DRAFT CYBERSECURITY GUIDELINES FOR FINANCIAL SERVICE PROVIDERS, 2026

BANK OF TANZANIA

March 2026

TABLE OF CONTENTS

PART I

PRELIMINARY

1.1 Citation

These Guidelines shall be cited as *the Cybersecurity Guidelines for Financial Service Providers, 2026.*

1.2 Authorization

These Guidelines are issued under Section 71 of *the Banking and Financial Institutions Act, 2006* and Section 56(3) of *the National Payment Systems Act, 2015*.

1.3 Application

These Guidelines shall apply to all financial service providers operating in the United Republic of Tanzania, except where prescribed otherwise by the Bank in other regulations, guidelines, circulars, or any other directives.

1.4 Interpretation of Terms

In these Guidelines, unless the context otherwise requires:

“Bank” means the Bank of Tanzania; and

“Financial service provider” means an institution licensed, regulated, and supervised by the Bank in accordance with *the Banking and Financial Institutions Act, 2006* and *the National Payment Systems Act, 2015*.

1.5 Purpose

The Guidelines are intended to:

(a) Strengthen the regulatory framework for ensuring a secure cyberspace for the financial service providers;

(b) Establish a coordinated approach towards prevention and response to cyber incidents;

(c) Promote continuous cybersecurity awareness creation to all relevant stakeholders;

(d) Promote compliance with appropriate technical and operational cybersecurity standards; and

(e) Maintain public trust and confidence in the financial sector ecosystem.

1.6 Scope

The Guidelines establish minimum standards that financial service providers shall adopt to implement effective cybersecurity governance and risk management frameworks, taking into account increasing digitization, the evolving cyber-threat landscape, the growing sophistication of cyber incidents, and the need to enhance cyber resilience.

PART II

GOVERNANCE

Financial service providers shall establish a robust cybersecurity governance structure to ensure the effective implementation and consistent application of these Guidelines. The key stakeholders within this governance structure shall include, at a minimum, the following roles and responsibilities:

2.1 Board of Directors

The Board of Directors of a financial service provider shall have ultimate responsibility for the formulation, approval, and oversight of the implementation of the institution’s cybersecurity strategy, policies, procedures, and minimum cybersecurity standards. At a minimum, the Board of Directors shall:

(a) approve and periodically review the institution’s cybersecurity strategy to ensure alignment with the institution’s overall business objectives, risk appetite, and regulatory obligations;

(b) ensure the establishment of an effective cybersecurity governance framework, including clear roles, responsibilities, and reporting lines across management and control functions;

(c) approve cybersecurity policies and frameworks, and define the institution’s cyber risk appetite and tolerance levels consistent with its overall risk management framework;

(d) oversee the identification, assessment, monitoring, and mitigation of cyber risks, including risks arising from third-party arrangements, outsourcing, and emerging technologies;

(e) ensure that management allocates sufficient financial, technical, and human resources to implement and maintain effective cybersecurity controls and capabilities;

(f) oversee the institution’s cyber resilience, including incident response, crisis management, business continuity, and disaster recovery arrangements, and ensure regular testing and improvement of these capabilities;

(g) require timely, accurate, and meaningful reporting from senior management on the institution’s cybersecurity posture, material cyber risks, incidents, and remediation efforts;

(h) foster a strong cybersecurity culture by setting the tone at the top and ensuring that cybersecurity awareness and accountability are embedded throughout the organization; and

(i) ensure periodic independent assessments, audits, or reviews of the institution’s cybersecurity framework and controls, and oversee the timely remediation of identified weaknesses.

