SOUTHERN UNIVERSITY AND A&M COLLEGE SYSTEM
J.S. CLARK ADMINISTRATION BUILDING
4TH FLOOR
BATON ROUGE, LOUISIANA 70813

OFFICE OF THE
VICE PRESIDENT FOR
FINANCE AND BUSINESS AFFAIRS

TELEPHONE: (225) 771-5550
FAX: (225) 771-2922

May 2, 2022

Dr. Ray L. Belton
President-Chancellor
Southern University System
4th Floor, J.S. Clark Administration Building
Baton Rouge, LA 70813

RE: SUS Cybersecurity Plan and Procedures for Management of Cash Assets

Dear Dr. Belton:

Attached for consideration by the Southern University Board of Supervisors is the Southern University System Cybersecurity Plan and Procedures for Management of Cash Assets. We have developed the policy and procedures for the Southern University System in accordance with Louisiana House Bill No. 128 Act 66 of the 2021 Regular Session of the Louisiana Legislature.

We are requesting your approval and the approval of the Board of Supervisors.

If you have any questions or need additional information, please let me know.

Sincerely,

Flandus McClinton, Jr.
Vice President for Finance and Business Affairs, SUS

Approved: ______________________________
Dr. Ray L. Belton, President-Chancellor

POLICY TITLE

Cybersecurity Plan for Management of Cash Assets

POLICY NUMBER

5-001

Responsible Unit: *Office of Vice President for Finance and Business Affairs*	**Effective Date:** *05/20/2022*
Responsible Official: *Vice President for Finance and Business Affairs*	**Last Reviewed Date:**
Policy Classification: *Finance*	**Origination Date:** *05/20/2022*

I. POLICY STATEMENT AND RATIONALE

The Southern University System Board of Supervisors (System) established this policy to protect confidential/sensitive online cash management data from malicious digital cyber-attacks which includes accessing, changing or deleting sensitive data as well as gaining access to online banking modules for the purpose of stealing or manipulating cash assets in accordance with Louisiana House Bill No. 128 Act 66 of the 2021 Regular Session of the Louisiana Legislature.

II. POLICY SCOPE AND AUDIENCE

This policy applies to all employees requiring direct access to System bank accounts of the Southern University System as well as Information Technology (IT) related equipment and devices comprising the System's network. System employees shall comply with the Cybersecurity Plan (Plan) and Financial Security Procedures (Procedures) in use of System information technology systems and networks for the protection of digital data on System network(s) related to management of cash assets.

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 as outlined in the applicable user policies and Handbook of University Personnel.

IV. POLICY DEFINITIONS

a. *Southern University System IT Resources* Southern University System owned computers, networks, devices, storage, applications, or other IT equipment.

"Southern University System owned" is defined as equipment purchased or leased with either organization funding (including sources such as Foundation funds, etc.).

b. *Networks* Include, but not limited to, hardware, software, communications networks, physical facilities, personal computers and printers, and personal handheld devices.

V. POLICY IMPLEMENTATION PROCEDURES

a. Responsibilities of the System President-Chancellor

Establishing an approved Cybersecurity Plan (Plan) and Financial Security Procedures (Procedures) and ensuring employees are fully aware of information security requirements for cash management and financial security.

Designating an administrator for the implementation and ongoing maintenance of the Plan.

Submitting revisions of the Plan and Procedures to the Cash Management Review Board for approval.

b. Designation of an Administrator and Responsibilities

The System President-Chancellor shall designate the System Vice President for Finance and Business Affairs as the System Administrator. The Chancellor of each institution within the System, shall designate an Administrator for each campus.

The responsibilities of the System Administrator are as follows:

1) Recommending to the President-Chancellor recommended updates to the Plan and Procedures to incorporate advancements in cybersecurity of cash resources of the System.
2) Enforcing the compliance with the Plan and Procedures.
3) Designating network rights to System staff based on operational needs of the System.
4) Notifying System Chief Information Officer of security incidents and providing recommended resolutions to the security incident.

