UF | College of Pharmacy
UNIVERSITY of FLORIDA

Information Technology Department

Document Number:	IT-SEC-0013	**Document Name:**	Server Security Policy
Effective Date:	?	**Approval Date:**	?
Document Type:	Policy	**Page Count:**	4
Document Status:	?	**Document Category:**	IT – Security
Document Owner:	Lane Blanchard	**Document Version:**	2.4

1.0 Revision History

Version	Date	Author(s)	Change Description
1.0	6/25/2015	Vincent Sposato, Nicholas Carter	Initial document drafted
2.o	10/17/2017	Lane Blanchard	Adopted initial drafted document from CQM as baseline
2.1	12/15/2018	Lane Blanchard	NONE
2.2	11/05/2019	Lane Blanchard	NONE
2.3	01/15/2021	Lane Blanchard	Added LINK to ***UF IT Security Monitoring of UF Information Technology Resources and Retrieval of Communications***
2.4	04/04/2023	Lane Blanchard	NONE

2.0 Policy Approval

Name of Approver: Shaima Coffey

Title of Approver: ISA and Executive Director

Approval Date: ?

3.0 Purpose

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

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

4.0 Policy Details

4.1 General Requirements

4.1.1 An operational group is responsible for system administration and must own all internal servers deployed at the College of Pharmacy. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the College of Pharmacy Information Security Manager (ISM). 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 College of Pharmacy ISM. The following items must be met:

- 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

4.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the ***UF IT Security Monitoring of UF Information Technology Resources and Retrieval of Communications***. LINK

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved UF Information Security guidelines.

4.2.2 Services and applications that will not be used must be disabled where practical.

4.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

4.2.4 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.

4.2.5 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 is sufficient.

4.2.6 Consistent adherence to the standard security principle of least required privilege to perform a function. For example, do not use the root or administrative account when a non-privileged account will provide sufficient access.

4.2.7 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 Secure Shell (SSH) or Internet Protocol Security (IPSec)).

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

4.2.9 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

4.3.1 All security-related events on critical or sensitive systems must be monitored via a log and audit trails, with the documentation of such saved as follows:

- All security related logs would be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 3 months.

4.3.2 Security-related events will be reported to College of Pharmacy ISM, who will review logs and report incidents to the College of Pharmacy ISM. 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

5.0 Policy Compliance

5.1 Compliance Measurement

The College of Pharmacy Information Security Manager (ISM), or their designee, will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru inspections, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner and privacy committee.

5.2 Exceptions

The College of Pharmacy Information Security Manager (ISM), or their designee must approve any exception to the policy in advance.

5.3 Non-Compliance

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

6.0 Policy Scope

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

This policy specifies requirements for equipment on the internal College of Pharmacy network.

7.0 Related Policies

No related policies were provided

8.0 Definitions

No definitions were required for this policy.

9.0 Supporting Information

No additional supporting information was provided.