# Server Provisioning and Deprovisioning STANDARD (SEC-S008)

Austin Peay State University

## 1.0 OBJECTIVE:

1.1 Austin Peay State University (APSU) is responsible for ensuring the confidentiality, integrity, and availability of data stored on its systems. Improperly configured systems, including both servers and workstations, can be compromised and the data destroyed or stolen, or used to store illegal data, relay span email, or attack other systems. This document establishes a standard for securing and documenting server systems on the campus network.

## 2.0 RESPONSIBILITIES:

2.1 The Information Technology Security director is responsible for implementation and enforcement of this Standard.

2.2 All server administrators, including Information Technology staff and/or other university employees who have or are responsible for the configuration and maintenance of any computer system that functions as a server on the campus network are required to abide by this Standard.

## 3.0 APPROVAL AUTHORITY:

3.1 Chief Information Officer

## 4.0 SCOPE:

4.1 This Standard, operating under University Policy 4:042 Information Security and Data Classification, defines terms and procedures for properly provisioning, deprovisioning, and restoring Austin Peay State University servers.

## 5.0 DEFINITIONS:

5.1 Campus Network – The wired and wireless components and information systems connected to the network managed by the university. Excluded are: the residence hall network, student wireless, and guest wireless.

5.2 Supported operating system – The entity (ex: vendor, open source or an individual) providing the operating system is actively and routinely providing and deploying patches and security updates for the operating system.

5.3 Server – Any computer in the campus network that is used to provide services (such as access to files or shared peripherals or the routing of email) and/or manages access to a centralized resource or application. Desktop, laptop, and lab equipment are not relevant to the scope of this Standard unless they are operating as a server.

5.4 Server Administrator – A university employee that configures and maintains one or more university servers. Most of the university's servers are maintained by the IT Infrastructure team.

5.5 University Information System – An application or software that is used to support academic, administrative, research, and outreach activities of the university, whether operated and managed by the university or a third-party vendor.

## 6.0 REQUIREMENTS:

### 6.1 Server Provisioning

a. Prior to any server installation, the server administrator must submit a service request ticket: Server Provisioning. Select "Build New Server" in the Request Type.

b. Provisioning a Windows server:

   i. Install the most current Windows supported operating system available that is specified by the server function or application. The end of support for the operating system must not be less than one year in the future from installation.
   ii. Join the new server to the APSU Windows domain unless otherwise authorized and documented by Information Technology Security.
   iii. Rename the local administrator account to something other than "administrator" and set the password for this account to meet or exceed the minimum requirements of the Password Management Policy.

c. Provisioning a Linux server:

   i. Install a Linux operating system distribution approved by the Office of Information Technology (OIT).
   ii. SSH access is blocked for the administrative account ROOT; a user requiring ROOT access must log in with a separate authorized account and then switch user with sudo.

d. Apply all relevant patches and security updates.

e. Onboard the server into the university's patch management system.

f. Onboard the server into the university's Endpoint Detection and Response (EDR) system.

g. If the server or application on the server will be operating as an SMTP server, OIT Infrastructure must approve and enable this requirement.

h. Notify OIT Infrastructure to add the server to the university's enterprise backup system.

i. Notify IT Security when the server is fully installed. This can be done by reassigning the service ticket to the IT Security team.

### 6.2 Server Deprovisioning

a. Prior to deprovisioning a server, the server administrator must submit a service request ticket: Server Deprovisioning.

b. Backup, transfer, or delete all data on the server.

c. If the server is a physical server, remove the server's disk drives and destroy them. Send the server to university surplus.

d. If the server is a virtual server, remove the server from the virtual environment.

e. Notify IT Security when the server is fully deprovisioned. This can be done by reassigning the service ticket to the IT Security team.

### 6.3 Server Restoration from Backup

a. Prior to any server installation, the server administrator must submit a service request ticket: Server Provisioning. Select "Restore Server From Backup" in the Request Type.

b. Request server restoration from the IT Infrastructure team.

c. When the server is restored, ensure the server provisioning requirements in section 6.1 of this Standard are met.

**d.** Notify IT Security when the server is fully restored. This can be done by reassigning the service ticket to the IT Security team.

### 6.4 Exceptions

a. Any exceptions to the requirements in sections 6.1, 6.2. and 6.3 must be approved by the Director of IT Security and documented in the service ticket.

## 7.0 ASSOCIATED DOCUMENTS:

7.1 4:042 Information Security and Data Classification Policy

7.2 4:029: Acceptable Use of Information Technology Resourses

7.3 4:039 Password Management Policy

## 8.0 RECORD RETENTION TABLE:

| Identification | Storage | Retention | Disposition | Protection |
|---|---|---|---|---|
| OITManagers Network Share | Electronic | Perpetual | Delete | Electronic Back-up |

## 9.0 REVISION HISTORY:

| Date: | Rev. | Description of Revision: |
|---|---|---|
| 8/18/2022 | | Initial Release |

*****End of Standard*****