2.2 Senior Management

(a) develop, implement, and maintain Board-approved cybersecurity strategy, policies, and frameworks in line with the institution’s business objectives, risk appetite, and regulatory requirements;

(b) establish and maintain an effective cybersecurity governance structure, including assigning clear roles, responsibilities, accountability, and escalation mechanisms across business units, risk management, and control functions;

(c) identify, assess, monitor, and manage cyber risks on an ongoing basis, including risks arising from information systems, digital channels, data assets, third-party service providers, outsourcing arrangements, and emerging technologies;

(d) design, implement, and operate appropriate cybersecurity controls and safeguards to prevent, detect, respond to, and recover from cyber threats, consistent with the institution’s risk appetite and tolerance levels;

(e) ensure adequate financial, technical, and human resources are allocated to support effective cybersecurity operations, including skilled personnel, tools, technologies, and training programs;

(f) ensure timely escalation and reporting of significant cyber risks, incidents, vulnerabilities, and control weaknesses to the Board and relevant committees, including root-cause analysis and remediation progress;

(g) promote and embed a strong cybersecurity culture across the institution by ensuring staff awareness, training, adherence to policies, and accountability for cybersecurity responsibilities at all levels;

(h) manage third-party and outsourcing cyber risks by conducting due diligence, defining security requirements in contracts, monitoring service providers, and ensuring compliance with regulatory and internal cybersecurity standards;

(i) ensure continuous monitoring, testing, and improvement of cybersecurity controls, including vulnerability assessments, penetration testing, and remediation of identified weaknesses;

(j) support independent assurance activities by facilitating internal audit, external audit, and regulatory reviews, and ensure timely and effective remediation of findings and recommendations; and

(k) Promote financial sector collaboration and information sharing on matters related to cyber threats.

2.3 Cybersecurity Steering Committee

Each financial service provider shall establish a Cybersecurity Steering Committee responsible for governing its cybersecurity program. The steering committee shall comprise senior representatives from relevant departments. The functions of the committee shall be:

(a) support senior management in translating the Board-approved cybersecurity strategy, risk appetite, and policies into actionable plans, priorities, and initiatives across the institution;

(b) provide oversight of the implementation and ongoing effectiveness of the cybersecurity governance framework, ensuring clear coordination among business units, IT, information security, risk management, compliance, and internal audit;

(c) review and recommend approval of cybersecurity policies, frameworks, standards, and major program initiatives to senior management and the Board;

(d) monitor the institution’s cybersecurity risk profile, including assessment and treatment plan and ensure risks remain within the approved cyber risk appetite and tolerance;

(e) monitor the management of cyber risks arising from third-party arrangements, outsourcing, cloud services, and other external dependencies, and ensure consistent application of cybersecurity requirements;

(f) review significant cybersecurity incidents, near misses, and control weaknesses, including root-cause analysis, lessons learned, and remediation actions, and ensure appropriate escalation to senior management and the Board;

(g) review and monitor the adequacy of cybersecurity resources, including budget, staffing, skills, tools, and technologies, and recommend enhancements to senior management where gaps are identified;

(h) ensure timely, accurate, and meaningful cybersecurity reporting is prepared for senior management and the Board, covering risk posture, incidents, compliance status, and remediation progress;

(i) promote a consistent and strong cybersecurity culture by supporting institution-wide awareness initiatives, training programs, and accountability mechanisms;

(j) track findings from internal audits, independent assessments, penetration tests, regulatory examinations and any review related to cybersecurity, and monitor the timely remediation of identified issues;

(k) facilitate coordination during major cyber incidents and crises, ensuring alignment across business, technology, communications, legal, and risk functions; and

(l) facilitate financial sector collaboration and information sharing on matters related to cyber threats.

2.4 Chief Information Security Officer

Each financial service provider shall appoint a Chief Information Security Officer (CISO) who shall ensure that cybersecurity policies and procedures are adhered to and incidents are dealt with on time. At a minimum, CISO shall:

(a) serve as the secretariat of the Cybersecurity Steering Committee;

(b) put in place the necessary security controls and processes to minimize cybersecurity-related risks;

(c) ensure any potential cyber threats detected are effectively communicated to the Chief Executive Officer;

(d) monitor all IT platforms and enforce full adherence to strict cybersecurity standards;

(e) develop policies, procedures, standards and plans related to cybersecurity within the organization; and

(f) conduct frequent cybersecurity awareness training for all staff at least once a year.

2.5 Risk Management Function

Risk management shall comprise risk and compliance oversight functions, which ultimately ensure that the management of data, processes, risks, and controls of a financial service provider is operating effectively. Risk management function has the duty to ensure that cyber risks are integrated into the enterprise risk management framework. Specifically, risk management function shall;

(a) establish a comprehensive risk management framework for the identification, measurement, control, and monitoring of cyber risks.

(b) independently evaluate all the risks proactively relating to cybersecurity and report to Senior Management and Board; and

(c) maintain a cybersecurity risk register and treatment plan.

PART III

CYBERSECURITY TECHNICAL AND OPERATIONAL CONTROLS

3.1 Information Assets Management

Every financial service provider shall establish and maintain an asset management process that supports a single, accurate, and up-to-date asset register providing a comprehensive overview of all information assets, including their physical or logical location and other relevant attributes.

(a) Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained;

(b) Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification;

(c) An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization;

(d) Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization;

(e) All employees and external party users shall return all the organizational assets in their possession upon termination of their employment, contract or agreement; and

(f) Information assets shall be disposed of securely when no longer required, using formal procedures.

3.2 Identifying People and Roles

Everyone with access to an organization's systems or facilities, including employees, temporary staff, contractors, and visitors must have their identity, role, and authorized working hours documented. This applies to both physical and digital access. All of this information must be regularly reviewed and updated to ensure accuracy.

3.3 Identifying Business Processes and Activities

A regulated entity must have a clear understanding of its business, including its objectives, activities, and external stakeholders. It also needs to recognize its place within the broader supply chain and its influence within Tanzania's banking sector.

The entity shall maintain a comprehensive inventory of all its business processes. This inventory shall detail:

(a) Core and supportive processes and their associated activities;

(b) Dependencies between different processes;

(c) The IT assets that enable each business process; and

(d) A plan for the continuous and regular review and update of this inventory.

3.4 Asset Retention

3.4.1 Record retention involves retaining and maintaining important information as long as it is needed and destroying it when it is no longer needed. A regulated entity’s security policy typically shall identify retention timeframes according to applicable laws and regulations that dictate the length of time that an organization shall retain data.

3.4.2 The entity shall have the responsibility of identifying laws and regulations that apply and complying with them. However, even in the absence of external requirements, an entity shall still identify how long to retain data.

3.5 Human Capital Security

3.5.1 Employees play a dual role in the institution’s cybersecurity posture. While their access to systems and information assets may introduce insider risks, they also serve as a critical line of defense against cyber threats. Accordingly, a financial service provider shall implement risk-based controls throughout the employee lifecycle to mitigate potential insider threats and foster a strong culture of information security. At a minimum, a financial service provider shall:

(a) conduct background verification checks on all candidates before employment and on an ongoing basis, taking into consideration applicable legal and regulatory requirements;

(b) ensure that the terms and conditions of employment stipulate employees' responsibilities for information security;

(c) establish a formal disciplinary framework to address breaches of the information security policy by the Board, senior management, or other staff, ensuring that violations are dealt with consistently, transparently, and in accordance with the institution's governance and regulatory requirements; and

(d) assign information security responsibilities and ensure that post-employment obligations, including confidentiality and non-disclosure requirements, are defined, documented, communicated, and enforced for all personnel and relevant parties.

3.6 User Management and Access Control

3.6.1 Identity Management

Every financial service provider shall establish a mechanism for identification of individuals and systems accessing the institution's information systems and enable appropriate assignment of access rights. Specifically, the financial service provider shall:

(a) establish and maintain procedures for user registration and de-registration to ensure that access rights are granted, modified, and revoked in a timely and controlled manner;

(b) ensure the allocation and use of privileged access rights are restricted and controlled;

(c) ensure all users are uniquely identifiable and managed in line with least privilege and need-to-know principles;

(d) ensure user management activities (registration, modification and de-registration) are logged, monitored, and auditable;

(e) ensure user accounts are immediately deactivated upon termination of employment, contract, or engagement; and

(f) ensure that shared, generic, or default accounts are prohibited, unless technically unavoidable (e.g., service accounts), in which case they shall be strictly controlled and monitored.

3.6.2 Authentication

Financial service providers shall establish, implement, and maintain strong authentication controls to ensure that access to information systems, applications, and services is granted only to authorized users. At minimum, financial service providers shall:

(a) implement robust authentication mechanisms incorporating secure and standardized authentication protocols;

(b) implement multi-factor authentication (MFA) for all privileged user accounts, remote access, high-risk transactions, and customer-facing applications;

(c) design systems and applications with effective session management controls, ensuring that session identifiers, tokens, or tickets are issued only after successful authentication, are unique and unpredictable, and are validated for every access request;

(d) ensure passwords meet minimum complexity requirements, including length and a combination of characters (e.g., uppercase, lowercase, numbers, and special characters);

(e) enforce technical controls to protect stored passwords, including encryption and hashing;

(f) enforce password change requirements for information systems at regular, predefined intervals, in accordance with established security policies; and

(g) not log passwords; instead, they shall log authentication events only, such as success, failure, timestamp, and source address.

3.6.3 Access Rights Review

Every financial service provider shall implement access control frameworks based on Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC), aligned with defined business roles and responsibilities. Such frameworks shall enforce segregation of duties, apply zero-trust principles for access to critical systems, and ensure secure remote and mobile access through multi-factor authentication.

Privileged accounts shall be managed through appropriate privileged access management controls, with all access activities logged, securely stored, integrated with security monitoring systems, and subject to regular review, while user access rights shall be provisioned, reviewed, modified, and revoked in accordance with established access control policies.

3.7 Data Protection

Every financial service provider shall establish and maintain a data protection policy in compliance with applicable laws and regulations, including the Personal Data Protection Act, 2022. The policy shall address, at a minimum, data classification and handling, confidentiality, integrity and authenticity, data minimization and purpose limitation, access control, data masking and anonymization, data sharing and transfer, and data retention and disposal.

3.8 Vulnerability Management and Penetration Testing

3.8.1 Vulnerability Management

Financial service providers shall establish and maintain a formal vulnerability management program covering the full vulnerability lifecycle, from identification and assessment to prioritization, remediation, and validation. The program shall include regular risk-based vulnerability assessments conducted at least on a quarterly basis, monitoring of trusted threat intelligence sources, documentation and tracking of remediation actions, and periodic reporting to the Board and Senior Management on the effectiveness of the program and residual risks.

3.8.2 Penetration Testing

3.8.2.1 Every financial service provider shall conduct penetration testing on all mission-critical applications periodically, at least annually, in a manner that prevents service disruptions and data loss. The testing shall be performed by an accredited and independent firm licensed by the Tanzania Communications Regulatory Authority (TCRA) in accordance with applicable laws and regulations. The scope of testing shall be defined based on the criticality and sensitivity of the systems, prior vulnerability assessments, regulatory requirements, and industry best practices.

38.2.2 Penetration tests shall evaluate system resilience against technical and physical attacks, including social engineering techniques, and shall reflect real-world adversarial tactics, techniques, and procedures. All findings shall be properly documented, reported, and managed in accordance with the entity’s risk management framework.

3.9 Information Systems Security Management

3.9.1 Every financial service provider shall implement security controls covering, at a minimum, bring-your-own-device policies, servers, databases, networks, endpoints, storage, email, internet, and applications. All systems and applications shall be hardened in accordance with vendor recommendations and industry-recognized standards, ensuring installation of approved and up-to-date software, minimal functionality deployment, protection of data, and enforcement of least-privilege access and need-to-know principles.

3.9.2 Every financial service provider shall ensure secure authentication and session management, deploy protections against malware and other advanced threats, maintain comprehensive logging and monitoring of system activity, and synchronize system clocks to preserve log integrity. Compliance with approved security configuration standards shall be verified through testing, validation, and periodic review, including prior to deployment of new technologies.

3.10 Virtual Meetings and Video Conferencing

Every financial service provider shall ensure that access to virtual meetings and video conferences is granted strictly to the intended participants. Information shared during such meetings shall be adequately secured, and measures shall be implemented to prevent inadvertent disclosure to unauthorized individuals..

3.11 Clock Synchronization

Financial service providers’ information processing systems shall be synchronized to approved time sources.

3.12 Logging and Monitoring

(a) The financial service providers shall implement a centralized log management system to collect events from multiple sources (servers, network devices, OS, databases, applications, etc.) in a single repository;

(b) The clocks of all log sources shall be synchronized to a single reference time source for accurate timeline correlation and analysis;

(c) The financial service providers shall use correlation across multiple event sources during analysis to improve the detection of incidents;

(d) The system event logging shall be integrated with the Security Information and Event Management (SIEM) system for in-depth analysis;

(e) Privileged and normal users' activities shall be logged, produced, kept, and regularly reviewed;

(f) Multiple log servers may be deployed to ensure log collection is not interrupted in case of a single node failure;

(g) Logging facilities and log information shall be protected against tampering and unauthorized access;

(h) Log data shall be archived and retained according to the financial service provider’s log retention policy;

(i) financial service provider shall establish a comprehensive monitoring and detection process that enables the identification of anomalies, malicious activities, and security events across networks, systems, and applications; and

(j) financial service providers shall periodically review, test and update monitoring and detection controls to reflect emerging threats, evolving adversary tactics, and lessons learned from incidents.

3.13 Cryptography

Financial service providers shall develop secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

Financial service providers shall establish and maintain a Cryptography Policy that is documented, approved, implemented, periodically reviewed, and updated in line with emerging threats, industry standards, and regulatory requirements;

(a) Only strong, industry-accepted cryptographic algorithms and key lengths shall be used to protect the confidentiality, integrity, and authenticity of information.

(b) Cryptographic key management shall be governed by a secure formal process and mechanism that covers the entire key lifecycle, including generation, distribution, storage, rotation, usage, archival, and destruction.

(c) Cryptographic operations and key management activities must be logged, monitored, and auditable, ensuring accountability and detection of misuse.

(d) Where feasible, digital certificates issued by trusted Certificate Authorities (CAs) shall be used for authentication, signing, and encryption purposes. Internal PKI deployments shall follow industry best practices for certificate lifecycle management.

3.14 Digital Financial Services

Financial service provider shall implement and maintain robust cybersecurity frameworks to safeguard digital financial services (DFS). Adequate measures shall be taken to ensure the confidentiality, integrity, and availability of all DFS operations, and to mitigate risks arising from cyber threats to ensure the safe and secure provision of Digital Financial Services. At minimum, the financial service provider shall ensure that:

(a) Digital financial services adopt secure coding practices, peer code reviews, and static/dynamic security testing before release;

(b) mobile applications use certificate pinning, encrypted local storage, obfuscation, secure session management and anti-tampering mechanisms;

(c) USSD services incorporate session timeouts, input validation, and encryption at the transport level to prevent misuse; and

(d) applications (mobile apps, USSD, web platforms) follow OWASP security guidelines.

PART IV

GENERAL PROVISIONS

4.1 Monitoring and Reporting

4.1.1. financial service providers shall implement metrics and monitoring processes to assess, report, and ensure the effectiveness and efficiency of their overall cybersecurity program, supporting informed management decisions at all levels.

4.1.2. Every financial service providers shall establish effective and reliable reporting and communication channels to ensure the effectiveness and efficiency of the cybersecurity monitoring;

4.1.3. financial service providers shall submit to the Bank a report on significant cyber-attack incidents that may have an adverse impact on the financial service provider's ability to provide services to its customers or damage its reputation. The report shall be submitted to the Bank within 24 hours through the TZ-FINCERT portal;

4.1.4. financial service providers shall submit a cybersecurity incident report to the Bank for all incidents that occurred during the reporting quarter. The report shall be prepared in the format specified in **Schedule I** made under this guideline and submitted to the Bank within 15 days after the end of each reporting quarter;

4.1.5. financial service providers shall conduct vulnerability assessment on a quarterly basis. The vulnerability assessment report shall be submitted to the Bank within 15 days after the end of each reporting quarter; and

4.1.6. Financial service providers shall conduct independent penetration testing at least annually and submit the test report to the Bank within 30 days of completion.

