CYBER SECURITY POLICY

Information Security

December| 2022

Version 01

TABLE OF CONTENTS

1| APPROVAL AND DISSEMINATION

	Body	Date
Developed	Directorate of Organization and Quality	24.11.2022
Validated	Executive Committee	29.11.2022
Approved	Board of Directors	22.12.2022
Disseminated	Directorate of Organization and Quality	

2| HISTORY

Version	Title	Changes since last version	Date	Approved
01	Cyber Security Policy	N/A	22.12.2022	Board of Directors

3| INTRODUCTION

3.1| SUMMARY

Information assets play a critical role in the development and sustainability of Banco YETU SA (Bank)'s strategy and business. For this reason it is essential that these assets are protected and safeguarded so that the risk thresholds accepted by the Bank are not exceeded. Banco YETU recognizes that an Information Security incident can cause an interruption in its business operations, compromise its reputation and even have legal, regulatory and financial consequences.

3.2| OBJECTIVES

Banco YETU's Cybersecurity Policy aims to ensure the protection, maintenance of privacy, integrity, availability and confidentiality of information owned and/or under its custody, in addition to preventing, detecting and reducing vulnerability to incidents related to the cyber environment by defining the rules that represent, at a strategic level, the fundamental principles incorporated by the Bank to achieve information security objectives. The Cybersecurity Policy demonstrates Banco YETU's commitment to safeguarding and processing its Customers' information, in order to provide full satisfaction regarding the security and privacy of their information, demonstrating commitment to the Bank's regulatory and strategic aspects, thus being in compliance with the main regulations in force.

3.3| SCOPE

In compliance with legal and regulatory standards and recommendations from the regulatory authority on the need to establish rules on the Cybersecurity component, Banco YETU has implemented a set of controls, including policies, processes, procedures, organizational structures and technologies, in order to ensure the confidentiality, integrity and availability of networks, data and information systems.

All of Banco YETU Customers and Stakeholders must have access to and formal knowledge of the Cybersecurity policy. It is the responsibility of the Directorate of Organization and Quality (DOQ) to ensure the publication and dissemination of the Information Security Policy.

3.4| LEGAL AND REGULATORY FRAMEWORK

The Bank's Cybersecurity Policy is aligned with legal and regulatory provisions, namely:

- Law nº 40/20 – Angolan Payment System Law
- Law nº 14/21 - Law on the General Regime of Financial Institutions
- Notice No. 08/2020 – Cybersecurity Policy and Adoption of Cloud Computing
- Notice No. 12/2016 – Protection of Financial Products and Services Consumers
- Law 22/2011 – Personal Data Protection Law
- Directive 05/DSB/DRO/2022
- ISO/IEC 27001
- ISO/IEC 27005
- ISO/IEC 31000

4| CONCEPTS

For the purposes of this Policy, the following terms shall bear the following meaning:

Information Asset: Asset (physical or digital) that stores, processes or transfers Bank information.

Access: Privileges that a User/Account has to access data, systems, services or infrastructures of the Bank;

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities or processes;

Availability: Property of information being accessible and usable upon request from an authorized entity; Integrity:

Guarantee of consistency, completeness and accuracy of information and respective processing methods, throughout its entire life cycle;

Information Security Risk: Risk of the confidentiality, integrity or availability of an information asset being compromised;

Risk Responsible: person or entity with the responsibility and authority to manage a risk;

Cybersecurity: is a set of actions and techniques created to protect systems, programs, networks and equipment against intrusions.

Cybersecurity Incident: Event or a set of events that compromise or may compromise information and/or information systems, including acts or omissions, whether deliberate or not, that violate the Bank's Information Security policies.

Significant Cybersecurity Incident: Incident that results in non-compliance with legal or regulatory obligations.

Very Significant Cybersecurity Incident: Incident with potential systemic risk for the Angolan financial system.

Service providers: External entity that provides any type of services to support the Bank's activity.

Cybersecurity Event: Occurrence that may have a security significance, i.e. may represent a threat to the confidentiality, integrity and availability of a technological asset.

Vulnerability: Technical failure in an information system that can potentially be exploited with the aim of carrying out unauthorized actions in the information system.

Zero Day Vulnerability: Previously unknown vulnerabilities for which there is no known mitigation measure.

5| RESPONSIBILITIES

5.1| EXECUTIVE COMMITTEE

1. To define and approve the Information Security plan, strategy and objectives;
2. To ensure the necessary resources for the management and operationalization of the Cybersecurity Policy;
3. Sponsor the main initiatives that contribute to achieving the Bank's Information Security goals.
4. To monitor the implementation of the Information Security plan;
5. To identify and propose the resources (people, technologies, infrastructure, financial, etc.) necessary to implement the Information Security plan.
6. To ensure that information security reviews, assessments and tests are carried out to effectively identify vulnerabilities in systems and services.

5.2| SECURITY OFFICE

1. To identify, promote and manage the implementation of Information Security controls, initiatives and projects;
2. To develop and improve internal Information Security policies and regulations;
3. To ensure the correct identification, management and monitoring of the Bank's information security risks;
4. To train and raise awareness among Bank Employees on Information Security topics;
5. To promote Information Security culture within the Bank;
6. To encourage compliance with Information Security guidelines among the Bank's technical teams and business units;
7. Establish regular communication with the Bank's top management, in order to communicate and define remedy plans for identified risks.

5.3| DIRECTORATE OF TECHNOLOGIES AND INFORMATION SYSTEMS

1. To ensure the implementation of Information Security controls, initiatives and technological projects, provided for in the Information Security Plan;
2. To monitor and oversee security operation activities;
3. To ensure the operationalization of activities related to the management of information security incidents;
4. To support the Security Office in promoting Information Security culture at the Bank;
5. To support in the identification, evaluation and implementation of technologies that support the Bank's security objectives.

5.4| DIRECTORATE OF PERSONNEL DEVELOPMENT

1. To support the Security Office in promoting training and awareness initiatives for Bank Employees regarding Information Security;

2. To ensure the enforcement of Information Security requirements relating to the management of the life cycle of the contractual relationship between Employees and the Bank;

3. To report any relevant changes to the contractual relationship with Employees to the Directorate of Technology and Information Systems, as well as participate in the access review process.

5.5| CLIENTS

1. To ensure responsibility for the confidentiality, integrity and availability of the information to which they have access;

2. To ensure the correct use of the Bank's assets during the use of digital services.

6| CONFIDENTIAL INFORMATION

Access to confidential information, including personal data, collected and stored by Banco YETU is restricted to professionals authorized to use this information whenever necessary to provide their services, with use limited to other tasks or purposes, and must also respect the set out in the Information Classification policy.

Banco YETU may, at certain times, have to share personal data with third parties in accordance with the legislation in force in the country.

The entities that may request personal data:

1. General Tax Administration;
2. National Bank of Angola;
3. BODIVA;
4. Capital Markets Commission;
5. Correspondent Banks;
6. Attorney General's Office;
7. Courts;
8. Financial Information Unit.

7| CYBER SECURITY MANAGEMENT STRUCTURE

The management of Cybersecurity controls ensures that operational procedures are developed, implemented or modified in accordance with the objectives established in this Policy.

7.1| INFORMATION ACCESS MANAGEMENT

Access to information is controlled, monitored, restricted to the lowest possible permission and privileges, reviewed periodically, and canceled in a timely manner at the end of the Employee's or service provider's employment contract. Critical or sensitive information processing equipment and facilities are kept in secure areas, with appropriate levels of access control, including protection against physical and environmental threats. YETU Bank Employees must undergo training sessions periodically regarding cyber risks and information security control measures, through an effective awareness program and dissemination of cyber security culture.

