Bank of South Sudan

Cybersecurity Guidelines

July 2026

Contents

Bank of South Sudan Cybersecurity Guidelines

1. Preamble

Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by the worldwide distribution of information and communication technology (ICT) devices and networks. In light of the growth of IT in the banking sphere, providing the right kind of focus for creating a secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices, and networks has become one of the compelling priorities. Protecting information infrastructure and preserving the confidentiality, integrity, and availability of information in cyberspace is the need of the hour. This policy aims to ensure proper access to and usage of IT resources and prevent their misuse by users.

2. Purpose

These cybersecurity guidelines aim to protect information and infrastructure from cyber incidents through processes, guidelines, technology, and cooperation. This policy governs the usage of IT Resources from an IT perspective to the end user's perspective. This policy defines what we want to protect and what we expect of our system users. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords, and how we will monitor the effectiveness of our security measures.

3. Scope and Applicability

These cybersecurity guidelines apply to the Bank of South Sudan and all individuals and entities that interact with, access, or manage the Bank's information systems, data, and digital infrastructure. The Bank should ensure that all users uphold this policy's principles and urge them all to adhere to the provisions of this policy.

4. The Core Functions of the NIST CSF

The National Institute of Standards and Technology Cybersecurity Framework is a valuable resource for organizations of all sizes and industries seeking to improve their cybersecurity posture and manage risks.

a. **Identify:**

This function focuses on understanding the organization's assets, systems, and data and creating a cybersecurity strategy.

b. **Protect:**
   This function involves implementing security measures to safeguard assets and systems from threats.

c. **Detect:**
   This function focuses on monitoring and identifying security incidents and threats.

d. **Respond:**
   This function outlines how to respond to and mitigate security incidents, including communication plans and containment efforts.

e. **Recover:**
   This function focuses on restoring affected systems and services after an incident and ensuring business continuity.

f. Govern:
   This function guides the development of a cybersecurity governance model, including roles and responsibilities.

Cybersecurity Guidelines Statement

1. Inventory Management of Critical IT Assets

1.1. The Bank should maintain an accurate and up-to-date IT Asset Inventory Registry containing the following fields, as a minimum:

a. Details of the IT Asset (hardware, software, network devices, key personnel, services, etc.)
b. Details of the systems where customer data is stored.
c. Associated business applications, if any.
d. Criticality of the IT Asset (e.g., High/Medium/Low)
e. Software implemented.

1.2. Classify data/information based on the information's sensitivity criteria.

1.3. Appropriately manage and protect within and outside the bank/network, keeping in mind how the data/information is stored, transmitted, processed, accessed, and used within/outside the Bank's network and the level of risk exposure depending on the sensitivity of the data/information.

2. Preventing Installation/Use of Unauthorized Software

2.1. Maintain an up-to-date and preferably centralized inventory of authorized software/ approved applications/ libraries, etc.

2.2. Put in place a mechanism to control the installation of software/ applications on end-user PCs, laptops, workstations, servers, mobile devices, etc., and block/ prevent and identify the installation and running of unauthorized software/ applications on such devices/ systems.

2.3. Ensure licensed software/ applications are installed only on the servers/ end-user devices.

2.4. Software Installation and Use:

a. Authorized software: It can only be installed and allows bank employees to use software approved by the IT department. Unauthorized software installations are prohibited to prevent security vulnerabilities.

b. Software licensing: Ensuring all software is appropriately licensed, and employees do not engage in software piracy because pirated software comes with malware that results in security vulnerabilities.

3. Environmental Controls

3.1. Implement appropriate controls for securing physical location/ access to critical assets (as identified by the Bank under their inventory of IT assets), protecting them from natural and artificial threats. Permit only authorized access to critical infrastructure, such as Data Centers, and all entry/ exit should be logged and monitored.

3.2. Put in place mechanisms for monitoring breaches/ compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc.

4. Network Management and Security

4.1. Ensure that all network devices are secure and periodically accessed to ensure that such configurations are securely maintained.