The responsibilities of the Campuses' Administrators are as follows:

1) Recommending to the Chancellor and System Administrator recommended updates to the Plan and Procedures to incorporate advancements in cybersecurity of cash resources of the System.
2) Enforcing the compliance with the Plan and Procedures.
3) Designating network rights to Campus staff based on operational needs of the System or Campus.
4) Notifying System Chief Information Officer and Campus Information Technology Director of security incidents and providing recommended resolutions to the security incident.

c. Information Technology (IT) System Chief Information Officer (CIO) and Campus Information Technology Directors Responsibilities

The responsibilities of the IT System Chief Information Officer and Campus IT Directors are as follows:

1) Working with the System and Campus Administrators to setup employee online access to System's cash resources required to perform assigned duties related to cash management.
2) Recommending hardware, servers, cloud services, on premise software applications, software, infrastructure or platform that provides the safest online access to System's cash resources within the System's network.
3) Documenting and updating specific guidelines for password and network usage by incorporating System's Division of Information Technology's standards and industry best practices.
4) Requiring all computers connected to the System's network have current antivirus software installed and enabled and performing recurring scans for malicious viruses at least once a week.

d. System Employees Responsibilities

The responsibilities of the System employees are as follows:

1) Complying with the approved Cybersecurity Plan and Financial Security Procedures and taking reasonable steps to protect the System's computer systems and network.
2) Completing required online IT security awareness training programs.
3) Ensuring full protection of all assigned user ids, passwords, and bank security tokens.
4) Exercising caution when opening suspicious emails with links and/or attachments.
5) Passing periodic simulated phishing tests or similar criminal attempts to compromise the System's financial security of cash management.
6) Notifying IT immediately of any virus/malware/ransomware transmitted to computer.
7) Employees are required to immediately close websites used for bank account access after logging off and to logoff the System's network at the end of each workday.
8) Ensure no personal wireless devices such as personal laptops, cell phones, tablets, or similar may be accessed or connected to the System's network for the purpose of accessing System bank accounts, except in circumstances specifically authorized by the President-Chancellor, Chancellors, and/or System and Campus Administrators.

VI. POLICY RELATED INFORMATION

- Louisiana House Bill No. 128 Act 66 of the 2021 Regular Session of the Louisiana Legislature
- Cybersecurity Financial Security Procedures for Cash Management

- System Employee Acknowledgement Form

VII. POLICY HISTORY AND REVIEW CYCLE

This is a new policy. The effective date of this policy is determined by the approval date of the President-Chancellor of the Southern University and A&M College System and the Chair of the Board of Supervisors 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 to the Southern University System website under Board Policies at *www.sus.edu.*

IX. POLICY APPROVAL

The effective date of this policy is determined by the approval date of the President-Chancellor of the Southern University and A&M College System and the Chair of the Board of Supervisors of the Southern University and A&M College System.

_______________________________________ _____________________

Ray L. Belton, Ph.D. ***Effective Date of Policy***
President-Chancellor, Southern University and A&M College System

_______________________________________ _____________________

The Honorable Atty. Edwin Shorty ***Effective Date of Policy***
Chair - Southern University System Board of Supervisors

ATTACHMENT A

CYBERSECURITY PLAN and

FINANCIAL SECURITY PROCEDURES

RELATED to the MANAGEMENT OF CASH ASSETS

EMPLOYEE ACKNOWLEDGEMENT

My signature hereon acknowledges that:

1) I have received a copy of the System's Cybersecurity Plan and Financial Security Procedures.

2) I have read this Plan.

3) I understand the content of this Plan.

4) I agree to comply with the terms and provisions of this Plan.

5) I understand that compliance with this Plan is a condition of employment/continued employment; and

6) I understand that disciplinary action, including the possibility of termination, will be imposed for violating the terms and conditions of this Plan.

______________ **DATE**	______________________ **EMPLOYEE (Signature)**
	______________________ **EMPLOYEE (Printed Name)**

POLICY TITLE
Cybersecurity Financial Security Procedures

POLICY NUMBER
5-002

Responsible Unit: *Office of Vice President for Finance and Business Affairs*	**Effective Date:** *05/20/2022*
Responsible Official: *Vice President for Finance and Business Affairs*	**Last Reviewed Date:**
Policy Classification: *Governance*	**Origination Date:** *05/20/2022*

I. POLICY STATEMENT AND RATIONALE

The Southern University System Board of Supervisors (System) established this policy to protect confidential and sensitive online cash management data from malicious digital cyber-attacks, which includes accessing, changing or deleting sensitive data as well as gaining access to online banking modules for the purpose of stealing or manipulating cash assets in accordance with Louisiana House Bill No. 128 Act 66 of the 2021 Regular Session of the Louisiana Legislature.