7.2| PROTECTION OF THE BANK'S ENVIRONEMENT

Controls and responsibilities are established for the management and operation of information processing resources, with the aim of ensuring security in Banco YETU's technological infrastructure through an effective management model with regard to monitoring and treatment in response to incidents, with the aim of minimizing the risk of failures and safe administration of communications infrastructure and systems.

7.2.1. AUTHENTICATION

Access to information and technological environments at Banco YETU is only permitted to people authorized by the Information Owner, taking into account the principle of least privilege, the segregation of conflicting functions and the classification of information. Access control to systems is formalized and includes, at a minimum, the following controls:

1. The use of identifiers (access credentials) that are individualized, monitored and subject to blocking and restrictions (automated and manual);

2. The removal of authorizations given to Employees who have been removed or terminated from Banco YETU, or who have changed their role;

3. Periodic review of permissions granted

7.2.2| INFORMATION SECURITY INCIDENT MANAGEMENT

The behaviour of possible attacks is identified through detection controls implemented in the environment, such as application filter, malicious behavior detection tool, Antivirus, Anti-spam, Anti-malware, among others.

7.2.3| PREVENTION AGAINST INFORMATION LEAK

Use of control aimed at preventing data loss, responsible for ensuring that confidential data is not lost, stolen, misused or disclosed on social media or other digital channels by unauthorized Employees.

7.2.4| INTRUSION TESTS

Internal and external intrusion tests on the Bank's digital channels (SiteYETU, NetYETU) must be carried out annually.

7.2.5| VULNERABILITIES CHECKS

Checks on internal and external infrastructure must be performed periodically. Identified vulnerabilities must be addressed and prioritized according to their level of criticality.

7.2.6| CONTROL AGAINST MALICIOUS SOFTWARE

All assets (computers, servers, etc.) that are connected to the corporate network or make use of Banco YETU information are compatible and protected with an anti-malware solution determined by the Information Security area.

7.2.7| ENCRYPTION

Every encryption solution used at Banco YETU is parameterized with information security rules and standards.

7.2.8| MONITORING

All Banco YETU systems send their Log files to an event management and correlation platform in order to properly control all traffic generated in its communication infrastructure and systems.

Example of Logs:

1. Employee Authentication (valid and invalid attempts);
2. Access to information;
3. Actions performed by Employees, including creating or removing data in the system.

7.2.9| SAFE SOFTWARE SOLUTIONS

Banco YETU maintains a set of principles to develop systems securely, ensuring that cybersecurity is designed and implemented in the systems development lifecycle.

7.2.10| BACKUP

The backup implementation process is carried out periodically on Banco YETU's information assets, in order to avoid or minimize data loss in the event of incidents.

7.3| BUSINESS CONTINUITY

Banco YETU's business continuity process is designed with the aim of reducing the impacts and losses of information assets after a critical incident to an acceptable level, through the mapping of critical processes, business impact analysis and periodic testing of disaster recovery.

This process includes business continuity related to services contracted in the cloud and tests planned for cyber attack scenarios.

8| MAIN SECURITY RECOMMENDATION FOR CLIENTS

7.1| AUTHENTICATION AND PASSWORD

Clients are responsible for acts carried out using their identifier (login/acronym), which is unique and accompanied by an exclusive password for individual identification/authentication when accessing information and technology resources.

We recommend that they should:

1. Maintain confidentiality, memorize and not record the password anywhere. In other words, they should not tell their passwords to anyone and not to write it down on paper;

2. Change the password whenever there is any suspicion that someone may have seen it;

3. Create quality passwords, so that they are complex and difficult to discover;

4. Prevent the use of your equipment (mobile phone, computer) by other people, while they are using the Bank's digital services with your identification;

5. Always lock the equipment when one is away.

6. Whenever possible, enable a two-factor authentication (For example: SMS, Token, etc.).

7.2| ANTIVIRUS

We recommend that the Customer maintain an up-to-date antivirus solution installed on the computer or other equipment they use to access the services offered by the Bank. It is preferable to always have these devices updated with the latest IOS versions.

