Server Security Standard

Policy Title:
Server Security Standard

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This standard applies to servers procured through, operated, or contracted by Loyola University Chicago that house or interact with Loyola Protected data per the Data Classification Policy. The purpose of the Server Security Standard is to establish standards for the base configuration of servers. Effective implementation of this standard will minimize security incidents involving University resources.

II. Definitions

DHCP: A network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

DNS: The hierarchical and decentralized naming system used to identify computers reachable through the Internet or other Internet Protocol networks. The resource records contained in the DNS associate domain names with other forms of information.

NTP: An internet protocol used to synchronize with computer clock time sources in a network.

DMZ: A network (physical or logical) used to connect hosts that provide an interface to an untrusted external network – usually the internet – while keeping the internal, private network – usually the corporate network – separated and isolated form the external network.

SSH: A cryptographic protocol and interface for executing network services, shell services and secure network communication with a remote computer. Secure Shell enables two remotely connected users to perform network communication and other services on top of an unsecured network.

IPSEC: In computing, Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks.

SNMP: Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN). The purpose of SNMP is to provide network devices, such as routers, servers, and printers, with a common language for sharing information with a network management system (NMS).

SIEM: Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards, and reporting).

III. Policy

Ownership and Responsibilities

All servers deployed at the University must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs, and approved by the Chief Information Security Officer. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the University Information Security Office (UISO).

- Servers must be inventoried by each operational group. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Operating System, Version and Service Pack level
  - Main functions and applications, if applicable
- Server inventories must be kept up to date on a semi-annual basis.
- Configuration changes for production servers must follow the Change Management System Procedures.

Server Location

Servers that store, process, or transmit Loyola Protected data are classified as high security servers. Additionally, administrators may request that a server which does not store, process, or transmit Loyola Protected data be classified as a high security server. All high security servers must physically reside within secured ITS data centers.

If the high security server stores Protected data it must be segmented into a High Security (Internal) network security zone, per the ITS Network Firewall Policy.

If a high security server interacts with other high security servers and is required to publish content outside of the High Security network security zones, it must be segmented into the High Security DMZ network security zone per the ITS Network Firewall Policy.

General Configuration Guidelines

- Operating System configuration should be in accordance with approved Information Security guidelines, as defined in the References section of this document.
- A server housed in a High Security network security zone may not have more than one primary function. Core services (DHCP, DNS, NTP) may be housed on the same server in a High Security network security zone. If you are unsure of the number of functions on your server, contact the UISO.
- Disable all unnecessary and insecure services and applications.
- System access and security logging shall abide by the ITS Log Management Standard.
- Per PCI Standard 6.2, all servers within the high security environment must have the most recent OS and application security patches installed on the server within thirty days of its release.
- 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. Contact the UISO if you are unaware of alternatives to using trust relationships.
- All administrative access will be accomplished per the ITS Access Control Policy and Privileged Access Policy
- 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).
- Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).

Backup

- All security-related events on high security servers must be logged, saved, and sent to the Security Information Event Monitor (SIEM).
- All high security backups will be backed up to a separate tape pool. The list of items will be complied with:
  - Daily incremental backup will be retained for 30 days, and Items that are deleted will be retained for 400 days.
  - An inventory of this media will be maintained by the backup administrators.
  - No media moves outside of the secured data center.

- Any backup tapes that become decommissioned will be degaussed.

Monitoring

- Security-related events will be reported to the UISO. Corrective measures and information disclosure will be prescribed as needed, as per the ITS Incident Response Handbook. 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.

Compliance

- Audits will be performed on a yearly basis at a minimum by authorized UISO Office staff within the University.
- Audits will be managed by the UISO who will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- In accordance with the ITS Vulnerability Assessment Policy, every effort will be made to prevent audits from causing operational failures or disruptions.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Server Security Standard at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Data Classification Policy
- Change Management Policy
- ITS Access Control Policy
- ITS Incident Response Plan
- ITS Log Management Standard
- Privileged Access Policy
- ITS Vulnerability Assessment Policy
- ITS Security Policy
- RFC 1918
- The latest applicable CIS Benchmark

Approval Authority:	ITESC	**Approval Date:**	July 12th, 2018
Review Authority:	Jim Pardonek	**Review Date:**	July 31st, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu