IT and Anti-Cybercrime Policy for Kukumbi

i. Introduction and Background

Kukumbi – is a non-profit non-governmental organization founded in 1998, based in Quelimane city, Zambézia province, has a long-standing history of managing large-scale, multi-sectoral development and Humanitarian programs. Kukumbi's focus includes OVC, AGYW, Educação, Saúde, SBCC, WaSH and nutrition, livelihood, Climate Change Resilience, Biodiversity.

During this period Kukumbi have been able to implement several programs aiming to contribute towards strengthening vulnerable communities through their engagement in the process of local sustainable development and lobby and advocacy. Published its Statutes in the Bulletin of the Republic of Mozambique III SERIES Nr. 54 on July 8, 2014 registered with the Ministry of Justice of Mozambique under Nr.100160625.

VISION: See improved the wellbeing of the citizens of the central of Mozambique where their rights are not respected.

MISSION: To improve organizations and participation of Communities and Civil Society Organizations to demand their right in development processes that enhances their wellbeing.

Kukumbi's **IT and Anti-Cybercrime Policy**, enforces compliance with USAID and Non-USAID regulations, while focusing to ensure compliance with cybersecurity standards and supports the organization's operational efficiency on capacity building, financial management, and fraud prevention.

Acronyms

- **USAID**: United States Agency for International Development
- IT: Information Technology
- **M&E:** Monitoring and Evaluation
- **HR:** Human Resource
- **GDPR**: General data Protection Regulation
- **PGP :** Pretty Good Privacy
- **SEO:** Search Engine Optimization

IT and Anti-Cybercrime Policy Overview

It aims to ensure compliance with cybersecurity standards and supports the organization's operational efficiency. The implementation of access controls, encryption protocols, data management practices, and monitoring systems will provide a robust defines against cyber threats while improving Kukumbi' s capacity for data-driven decision-making and reporting.

Through the integration of cybersecurity measures, Kukumbi aims to promote transparency and operational excellence while maintaining the integrity of sensitive data, especially with regards to key operational databases, which tracks critical program information. Additionally, the policy includes guidelines for promoting Kukumbi' s work and projects through social media, and website as well as the implementation of systems to manage individual staff access to digital tools through electronic timesheets and leave management.

Thus, the policy seeks to ensure that everyone is aware of their responsibilities and commitments regarding information security, as well as providing guidance on how to protect Kukumbi's assets and data.

1. Objective

The **IT and Anti-Cybercrime Policy** is designed to protect Kukumbi's digital infrastructure, data, and sensitive information from unauthorized access, cyberattacks, and other threats.

The policy establishes security protocols for both internal staff and external partners, safeguarding the organization's IT systems. It ensures that internal strong controls are in place for access management, data encryption, secure communication, and compliance with international standards, such as ISO/IEC 27001 and GDPR.

2. Scope

This policy applies to all Kukumbi employees, volunteers, consultants, sub-recipients, and contractors who use Kukumbi' s IT resources, including computers, mobile devices, software, and data storage systems. It covers all digital activities and ensures the protection of Kukumbi' s assets across all operational levels, including cloud-based storage, email communication, data entry into management information systems (MIS), and digital interactions on behalf of the organization. The policy extends to all data management tools, including the **database**, which plays a critical role in tracking beneficiaries and ensuring compliance with donor reporting requirements.

3. IT Security

3.1. Access Control

The IT Department will implement **role-based access control (RBAC)** across all Kukumbi systems, ensuring that only authorized personnel can access sensitive data. Regular bi-annual

reviews will be conducted by the IT Department and HR to ensure that user access remains aligned with current job responsibilities. Additionally, **multi-factor authentication (MFA)** will be mandatory for all users accessing critical systems, ensuring that login activities are monitored for suspicious behaviour.

All information generated or acquired by Kukumbi, represents Kukumbi's property, regardless of how it is presented or stored. This means that the organization owns the rights over the information and its management considers donors' standards and regulations.

Kukumbi's resources and information should be used only for organization-related activities and that all, including employees, partners, and third parties, must follow internal standards when using these technological resources and information. The goal is to ensure that everything is used in compliance with organization and USAID and Non USAID funding partners' policy guidelines

3.2. Data Encryption

Kukumbi's IT Department will enforce **AES-256 encryption** for all sensitive data, both in transit and at rest, . Secure messaging systems, such as **PGP encryption**, will be used to ensure the confidentiality of email communications related to financial and beneficiary data. Automated encryption protocols will be in place for all external communications linked to donor reporting and sensitive program data, ensuring compliance with international cybersecurity standards.

Kukumbi's IT Department will implement AES-256 cryptography (in Compliance with International Standards of Cyber Security) for all sensitive data, both in transit and safely, including those stored in the benefits system.

For email communications related to financial data and benefits data system, PGP cryptography (Pretty Good Privacy) will be used. PGP guarantees the privacy of messages by means of encryption, allowing only authorized recipients to access communications content and ensuring that data integrity be preserved.

In addition, automated encryption protocols will be used for all external communications involving reports for donors and sensitive data program. These protocols ensure that all data exchanged with external parties are crypto graphed according to international cybersecurity standards.

These measures guarantee compliance with international data protection and cybersecurity standards, strengthening the protection of Kukumbi's sensitive data from possible threats and leaks, and ensuring that the organization maintains high standards of security and privacy

3.3. Backup Systems

The IT Department will implement **daily automated backups** for all financial, HR, and donor data. Quarterly tests of the backup systems will be conducted to ensure data recovery capabilities. Additionally, the IT Department will maintain an up-to-date **disaster recovery plan** and perform bi-annual recovery drills to guarantee that data can be restored efficiently in the event of a system failure. Backup systems will be compliant with international security standards, including ISO/IEC 27001.

The IT Department will implement automated daily backups for all financial, human resources, and financing partner data, with specific focus on data protection within the benefits system. These backups ensure that all critical information is regularly copied and stored securely.

In addition, quarterly testing of the backup systems will be conducted to verify data recovery capacity by ensuring that the data restoration will work properly when necessary.

Thus, to strengthen disaster preparation, the IT Department will maintain a recovery plan and hold recovery simulations every six months. These exercises will ensure efficient data restoration in case of system failure.

Backup systems conforms to international security standards, including ISO/IEC 27001, ensuring that backup and recovery practices meet international data protection and information security standards.

4. Cybercrime Prevention

4.1. Cybersecurity Awareness Training

Kukumbi' s IT and HR Departments will coordinate Quarterly cybersecurity awareness training, with a focus on emerging threats such as phishing, ransomware, and secure password management. Custom IT training sessions will also be provided to sub-recipients, ensuring their systems meet Kukumbi' s security standards. Training effectiveness will be assessed through simulated phishing attacks and system security tests.

4.2. Use of Emails

- **Exclusive use for corporate purposes:** Corporate email should be used for work and institution related activities only.
- **Prohibition of non-Corporate use:** It is forbidden to use corporate emails to desk at external sites not related to the organization such as blogs, forums, games and social media.
- **Required Communications:** All communication with partners, vendors, clients or tenders should be done exclusively through corporate emails.
- **Prohibition of access to Personal Emails:** It is forbidden to access personal emails using webmail's or other tools, even if protective policies do not block that access.
- **Monitoring Right:** The organization has the right to track, monitor, record, and inspect all information transmitted via corporate email.

4.3. Use of Internet

- **Exclusive use for Corporate purposes:** Corporate internet should be used for organization-related activities, intellectual enrichment, and search for information that contributes to the development of activities.
- **Personal use with Limitations**: Personal use of the internet, such as home banking and virtual stores, is allowed, but must be done with common sense and in compliance with corporate policies.
- **Prohibition of Improper Sites**: Access to improper sites is prohibited. This includes sites with illicit content, and obscene.

- **Blockage:** Internet usage is monitored by identification of the user, and access can be blocked at any time by the IT department if any risk or irregularity is identified.

4.4. Use of Social Midias

All matters related to external communication and social media must be managed by the areas of marketing, communication or other areas formally authorized by the organization. This ensures a coordinated and controlled approach to external communication.

4.5. Use of Corporate Computer Equipment

Corporate Resources should be used exclusively for organization activities and responsibility. Failure to comply can result in administrative sanctions.

- **Administration Control**: Users should not have administrator permissions on their machines, unless properly justified and documented exceptions.
- **Software:** Installation or running of unlicensed or unprovided software is prohibited. Only software authorized by the organization can be used. Kukumbi will ensure the acquisition and use of antivirus in establishments such as McCafee and Kaspersky for USAID and Non-USAID programs/projects
- **Operational System image**: The image of operational systems must be standardized, approved by the IT Department and updated with the latest security updates.
- **Maintenance and Configuration**: Only IT Department can carry out maintenance and configurations on corporate computers. Unauthorized changes are prohibited.
- **Report Incidents:** Any incident involving corporate machines such as viruses or attacks should be reported to the IT Department immediately.

4.6. Use of the Corporate Network

- **Digital Certificate:** All machines that access the corporate network must have a digital certificate to ensure safety and authenticity.
- **Remote Connections:** Using external remote connections in connected equipment to the corporate network is prohibited to prevent risk exposure and virus contamination.
- **Network Expansion:** It is not allowed to expand the corporate network with routers, switches or hubs without permission From the Department of Informatics.
- **Suppliers and Visitors:** They must use their own connections to access the Internet or segregated networks (such as the visitor network) to avoid risks to the corporate network.

4.7. Use of Landline Phone

The use of the landline phone in Kukumbi should be for professional purposes. Use for personal purposes with good-sense is allowed, for matters that are not conflicting with the organization's activities nor to impair any law, regulation or and internal policies of the organization.

4.8. Security Access

- **Responsibility for Accesses**: Each employee is responsible for any acts performed with their own accesses, whether physical (such as access to restricted areas) or log (such as logging in systems and applications).
- **Responsibility for the Workstation:** Each employee is responsible for any actions taken at your workstation while logged in. This means that any activity performed under your access identity is your responsibility.
- **Single and Intransferable access**: Each employee must maintain the confidentiality and integrity of their own accesses.
- **Password Management and Configuration:** Kukumbi establishes detailed guidelines and controls on password management and configuration. There are practices and requirements for the creation, maintenance and protection of passwords. Passwords will be updated quarterly and for their creation, combinations of strong passwords are used not exceeding eight to characters including a combination of uppercase, lowercase and special letters , configured according to the term of the employee's contract duration, thus making the information management system robust.

4.9. Firewalls and Antivirus Software

The IT Department will maintain enterprise-grade **firewalls** and **antivirus software** to protect Kukumbi' s network perimeter **database** from unauthorized access. Weekly system scans using anti-malware tools will be performed, and **Intrusion Detection System (IDS)** logs will be reviewed regularly for unusual activity.

4.10. Incident Response Plan

The IT Department will monitor all network traffic in real-time, using IDS to detect and respond to cyber threats. In the event of a security incident, the IT Department will conduct post-incident forensic investigations and submit detailed reports to senior management. A comprehensive **incident response log** will be maintained, including all breaches and corrective actions taken, with specific focus on securing sensitive data within the **system**.

5. MIS Management and Updates for Database

5.1. Database Management

Kukumbi's **database** plays a critical role in managing beneficiaries' data, tracking services, and reporting key outcomes. The M&E Team, in collaboration with the IT Department, will be responsible for the ongoing management, updates, and security of the database.

Key activities include:

- **System Updates**: The IT Department will ensure the **database** is regularly updated with software patches and security features. Quarterly reviews will identify vulnerabilities, and any required updates will be implemented promptly.
- **Data Quality Audits**: The M&E Team will conduct regular data quality audits to ensure that entries in the **system** are accurate and comply with reporting standards.

- **Access Control**: Role-based access controls will be applied to ensure only authorized personnel can access sensitive beneficiary data. The IT Department will review access permissions every three months.
- **Training**: Ongoing MIS training will be provided to staff responsible for data entry into the **system**, ensuring they are knowledgeable about secure data entry and management protocols.

6. Monitoring and Evaluation

6.1. Regular IT Audits

Quarterly IT security audits will be performed by the IT Department, focusing on password policies, access controls, and system configurations. Additionally, annual **penetration tests** will be commissioned to simulate cyberattacks and assess the security of all Kukumbi systems, particularly the **database**. All findings from these audits will be documented, and any vulnerabilities will be addressed within 30 days.

6.2. MIS Review for beneficiary

The M&E Team, with support from the IT Department, will perform quarterly reviews of the **system**, ensuring data integrity and compliance with donor reporting requirements. Technical issues or data discrepancies will be identified and resolved in a timely manner, with regular reports submitted to senior management for review.

7. Compliance and Reporting

7.1. Compliance with Cybersecurity Standards

Kukumbi' s cybersecurity policies, including those governing the **system**, will align with international standards such as **ISO/IEC 27001** and **GDPR**. Annual reviews will be conducted by the IT Department to ensure ongoing compliance with these standards, particularly in relation to the secure handling and storage of sensitive programmatic and administrative data.

This policy is a dynamic document thus, reviews and updates will be performed by the IT Department annually, or within a lower term, in terms of legal/regulatory changes or if Kukumbi view necessary in order to incorporate measures related to new or previously activities and procedures not addressed. takes effect from the date of its approval and must be interpreted in consonance with the other hands and policy of Kukumbi.

7.2. IT Assets Management

IT asset management and establishes the following guidelines:

- **Identification and Inventory:** All assets that contain corporate information must be identified and inventoried. This includes any resource that store, process or transmit information from the organization.
- **Designation of Manager (Owner**): For each asset, an owner should be designated regardless of its type (system, server, database, etc.). This manager (owner) should ensure proper asset protection based on the degree of risk and ensure that accesses are properly approved.

7.3. Incident Reporting

In the event of a data breach or cyberattack involving the beneficiary **database** or other sensitive systems, the IT Department will notify donors (e.g. USAID and Non-USAID) and affected stakeholders within 72 hours. Detailed logs of all incidents will be maintained, documenting the timeline, responses, and corrective measures taken.

8. Social Media Promotion and Website Updates

8.1. Social Media Promotion

Kukumbi will actively promote its work, including USAID and Non USAID-funded program/projects, through social media channels such as Facebook,, LinkedIn, and Instagram. The Communications Team will develop quarterly campaigns to highlight program/project milestones, impact stories, and key outcomes.

8.2. Website Updates (Social Media Plataform)

The IT Department, in collaboration with the Communications Team, will regularly update Kukumbi' s website, Youtube, Facebook and Instagram to reflect its achievements and ongoing program/projects, including the **beneficiary System**. SEO strategies will be implemented to improve visibility, and a dedicated page will showcase Kukumbi' s partnership with USAID and Non-USAID and other stakeholders.

Activity Table: IT and Anti-Cybercrime Policy

Activity	Details	Responsible Party
Network Security Devices (Firewalls, IDS)	• Purchase and install firewalls and IDS. • Monitor the network for unusual activity. • Conduct weekly reviews of IDS logs.	IT Department
Backup Systems (On-Site and Cloud-Based)	• Set up automated weekly backups. • Perform quarterly drills for data recovery. • Ensure cloud storage complies with international standards.	IT Department
Data Encryption and Secure Communications	• Implement encryption tools (AES-256, PGP) • Monitor communications for compliance with encryption protocols. • Conduct encryption audits quarterly.	IT Department
Multi-Factor Authentication (MFA)	• Implement MFA system across all critical systems. • Train staff and partners on MFA usage. • Monitor MFA system for suspicious login attempts.	IT Department
Cybersecurity Awareness Training	• Develop training content focusing on phishing, password management, and ransomware. • Organize annual training sessions. • Test staff with phishing simulations after training.	IT Department, HR Department
Penetration Testing	• Commission third-party penetration tests annually. • Document findings and patch vulnerabilities within 30 days. • Ensure all systems comply with international cybersecurity standards.	IT Department, External Cybersecurity Firm
Anti-Malware and Anti-Virus Software	• Purchase and configure enterprise-grade antivirus software. • Set daily scans and automated updates. • Monitor malware activity logs weekly.	IT Department
Electronic Timesheet and Leave Management System	• Set up and link timesheet and leave management systems to employee emails • Ensure system prohibits the use of personal accounts for work-related purposes.	IT Department, HR Department

Activity	Details	Responsible Party
	• Provide regular maintenance and updates.	
Internet Usage Monitoring	• Implement tools to monitor internet usage • Block access to suspicious or harmful websites (terrorist-linked sites, etc.). • Generate usage reports for management review.	IT Department
Social Media Promotion and Website Update	• Regularly update the website to reflect Kukumbi' s programs/projects and achievements. • Implement SEO strategies for better visibility. • Coordinate social media campaigns highlighting Kukumbi and USAID and Non USAID programs/ projects.	Communications Team, IT Department
MIS (beneficiary Database) Management	• Perform regular system updates and security reviews for the **beneficiary** database. • Conduct quarterly data quality audits to ensure accuracy of **beneficiary** entries. • Provide ongoing training for staff responsible for **beneficiary** data entry and management. - Ensure role-based access to sensitive data, with bi-annual access reviews.	M&E Team, IT Department

Kukumbi' s IT and Anti-Cybercrime Policy Budget

Activity	Cost Components	Estimated Cost
Network Security Devices (Firewalls, IDS)	• Purchase and installation of enterprise-grade firewalls • IDS setup and configuration • Ongoing monitoring and maintenance	$10,000 setup + $3,000 annually for monitoring and maintenance
Backup Systems (On-Site and Cloud-Based)	• Cloud storage subscription fees • On-site backup system purchase • Data recovery testing (quarterly drills)	$1,200 annually
Data Encryption and Secure Communications	• Encryption software (e.g., PGP) • Secure email platform • Regular encryption audits	$2,000 setup + $1,500 annually
Multi-Factor Authentication (MFA)	• MFA software subscription • User setup and training • Ongoing monitoring and maintenance	$1,000 annually

Activity	Cost Components	Estimated Cost
Cybersecurity Awareness Training	• Training materials • Trainer fees (internal/external) • Testing (phishing simulations)	$5,000 annually
Penetration Testing	• External cybersecurity firm for annual penetration tests • Vulnerability patching costs based on findings	$1,000 annually
Anti-Malware and Anti-Virus Software	• Purchase/subscription for enterprise-grade anti-malware and antivirus software • Regular updates and maintenance	$1,500 annually
Electronic Timesheet and Leave Management System	• System setup and linking with employee email accounts • Maintenance and training costs	$2,000 setup + $1,000 annually
Internet Usage Monitoring	• Implementation of internet monitoring tools • Report generation and system maintenance	$500 setup + $200 annually
Social Media Promotion and Website Update	• Social media campaign management fees (e.g. Male mobilisation campaign on self-testing) • Website design updates • SEO tools and content creation	$3,000 annually
MIS beneficiary Database) Management	• Training sessions for beneficiary data entry staff • Data quality audits and role-based access reviews	$ 3,0000 annually