4.2. The Network Department must change all default passwords of the network devices/ systems after installation.

4.3. Put appropriate controls in place to secure the wireless local area network, access points, and client access systems.

4.4. The critical infrastructure of the Bank (CBS, SWIFT, NPS, BSA, ERP, EBS, etc.) should have adequate network segregation controls.

4.5. Conduct quarterly vulnerability assessments on the critical banking system, network devices, servers, and penetration testing at least annually or after any significant change in infrastructure or configuration.

4.6. Block access to specific IPs and Ports based on an Active Directory Group. Using Windows Firewall Advanced Security (WFAS).

4.7. The ICT should restrict Internet usage to identified standalone computer(s) in the Bank that are strictly separate from the systems identified for running day-to-day business.

4.8. Ensure internet access through a domain controller and restrict it to domain-joined computers, configure the network infrastructure to route

internet traffic through the domain controller, and use firewall rules or network policies to block internet access for non-domain computers.

4.9. Turn off the mobile hotspot feature in Windows through a Group Policy Object (GPO) by configuring the *"Prohibit use of Internet Connection Sharing on the DNS domain network"* policy.

4.10. Internet usage: The Bank must restrict the use of Internet resources to professional activities only.

Specifically:

a. Work-related browsing: Employees should use the internet to research, communicate with clients, or access work-related databases.

b. Social media: Access to social media during work hours is limited to company-related activities, such as managing official social media accounts. The network department staff should reserve personal social media activity for break times by creating policies in the AD Group Policy.

5. Secure Configuration

5.1. The Network Department should periodically evaluate critical device configurations (such as firewalls, network switches, security devices, etc.).

5.2. The Bank should use systems such as networks, applications, databases, and servers dedicated to their configured purpose.

5.3. Ensure that the servers, network devices, etc., are hardened per standards and best practices.

6. Antivirus and Patch Management

6.1. Implement systems or processes to identify, track, manage, and monitor the status of patches to servers, operating systems, and application software running on the systems used by the bank staff (end-users).

6.2. Implement and update endpoint antivirus protection for all servers and end-user computers, preferably through a centralized system.

7. User Access Control/ Management

7.1. Disable/ disallow administrative rights on end-user workstations/PCs/Laptops and provide access rights on a 'need to know' and 'need to do' basis.

7.2. Configure Active Directory Server with domain administration rights and include end-user computers as part of the central domain server.

7.3. Passwords should be complex and lengthy, and users should not use the same passwords for all applications/systems/devices.

7.4. Implement appropriate (e.g., centralized) systems and controls to allow, manage, log, and monitor privileged/superuser/administrative access to critical systems (servers/databases, applications, network devices, etc.)

7.5. Prioritize data security, compliance, and employee accountability, covering aspects like password management, software usage, data handling, and acceptable online activities while ensuring clear communication and enforcement.

8. Secure Mail and Messaging Systems

8.1. Implement secure mail and messaging systems that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links, etc.

8.2. Implement secure practices such as 2-step verification for mail logins.

9. Removable Media

9.1. Restrict USB access on a Domain Controller. Use Group Policy to create a policy that denies access to removable storage.

9.2. As a default rule, removable devices and media should not be permitted in the banking environment unless authorized explicitly for defined use and duration.

9.3. Secure the usage of removable media on workstations/PCs/Laptops, etc., and secure erasure/ deletion of data on such media after the user.

9.4. Scan the removable media for malware/ antivirus before providing read/ write access.

9.5. Employees must securely wipe removable media or physically destroy it before disposal or reuse to ensure no recoverable data remains.

10. User/Employee/Management Awareness

10.1. Communicate to users/employees, vendors, and partners security policies covering secure and acceptable use of the Bank's network/assets, including customer information/data, educating them about cybersecurity risks and protection measures at their level.

10.2. Conduct awareness/training for management/staff on basic information security controls (Do's and Don'ts), incident reporting, etc.

10.3. The ICT Directorate may update Board members on basic tenets/principles of IT risk/cybersecurity risk at least once a year.

