:*

- Applicable to Physical Servers only.
- A set of defined measures should be followed to decommission servers.
- A “final” backup shall be made before decommissioning the server. This backup is kept for a year and then will be deleted sometime after the year is up.
- The data on the servers must be completely destroyed before the machine is taken out of service. The machine should be labeled accordingly.

## 4.6 Compliance

Audits will be performed on a regular basis by authorized organizations within LeMoyne-Owen College.

Audits will be managed by the internal audit group or LeMoyne-Owen College IT, in accordance with the Internal Audit Policy. LeMoyne-Owen College IT will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

Every effort will be made to prevent audits from causing operational failures or disruptions.

*Policy Conditions:*

- Applicable to Cloud Managed Systems and Cloud Managed Instances.
- LeMoyne-Owen College shall obtain and review ISO 27001/SOC 2 or equivalent compliance certificates for all Cloud Servers.

# 5.0 Enforcement

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

# Controls

## AC9.0 - Production Server AV/AS

Antivirus and antispam (AV/AS) software is installed and maintained on physical servers running production services.

## AC9.10 - Server Log Access

Access controls are implemented to prevent unauthorized access to event logs.

## AC9.11 - Server Performance and Capacity Monitoring

Resources are being monitored for capacity requirements.

## AC9.12 - Server Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain are synchronized to a single reference time source.

## AC9.13 - Server Security Configuration

Servers deployed are configured securely and its operating system (OS) hardened.

## AC9.14 - Server System Configuration Backups

Servers and hosts that contain critical and sensitive information are backed up periodically. The software system settings and data backups are systematically scheduled based on backup policies and procedures.
Alerts are configured to report to IT operations the status of completed backups.

## AC9.15 - Server Decommissioning

Best practices for decommissioning servers are followed.

## AC9.16 - Monitoring and Alerting System

Install/enable monitoring tool to increase visibility, check availability and reliability of the organization's infrastructure and application. The tool has an alerting function that sends notifications based on defined conditions.

## AC9.1 - Production Server Inventory

A server management inventory is updated every six months.

## AC9.2 - Production Server Firewalls

Firewalls are installed and enabled on all servers.

## AC9.3 - Production Server IDS or IPS

Intrusion detection systems (IDS) or Intrusion prevention systems (IPS) are installed and monitor production servers.

## AC9.4 - Production System Software Tracking

Software installations/upgrades on all production systems are controlled and documented.

## AC9.5 - Information Security Configuration for New and Updated Production Systems

Configuration standards are in place and are required to be utilized when deploying new systems into production.

## AC9.6 - Server Log Management

A centralized event and log management system is implemented.

## AC9.7 - Server Log Review

Logs generated from the management system are reviewed quarterly.

## AC9.8 - Server Log Integrity

Event log file integrity monitoring and alerting is set up to ensure logs remain intact and have not been tampered with.

## AC9.9 - Server Log Protection

Event logs are encrypted while in transit and encrypted while at rest within the centralized event & log management platform.