Vendor Device Requirements Procedure

Office: Information Technology
Procedure Contact: Chief Information Officer
Related Policy or Policies: Information Security Policy

Revision History

Revision Number:	Change:	Date:
1.0	Initial Version	**April 2019**

A. Purpose

Vendor devices on the SOU network present a potential security risk to the University. Vendors are expected to take responsibility for the security of their devices. This document outlines the procedure for approving and installing vendor devices on the SOU network.

B. Definitions

A "network" is a system of electronic devices interconnected by telecommunication equipment or cables used to transmit or receive information. The bounds of a "network" may be defined by the ability of traffic to pass unimpeded between devices, similar to a broadcast domain, or a specific range of IP addresses, around which connectivity restrictions are based.

A "device" is a unit of physical microprocessor equipment, that either resides on the network, or has direct access to the data/traffic on the network.

Accessing a device "remotely" refers to any non-console access, or any console access that does not require physical presence at the device.

C. Institutional Approval

All vendor devices must be approved by SOU prior to installation on the network. SOU will perform appropriate steps to minimize the possible impact a compromised vendor device may have on the rest of network. This may include segregating the device on the network and/or providing physically secure locations for vendor hardware.

D. Indemnification

Vendor shall provide a legal document stating the vendor will indemnify and hold harmless SOU, its officers, officials, employees, students, and volunteers from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of or in connection with the use, function or activity of the device in question.

E. Remote Access

Remote access to devices shall not be allowed without connecting through a VPN, or another approved secure channel. SOU must approve remote access before implementation.

F. Physical Inspection

1. Any suspected tampering, replacement, or other suspicious activity involving devices on the network shall be immediately reported to the SOU Information Technology department.
2. SOU reserves the right to inspect the devices for compliance at any time without warning and remove devices at their discretion.

G. Device Hardening Recommendations

SOU recommends that vendors take the following measures to secure their hardware:

1. Ensure the device is running a supported version of its firmware or operating system, such that the device will receive critical security updates.
2. Ensure the following unsafe protocols are not allowed to operate on the device:
    a. Telnet
    b. SMTP
    c. FTP
    d. SSL/Early TLS
3. Remove any default SNMP community strings set by the manufacturer or vendor.
4. For all accounts that allow access to the device, set strong passwords.
5. Remove or disable any non-critical accounts allowing access to the device.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.