Michigan State University

College of Communication Arts & Sciences

Server Security Policy

Table of Contents

Server Security Policy

1 Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious actors. Consistent server installation policies, ownership and configuration management are all about doing the basics well and protecting the University.

2 Purpose

The purpose of this policy is to establish standards for physical hosting and base configuration of internal server equipment that is owned and/or operated by Michigan State University (MSU) and the College of Communication Arts and Sciences (CAS). Effective implementation of this policy will minimize unauthorized access to MSU proprietary information and technology. Use of these standards ensures that CAS and MSU consistently:

- Protects information assets;
- Helps satisfy legal, regulatory, and contractual requirements; and
- Applies best practices for information technology security and risk management while protecting the unimpeded flow of information.

3 Scope

All employees, faculty, staff, contractors, consultants, temporary and other workers at CAS must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by CAS or registered under a MSU-owned internal network domain.

4 Policy

4.1 General Requirements

4.1.1 Ownership

All internal servers deployed at CAS will be under the direct management of the CAS Systems Administrator and must be owned by an operational group that is responsible for system administration. Operational groups should monitor configuration compliance and implement policy tailored to their environment. The following items must be met:

- Servers must be registered within the CAS Technology asset management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a secondary contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the CAS Technology asset management system must be kept up-to-date.
- The CAS Systems Administrator must have administrator access to the server.

4.1.2 Auditing

For security, compliance, and maintenance purposes, authorized CAS Technology personnel may monitor and audit equipment, systems, processes, and network traffic.

4.2 Configuration Requirements

4.2.1 MSU Baseline Security Standards

System configuration must be in accordance with MSU baseline security standards.

4.2.2 MSU Website Security Standards

In addition to the baseline security standards, all MSU systems that host web services to the Internet must meet the MSU website security standards where appropriate.

4.3 Location Requirements

4.3.1 Security

Servers should be physically located in an access-controlled environment.

4.3.2 Prohibited Spaces

Servers are specifically prohibited from operating from uncontrolled office, lab, or cubicle areas.

4.3.3 Approved Locations

Approved locations for server hosting are limited to the following:

- Colocation
    - Colocation allows departments to place their existing servers in an enterprise university data center where other university applications, systems, and servers are housed.
- Virtual Servers
    - Virtual server hosting. This service offers access to the same high-performance, high-availability hardware, and security features that MSU and CAS use to deliver mission-critical applications and systems.

5 Policy Compliance

5.1 Compliance Measurement

The CAS Technology team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the CAS Technology team in advance.

5.2.1 Grandfather Clause

Any pre-existing CAS servers prior to April 30, 2017 are considered grandfathered in terms of server location only (section 4.3).

5.3 Non-Compliance

An employee found to have violated this policy may have server(s) under their purview removed from the network until said server(s) are verified to be in compliance.

6 Related Standards, Polices, and Processes

- MSU Baseline Security Standards
- MSU Website Security Standards

7 Revision History

Date of Change	Responsible	Summary of Change
April 2017	Samuel Mills	Policy document created