Desktop Configuration – Antivirus - Network Authentication Policy
Policy Number 8-0002

Responsible Unit: Information Technology **Responsible Official**: Associate Vice Chancellor, Information Technology **Policy Classification**: Information Technology	Effective Date: 7/20/2008 Last Reviewed Date: 7/15/2019 Origination Date: 7/20/2008

1.0 Rationale:

The purpose of this document is to ensure security, minimize malicious attempts, and minimize software piracy on computing devices. This policy covers security of all Southern University Law Center (SULC) owned and/or supported devices.

2.0 Policy Scope:

This policy applies to all SULC users accessing and utilizing SULC technology resources.

3.0 Definitions:

User – SULC employees and students, contractors, vendors, and agents working under the auspices of the Law Center.

4.0 Policy Compliance:

Failure to with the policy will result in progressive disciplinary action up to and including termination.

5.0 Procedure:

1. **Desktop Configuration**: This section covers proper configuration of all SULC computers.

   For all SULC-supported operating systems running Windows 7 or above:

   - All computers, prior to being deployed on the SULC network, must be verified by the appropriate systems administrator.
   - All computers must have a unique name; no two machines should have the same name.
   - All local administrator accounts on computers ***must*** have passwords.
   - All computers should be installed as domain computers. (Any exceptions must be approved by Network Administrator.)
   - All computers must have the latest service packs, patches, and/or hot fixes for the operating system and Office applications.
   - All computers must have the latest anti-virus definitions.
   - All Faculty and staff, by default, are granted domain user privileges. Escalated permissions must be approved.
   - All local administrator passwords must have a minimum of seven (8) characters with a combination of upper and lowercase letters and numbers.
   - All local administrator passwords must be communicated to the Network Administrator.

- All in-house computer relocations must be handled by Information Technology Support Services staff.
- Peer-to-peer networking is prohibited.
- All file and printer sharing must be coordinated by the Network Administrator.
- All software installations must be coordinated by the Network Administrator.
- Unlicensed software is strictly prohibited from use on University-owned and supported computers.

2. **Guidelines on Anti-Virus Process**: This section ensures that all SULC computers have the latest anti-virus software installed that the necessary steps are taken in order to prevent and/or minimize viral attacks.

   For all SULC supported PCs running Windows 7 or above:

   - Always run the Enterprise Standard (CISCO AMP Antivirus), supported anti-virus software, which is available from the SULC server or through Active Directory (AD) Organizational Unit (OU) Placement. Download and run the current version and schedule a virus scan to run at regular intervals (e.g., 12:00am, daily) NOTE: Desktop computers must be configured as Managed clients through AD OUs.
   - NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
   - Delete spam, chain, and other junk email without forwarding, in accordance with SULCs *Email Use* policy.
   - Never download files from unknown or suspicious sources.

   - Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
   - Always scan a removable media from an unknown source for viruses before using it.
   - Back-up critical data and system configurations on a regular basis and store the data in a safe place.
   - When the anti-virus software is disabled, do not run any applications that could transfer a virus (e.g., email or file sharing).
   - All SULC owned computers must have SULC's standard, supported anti-virus software installed and scheduled to run at regular intervals.
   - All computers must maintain up-to-date patches, service packs, and/or hot fixes.
   - Virus-infected computers must be removed from the network until they are verified as virus-free.
   - SULC Administrators are responsible for creating procedures that ensure that anti-virus software is run at regular intervals.
   - SULC Administrators are responsible for ensuring that desktop computers are verified as virus-free.
   - Any activities with the intention to create and/or distribute malicious programs into SULC's network (e.g., viruses, worms, trojan horses, malware, etc.) are prohibited, in accordance with the SULC Email Use Policy.

3. **Network Authentication Policy:**

For all SULC Domain connected operating systems:

- A single domain provides a redundant, secure, and cost-effective management solution for University-owned computers.
- A single domain also means a single authentication is obtained.
- Single Sign-On access for federated services (e.g., Microsoft Office 365)

APPROVED: Lata Johnson **DATE:** 7/15/2019