4.2 Training and Awareness

A financial service provider shall establish and maintain a structured cybersecurity training and awareness program to ensure that senior management and other staff possess knowledge and skills necessary to support cyber resilience. To achieve this objective, the program shall;

(a) ensure continuous awareness and reinforcement of cybersecurity responsibilities by conducting cybersecurity training on a regular basis and at least annually;

(b) promote good IT security practices, provide awareness of common cyber threat types, and communicate the institution’s cybersecurity policies and procedures;

(c) support effective implementation of cybersecurity controls by providing specific training to cybersecurity specialists; and

(d) incorporate periodic review and enhancement processes to ensure its content and delivery remain aligned with changes in the institution’s IT security policies, emerging and prevailing cyber risks, the evolving threat landscape, and outcomes of previous training initiatives.

4.3 Threat Intelligence, Information Sharing and Collaboration

4.3.1. Financial service providers shall establish and maintain a Cyber Threat Intelligence (CTI) process to enhance their ability to understand, anticipate, and defend against emerging and targeted cyber threats.

4.3.2. Financial service providers shall appoint a primary and an alternative focal point of contact to participate in TZ-FINCERT engagements.

4.3.3. Financial service providers shall engage with TZ-FINCERT for the sharing and dissemination of cyber threat intelligence and incidents happening in the institutions.

PART V

ADMINISTRATIVE SANCTIONS

5.1 Sanctions

Without prejudice against the other penalties and actions prescribed by the Act, the Bank may impose one or more of the following sanctions where any of the provisions herein are contravened:

(a) civil penalty on the financial service provider or directors, officers or employees responsible for non-compliance in such amounts as may be determined by the Bank;

(b) suspension of access to the credit facilities of the Bank;

(c) suspension of lending and investment operations;

(d) suspension of capital expenditure;

(e) suspension of the privilege to accept new deposits;

(f) suspension from office of the defaulting director, officer or employee;

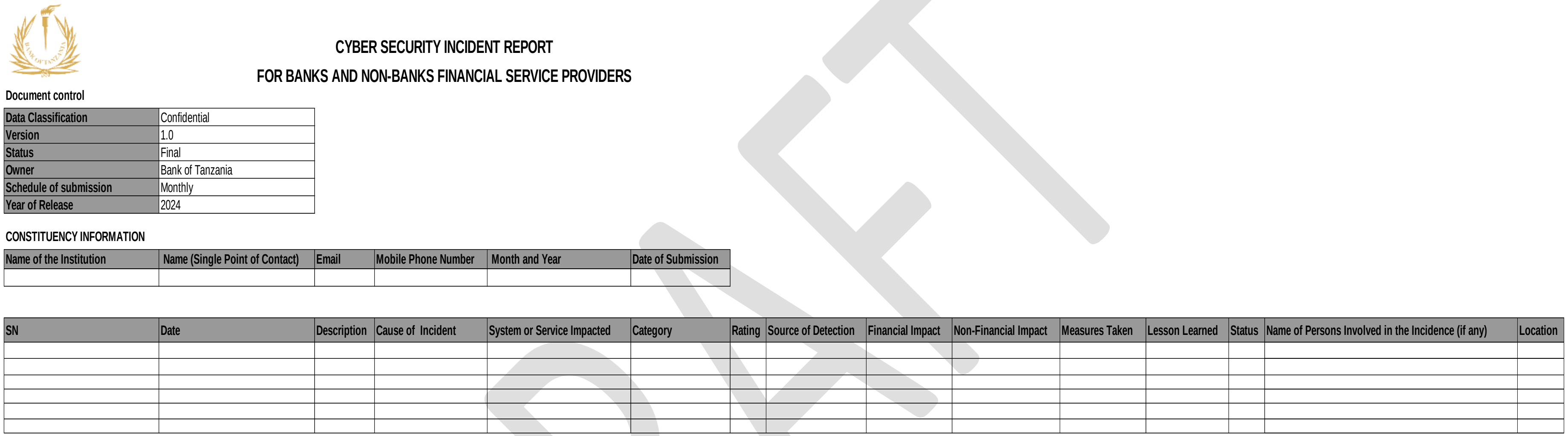
(g) disqualification from holding any position or office in any financial service provider regulated and supervised by the Bank of Tanzania; and

(h) revocation of the license issued by the Bank.