7.3| SOCIAL ENGINEERING

Social engineering, in the context of information security, refers to the technique by which one person seeks to persuade another, often abusing the user's naivety or trust, with the aim of deceiving them, applying scams in order to obtain confidential information.

7.3.1| PHISHING

Technique used by cybercriminals to deceive users by sending malicious e-mails in order to obtain personal information such as passwords, credit cards, personal identification numbers, bank account numbers, among others. Phishing email approaches can occur in the following ways:

1. They seek to attract people's attention, whether due to the possibility of obtaining some financial advantage, out of curiosity, or out of charity;

2. They try to pretend to be official notice from well-known institutions such as: Banks, e-Commerce Stores, among other popular websites;

3. They try to trick people into filling out forms with their personal and/or financial data, or even installing malicious software that aims at collecting sensitive information;

7.3.2| SPAM

These are unsolicited emails, which are generally sent to many people, typically containing content for advertising purposes. Furthermore, spam is directly associated with security attacks, being one of the main responsible for the spread of malicious codes, illegal sale of products and dissemination of scams.

7.3.3| FAKE TELEPHONE CONTACTS

These are techniques used by criminals to obtain information such as personal data, passwords, tokens, cell phone identification code (IMEI) or any other type of information to commit fraud.

9| LEGAL COMPLIANCE

9.1| COMPLIANCE WITH LEGAL, REGULATORY AND CONTRACTUAL OBLIGATIONS

1. The Bank must keep a record of legal, regulatory and contractual obligations regarding Information Security and personal data protection.

2. For each legal, regulatory and contractual obligation in matters of Information Security and personal data protection, the area of Banco YETU responsible for ensuring compliance must be mapped.

3. Whenever applicable, Banco YETU's Information Security Policy, as well as Information Security operational processes, must be adjusted to ensure compliance with new legal, regulatory and contractual obligations of Banco YETU in matters of Information Security.

9.2| INTELLECTUAL PROPERTY RIGHTS AND LICENSING

1. Banco YETU has procedures for using licensed Software, thus respecting the intellectual property rights of the software installed in information systems to support the Bank's business activities.

2. Reproduction/copying of software licensed at the Bank, or installation of this type of software, is not permitted without validation and authorization by the Executive Committee.

9.3| DATA RETENTION

1. The Bank needs to maintain a record of data retention periods in order to comply with legal, regulatory, contractual and business obligations.

2. To prevent an excess of information that is not useful to the Bank, it is necessary to implement data purge mechanisms to ensure that data is eliminated, in a secure manner, whenever the maximum defined deadlines are reached, whether the data are resident on physical media (e.g. paper) or digital media (e.g. databases, files, backups).

10| FINAL PROVISION

1. The Executive Committee has the right to investigate possible non-compliance with the requirements of this Policy and the Standards that support it;

2. Any Employee who uses Banco YETU's information assets in an improper or unauthorized manner is subject to the penalties provided for in the Bank's internal regulations and applicable legislation;

3. Failure to comply with the provisions contained in the Information Security Policy and procedures constitutes a functional infraction, to be investigated in an administrative disciplinary case, without prejudice to criminal and civil liabilities;

4. All authorized exceptions are identified and recorded, so that such situations are included in the next review of the Information Security Policy or are formalized as exceptions.

5. The Cybersecurity Policy is reviewed whenever justified, due to the occurrence of significant changes in applicable legislation and regulation, the Bank's business strategy and/or risk profile.

6. All changes to the Cybersecurity Policy are approved by the Bank's Board of Directors, with the new version published and disseminated to all Bank Employees and other external entities involved in the Bank's activities with access to the Bank's information.

--//--

This Policy comes into effect immediately.

Luanda, on 22nd December 2022.

_____

Abrahão Pio dos Santos Gourgel
Chairperson of the Board of Directors
Banco YETU, S.A

.