10.4. The end-users should be aware that they should never open or download an email attachment from an unknown source.

10.5. The ICT Directorate should regularly organize training and awareness programs on IT resource use. To ensure security awareness amongst Employee to enable them to meet their security obligations.

11. Data Classification and Protection

11.1. Data Classification:

a. Confidential data: This may require encryption, secure storage, and restricted access based on a "need to know" basis.

b. Public data: This may be accessible to anyone, with minimal security requirements.

a. Protected data: This may be subject to specific regulations, such as DPP, Cybercrimes, and Computer Misuse Provisional Order 2021, or HIPAA, requiring additional security measures.

11.2. Data Protection:

a. Guidelines and practices to ensure the privacy, security, and compliance of personal data. It outlines how data is collected, stored, processed, and shared, and the rights of individuals whose data is being handled.

12. Backup and Restoration

12.1. Take periodic backups of the critical data and store this data offline (i.e., transferring essential files to a storage device detached from a computer/system after copying all the files).

13. Vendor/Outsourcing Risk Management

13.1. All the outsourcing service level agreements (SLAs) signed with the vendors must mention the responsibility of the Bank and the vendor in case of any service failure.

13.2. The Bank shall periodically review vendors' service level agreements for performance in security controls.

14. Policy Compliance and Dissemination

a. All employees must adhere to the policy, and the management has the right to take disciplinary action in case of its violation, such as written warnings, temporary suspension, or any other disciplinary action in line with the ETS and EDR.

b. Individuals could be subject to legal consequences under the applicable laws if violations involve illegal activities.

c. Employees operating from remote/outside organization networks should strictly connect via VPN to access applications and corporate networks.

d. All employees should implement appropriate controls to ensure their compliance with this policy.

e. The ICT Directorate will ensure the resolution of all incidents related to the security aspects of this policy by its users.

f. Users should not install any network/security device on the network without consultation with the Implementing Department.

g. The ICT Directorate should ensure proper dissemination of this policy annually and update it as needed to ensure continued compliance with best practices and legal requirements.

h. The ICT Directorate may use newsletters, banners, bulletin boards, corporate websites, intranets, etc., to increase awareness of this policy amongst its users.

i. Orientation programs for recruits should include a session on this policy.

15. Monitoring and Review

a. The Bank shall have the right to audit networks and systems at regular intervals from the point of compliance with this policy.

b. The Bank may access, review, copy, or delete any electronic communication or files stored on the user's devices for security-related reasons or compliance with applicable laws. That includes files, emails, and Internet history.
c. The Department of Governance & Cybersecurity must monitor and review this policy.
d. The Directorate of ICT should establish a periodic reporting mechanism to ensure compliance with this policy.

Approval:

This Cybersecurity Framework Control Policy is approved and signed by Hon. Dr. Addis Ababa Othow, Governor of the Bank of South Sudan, and shall take effect from ...13..... The month of...August..., 2026.

Appendices:

Appendix A: Definitions of Terms and Acronyms

a. "The Bank," the "Central Bank," and "BoSS"- All refer to the Bank of South Sudan
b. Cybersecurity Control Policy - A document that outlines the rules and practices the Bank uses to safeguard its data and resources from cyber threats and attacks
c. NIST CSF - Stands for National Institute of Standards and Technology Cybersecurity Framework
d. Cybercrimes and Computer Misuse Provisional Order 2021 - A law enacted to prevent and address crimes committed using computers, the internet, or related technologies in South Sudan.
e. MFA - Multi-factor Authentication
f. CBS - Core Banking System
g. SWIFT - stands for Society for Worldwide Interbank Financial Telecommunications. A global messaging service that allows financial institutions to communicate and transfer funds securely and quickly.
h. NPS-National Payment System
i. BSA - Banking Supervision Application
j. ERP - Enterprise Resource Planning
k. EBS - Enterprise Business System
l. DPP - Data Protection Policy
m. HIPAA - Health Insurance Portability and Accountability Act