Dodoma,	Emmanuel Mpawe Tutuba
____/____ /2026	Governor

SCHEDULE I

(Made under guideline 5.1.4)



CYBER SECURITY INCIDENT REPORT

FOR BANKS AND NON-BANKS FINANCIAL SERVICE PROVIDERS

Document control

Data Classification	Confidential
Version	1.0
Status	Final
Owner	Bank of Tanzania
Schedule of submission	Monthly
Year of Release	2024

CONSTITUENCY INFORMATION

Name of the Institution	Name (Single Point of Contact)	Email	Mobile Phone Number	Month and Year	Date of Submission

SN	Date	Description	Cause of Incident	System or Service Impacted	Category	Rating	Source of Detection	Financial Impact	Non-Financial Impact	Measures Taken	Lesson Learned	Status	Name of Persons Involved in the Incidence (if any)	Location

(a) Date: The actual date an incident occurred

(b) Description: Provide a short, detailed explanation of the incident

(c) Cause of Incident: How did the incident happen, i.e., known vulnerabilities exploited, security misconfiguration, weakness in controls, etc.

(d) System or Service Impacted: Mention the system(s) or service(s) impacted by the incidence

(e) Category: Unauthorized Access, Unauthorized Use, Unauthorized Modification, Destruction, Denial of Access

(f) Rating:

High:

1. The institution is no longer able to provide some critical services.
2. Sensitive data was accessed and exfiltrated.
3. Data was changed or deleted and cannot be recovered
4. Recovery from the incident is not possible

Medium:

1. The institution has lost the ability to provide a critical service to a subset of the system.
2. Sensitive data was accessed but not exfiltrated.
3. Data was changed or deleted, but can partially be recovered.
4. Time to recovery is unpredictable.

Low:

1. Minimal effect: the institution can still provide all critical services but has lost efficiency.
2. Unclassified Data was accessed or exfiltrated.
3. Data was changed or deleted but can be recovered.
4. Time to recovery is predictable with additional resources.

None:

1. No effect on the institution's ability to provide all services to all users.
2. No information was exfiltrated, changed, deleted, or otherwise compromised.
3. Time to recovery is predictable with existing resources

(g) Source of Detection: IDS/IPS, SIEM, Antivirus, Email Security Gateway, EDR, NDR, Network Flow, Content Web Filtering, File Integrity Monitoring, Operating System Logs, Application Logs, Virtualized Environment Logs, Database Logs, Third Party Monitoring Services, Network device logs, Security Operating Centre, People from within the organization, People from outside the organization, Other(Please specify)

(h) Financial Impact: Mention the category of loss and in bracket associated monetary value in TZS:

A. Direct Loss - Financial loss directly due to cyber criminals' activities

B. Loss of revenue (The amount lost due to the downtime caused by the incident)

C. Penalties or fines (Due to the failure to meet regulatory requirements)

D. Compensation (Amount paid to the third parties due to the failure of meeting contractual or SLA obligations).

(i) Non-financial impact:

A. Corporate objectives- (Failure to achieve corporate objectives)

B. Public image (Loss of reputation to the public)

C. Legal and or compliance- (Exposure to be sued or penalties due to contract entered or regulatory body)

D. Customer Satisfaction (Inability to maintain Customer Satisfaction)

E. Data Breach (Loss of Confidentiality, Integrity, or Availability)

F. Other (Please specify)

(j) Measures Taken: The actions taken to prevent the incident or event from spreading across the network, wipe the threat completely from the services or systems and lastly bring back the systems or services to their former functionality and use.

(k) Lesson Learned: How and why the incident occurred and what can be done to reduce the risk of future incidents. Getting to the root of how and why it happened, evaluating how well your incident response plan worked to resolve the issue, and identifying improvements that need to be made.

(l) Status: Is the incident Closed, Still Open, or Work in Progress

(m) Name of Persons Involved in the Incident (if any): Names and Contact Details of Individual(s) Involved in the Incident

(n) Location: Area where an incident took place, may be at Branch, Head Office, Agency, Third Party