POLICY TITLE

Cybersecurity Policy

POLICY NUMBER

8-001

Responsible Unit: *Division of Information Technology*	**Effective Date:** *03/12/2021*
Responsible Official: *Associate Vice President for Information Technology*	**Last Reviewed Date:** *03/01/2021*
Policy Classification: *Information Technology*	**Origination Date:** *01/01/2021*

I. POLICY STATEMENT AND RATIONALE

The Southern University System Cybersecurity Policy (SUS-CSP) provides the guiding principles for securing Information technology (IT) resources across the Southern University System.

II. POLICY SCOPE AND AUDIENCE

All Southern University System IT resource users and resources are covered by this policy.

III. POLICY COMPLIANCE

Violations of this policy may result in loss of Southern University system and network usage privileges, and/or disciplinary action, up to and including termination or expulsion as outlined in the applicable user policies.

IV. POLICY DEFINITIONS

- Endpoint: Laptop computers, desktop computers.
- Southern University System IT Resources: Southern University System owned Computers, Networks, Devices, Storage, Applications, or other IT equipment. "Southern University owned" is defined as equipment purchased or leased with either organization funding (including sources such as Foundation funds etc.)

V. POLICY IMPLEMENTATION PROCEDURES

Responsibilities: Information Security Officer

The Information Security Officer (ISO) leads the Cybersecurity team responsible for creating and maintaining the Southern University System's Information Security program. The purpose of the Information Security program is to maintain the confidentiality, integrity, and availability of organization IT Resources and organization data. In addition, the Information Security Officer, or a designee, is responsible for leading the investigation of and response to cybersecurity incidents. The response to any incident will be developed in collaboration with the data steward, organization Communications, legal counsel, and other campus offices as appropriate.

Users

Users are allowed access to only those systems that are required for the execution of their job duties. Southern University System IT Resource users are responsible for protecting the security of all data and IT Resources to which they have access. This includes implementing appropriate security measures on personally owned devices that access Southern University System IT Resources. Users are required to be knowledgeable in identifying general SPAM and Phishing tactics. In addition, users are required to keep their accounts and passwords secure in compliance with the Southern University System's existing *Acceptable Use of Technology Resources and Password Policies.*

Network Management

The Division of Information Technology (DoIT) team is responsible for planning, implementing, and managing the Southern University System's network, including wireless connections.

Only authorized IT personnel can install new devices on the Southern University System network. The Southern University System prohibits users from installing any of the following equipment:

- Routers
- Switches
- Hubs
- Wireless access points
- Voice over IP (VOIP) infrastructure devices
- Intrusion detection systems (IDS)
- Intrusion prevention systems (IPS)
- Virtual Private Networking (VPN)
- Consumer grade network technologies
- Wireless Printers
- Other networking appliances (that may not be included in this list)

Software System Administration

The DoIT System Administrator's team is responsible for proper maintenance of university-wide system resources, including servers, virtual machines (VM), cloud-based services, and backup and recovery systems.

IT Resources that are housed and managed by academic units and campus-based organizations must have a designated Software System Administrator. The Software System Administrator is responsible for proper maintenance of the system, even if the Software System Administrator is not a member of the DoIT technical support team. This responsibility must be acknowledged and documented. In addition, departmental and organizational system resources must be accessible to the DoIT technical support team for incident management purposes unless legal restrictions will not allow such access.

Negligent management of an organization owned IT Resource resulting in unauthorized user access or a data breach may result in the loss of system administration privileges.

Software system administration responsibilities for all organization-owned IT Resources, including those that are self-administered, include the following:

- Complying with all applicable Southern University System IT policies and procedures which includes adherence to username and password policies and procedures
- Performing an annual cybersecurity self-assessment, or as directed by the Cybersecurity Team, for the set of IT Resources administered
- Working with the IT support team to establish the following:
  - Installing and running endpoint security/management agents that have been approved by Southern University System's DoIT
  - Establishing an appropriate backup strategy and performing regular system backups
  - Regularly updating the operating system and other applications installed on the machine
  - Using, where possible and practical, central Southern University System's DoIT services for system login and account management (e.g. Active Directory)

General Procedures:

1. **Incident Reporting**: If a Southern University System IT Resource user suspects that a security incident has occurred or will occur, they should report the suspicion immediately to the Software System Administrator or IT Department. Users may also report the suspected security incident directly to appropriate campus DoIT Cybersecurity team at helpdesk@sus.edu, service@suno.edu, helpdesk@susla.edu, helpdesk@sulc.edu, helpdesk@suagcenter.com.

Software System Administrators who have identified any of the following security events should report the suspected security event to Southern University System Cybersecurity team at helpdesk@sus.edu, service@suno.edu, helpdesk@susla.edu, helpdesk@sulc.edu, helpdesk@suagcenter.com or an IT Team Member:

- Any occurrence of a compromised user account
- Any breach or exposure of protected or sensitive data
- Any occurrence of a server infected with malware
- Any occurrence of endpoints infected with malware
- Any other instance of malware or suspected intrusion that seems abnormal

2. **Enforcement:** Violations of this policy may result in loss of Southern University system and network usage privileges, and/or disciplinary action, up to and including termination or expulsion as outlined in the applicable user policies.

VI. POLICY RELATED INFORMATION

- Information Security Policy (Plan)
- Incident Response Plan
- Acceptable Use of Technology Resources

VII. POLICY HISTORY AND REVIEW CYCLE

This is a new policy. The effective date of this policy is determined by the approval dates of both the Chair of the Southern University System Board of Supervisors and the President-Chancellor of the Southern University and A&M College System. Additionally, the policy last review and origination dates are identified. This policy is subject to a five-year policy review cycle.

VIII. POLICY URL

The approved policy will be posted on the Southern University System website under Board Policies at *www.sus.edu.*

IX. POLICY APPROVAL

Ray L. Belton, Ph.D.
President-Chancellor, Southern University and A&M College System

Effective Date of Policy

The Honorable Attorney Domoine D. Rutledge
Chair - Southern University System Board of Supervisors

Effective Date of Policy