II. POLICY SCOPE AND AUDIENCE

This policy applies to all employees requiring direct access to System bank accounts of the Southern University System as well as Information Technology (IT) related equipment and devices comprising the System's network.

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 as outlined in the applicable user policies and Handbook of University Personnel.

IV. POLICY DEFINITIONS

a. *Southern University System IT Resources* Southern University System owned computers, networks, devices, storage, applications, or other IT equipment. "Southern University System owned" is defined as equipment purchased or leased with either organization funding (including sources such as Foundation funds, etc.).

b. *Networks* Include, but not limited to, hardware, software, communications networks, physical facilities, personal computers and printers, and personal handheld devices.

c. *ACH* Automated Clearing House (ACH) is an electronic network for financial transactions in the United States.

d. *ACH Debit Block* An additional safeguard to keep business accounts secure. Adding a payee to the allowed payees list permits the payee to debit funds by ACH from bank accounts.

e. *Zero Balancing Accounts (ZBA)* A ZBA is a checking account in which a balance of zero is maintained. When funds are needed in the ZBA, the exact amount of money required is automatically transferred from a central or master account.

f. *Positive Pay Services* Positive pay is an automated cash-management service used by financial institutions employed to deter check fraud. Banks use positive pay to match the checks a company issues with those it presents for payment. Any check considered suspect is sent back to the issuer for examination.

g. *Post No Checks Service* Completely blocks any fraudulent checks from posting to accounts that do not issue checks.

V. POLICY IMPLEMENTATION PROCEDURES

a. Responsibilities

The System Vice President for Finance and Business Affairs is responsible for the Plan's maintenance and enforcement. System and Campus Administrators are responsible for assigning administrative rights and controls. Administrators will respond to and resolve security issues. Everyone with access to online bank accounts is responsible for adhering to this policy.

b. Safeguards Over Cash Management

All System bank accounts will have the following safeguards in place. If any exceptions are needed for business purposes, approval will be properly documented and requested from the System President-Chancellor and/or System Vice President for Finance and Business Affairs.

- ACH Debit blocks will be utilized on all Zero-Balancing Accounts (ZBAs).
- Post No Checks services, if available, will be utilized on all Deposit Only Accounts.
- Positive Pay services, if available, are required for all bank accounts disbursing funds via check.

- Wires or ACHs will not be sent from any ZBA accounts.
- All ACH files will be dated at least one day after the file is transmitted to the bank.
- ZBAs will be required to have at least two security administrators.

The following are requirements for all System employees with access to online cash assets:

- Attend online cyber training presented by JPMorgan Chase or campus banking institution on an annual basis.
- Multi-factor authentication must be used when accessing online bank accounts.
- Banking information must be kept confidential and only provided to others when necessary and upon approval of System or Campus Administrator.
- All user ids, passwords, and multi-factor authentications shall not be shared with others.
- Users shall use caution when clicking on any links in emails or other messages.
- All payment information, including any changes, should always be validated and documented before making the payment or the change in accordance with standard procedures.
- Any information, banking or payment related, sent via email should only be sent if encrypted.
- The System and Campus Administrators shall be notified of any issues or potential issues.

All bank accounts that have been dormant for more than twelve (12) months will be closed and the Cash Management Review Board (CMRB) shall be notified.

All bank accounts will be reconciled within a timely manner.

VI. POLICY RELATED INFORMATION

- Louisiana House Bill No. 128 Act 66 of the 2021 Regular Session of the Louisiana Legislature
- System Cybersecurity Plan for Cash Management
- System Employee Acknowledgement Form

VII. POLICY HISTORY AND REVIEW CYCLE

This is a new policy. The effective date of this policy is determined by the approval date of the President-Chancellor of the Southern University and A&M College System and the Chair of the Board of Supervisors 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 to the Southern University System website under Board Policies at *www.sus.edu.*

IX. POLICY APPROVAL

The effective date of this policy is determined by the approval date of the President-Chancellor of the Southern University and A&M College System and the Chair of the Board of Supervisors of the Southern University and A&M College System.

Ray L. Belton, Ph.D. *President-Chancellor, Southern University and A&M College System*	***Effective Date of Policy***
The Honorable Atty. Edwin Shorty *Chair - Southern University System Board of Supervisors*	***Effective Date of Policy***