PCI Linux Configuration Standard

Policy Title:
PCI Linux Configuration Standard

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Officer

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

I. Policy Statement

This standard applies to all Linux Servers inside High Security Environment. This document outlines the standard process for deploying any Linux Virtual Machine for PCI in the High Security Environment.

II. Definitions

Not applicable.

III. Policy

Linux Virtual Machines inside High Security Environment must be deployed using the approved hardening standards as defined by the University Information Security Office. Only supported commercial versions of Linux are approved for deployment within PCI High Security.

The following outlines the security requirements:

- Password aging information to 90 days.
- Verify that in /etc/ssh/sshd_config file SSH for root is disabled.
- Apply IPTABLES rules as needed.
- Verify /etc/motd file has the appropriate warnings regarding PCI environment.
- Install latest file integrity monitoring agent on server and configure appropriately. Contact Security Administrator for latest agent and configuration details.
- Install needed services and applications making sure to change default passwords.

- Inform Backup Administrator of new PCI server
- Edit /etc/sudoers file to require root's password for "sudo su" command.
- Configure /etc/syslog/syslogng.conf file to send logs to SIEM. (Contact Security Administrator for settings).

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

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

VI. Related Policies

Please see below for additional related policies:

- Security Policy

Approval Authority:	ITESC	**Approval Date:**	August 4th, 2014
Review Authority:	Jim Pardonek	**Review Date:**	July 7th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu