CENTRE FOR ENVIRONMENT AND MIGRATION ASSISTANCE (CEMA)

Asset Management Policy

May 2024

TABLE OF CONTENT

1. Purpose

This Asset Management Policy provides a structured framework for the effective and responsible acquisition, utilization, maintenance, safeguarding, and disposal of assets owned or controlled by the Centre for Environment and Migration Assistance (CEMA). The purpose of this policy is to ensure that all assets—whether purchased, leased, or donated—are managed in a manner that upholds the organization's core values of transparency, accountability, efficiency, and sustainability.

This policy aims to:

- **Promote accountability and stewardship** by assigning clear responsibilities for asset custody, usage, and tracking to designated staff and departments.
- **Safeguard CEMA's physical and intangible resources** from loss, theft, damage, or misuse through the implementation of effective control measures and regular monitoring.
- **Support informed decision-making** regarding asset procurement, deployment, and disposal through accurate and up-to-date asset records.
- **Ensure value for money and operational efficiency** by optimizing the lifespan and performance of assets through regular maintenance and appropriate usage.
- **Comply with applicable laws and regulations** in Uganda, including financial reporting standards, tax requirements, and relevant government policies.
- **Align with donor expectations and contractual obligations** related to the ownership, visibility, and reporting of project-funded assets.
- **Facilitate internal and external audits** through the provision of a comprehensive and verifiable asset register.
- **Contribute to long-term organizational sustainability** by integrating asset management into CEMA's broader strategic and financial planning.

Ultimately, the policy reinforces CEMA's commitment to effective resource management as a foundation for delivering quality services to the communities we serve, enhancing operational integrity, and strengthening stakeholder trust.

2. Scope

This Asset Management Policy applies to all tangible and intangible assets owned, leased, or controlled by the Centre for Environment and Migration Assistance (CEMA), regardless of the source of funding or method of acquisition. It covers assets used across all CEMA offices, project locations, field operations, and partner sites within Uganda and in any other locations where CEMA operates or may operate in the future.

The policy is binding on all staff, volunteers, consultants, and third parties entrusted with the use or care of organizational assets. It establishes uniform guidelines and procedures for managing assets throughout their lifecycle—from acquisition and registration to usage, maintenance, and eventual disposal.

The scope of this policy includes but is not limited to:

- **Furniture and Equipment:** Office desks, chairs, cabinets, shelves, and related fixtures used in administrative or field offices.
- **Vehicles and Motorcycles:** All forms of organizational transport used for fieldwork, staff mobility, project delivery, or logistics, including those procured through donor funds or transferred from partner organizations.
- **ICT Equipment:** Computers, laptops, tablets, mobile phones, printers, scanners, projectors, and network infrastructure.
- **Buildings and Land:** Office buildings, storage units, warehouses, training centers, and any land parcels acquired, leased, or donated for use by CEMA.
- **Software Licenses and Digital Assets:** Licensed software, proprietary digital tools, cloud-based systems, databases, digital content, and other non-physical resources used to support operations or deliver digital services.
- **Leased or Donated Assets:** Any assets provided to CEMA under lease agreements, donations, or grants, whether temporarily or permanently, with associated conditions or agreements.

The policy also encompasses:

- Assets acquired through partnerships, joint ventures, or consortium arrangements.
- Project-specific assets purchased under donor-funded agreements, which may carry specific management and reporting obligations.
- Disposed or written-off assets, ensuring proper documentation and accountability at the end of the asset life cycle.

---

3. Objectives

The primary objectives of this Asset Management Policy are to establish a comprehensive and systematic approach to managing all organizational assets in a manner that enhances efficiency, transparency, and sustainability across CEMA's operations. These objectives are integral to strengthening institutional governance, fulfilling donor obligations, and maximizing the value of resources entrusted to the organization.

Specifically, the policy aims to:

- **Ensure Accurate Recording and Tracking of Assets:**
  Establish and maintain an up-to-date Asset Register that captures essential details such as asset type, location, custodian, condition, depreciation, and value. This enables CEMA to maintain a complete and reliable inventory for internal control, audit readiness, and decision-making.
- **Protect CEMA's Assets from Loss, Damage, Misuse, or Theft:**
  Implement preventive measures including physical security, proper storage, usage protocols, insurance, and staff training to reduce the risk of asset deterioration or unauthorized use. The policy ensures accountability and responsiveness in the event of asset-related incidents.
- **Comply with Financial Reporting and Donor Requirements:**
  Ensure that asset management practices align with international accounting

standards, Ugandan legal frameworks (such as the NGO Act and Income Tax Act), and the specific reporting and audit requirements of donors. This enhances transparency, builds donor confidence, and supports continued funding.

- **Guide Staff on Asset Use, Responsibility, and Accountability:**
  Provide clear instructions and assign custodial responsibility to individuals or departments, promoting responsible asset use and reinforcing the culture of stewardship. This includes guidance on proper handling, maintenance schedules, and reporting obligations.
- **Provide Procedures for Asset Acquisition, Maintenance, Transfer, and Disposal:**
  Offer standardized procedures and documentation for the full asset lifecycle—from procurement and tagging, through use and servicing, to reallocation or disposal—ensuring consistency, fairness, and value-for-money in all asset transactions.

---

4. Definitions

For the purpose of this policy, the following key terms are defined to ensure a clear and consistent understanding among all users of the policy:

- **Asset:**
  An asset is any item, whether tangible or intangible, that is owned, leased, or controlled by the Centre for Environment and Migration Assistance (CEMA) and is expected to be used in operations for a period exceeding one year. For financial and management purposes, assets covered under this policy are those with an initial acquisition cost equal to or greater than **UGX 500,000**. This includes, but is not limited to, office furniture, vehicles, computers, buildings, land, and licensed software. Assets are considered organizational resources and are subject to tracking, safeguarding, and reporting procedures throughout their lifecycle.
- **Custodian:**
  A custodian is a designated staff member who has been officially assigned the responsibility for the day-to-day care, proper use, safekeeping, and routine maintenance of a specific asset or group of assets. Custodians are accountable for reporting any loss, damage, or malfunction and ensuring that the asset is used in accordance with CEMA's operational and ethical standards. Custodianship does not imply ownership, but rather stewardship on behalf of the organization.
- **Asset Register:**
  The Asset Register is an official, centralized database or record system used to document and manage all assets owned or controlled by CEMA. It includes key information such as asset identification numbers, descriptions, locations, purchase dates, costs, depreciation values, conditions, and custodian details. The register is maintained and regularly updated by the Finance and Administration Department and serves as the authoritative source for asset verification, financial reporting, insurance, and audit purposes.

5. Roles and Responsibilities

Effective asset management requires the coordinated effort of various roles within the Centre for Environment and Migration Assistance (CEMA). This section outlines the specific responsibilities assigned to key positions to ensure accountability, transparency, and proper stewardship of organizational assets.

Role	Responsibilities
Executive Director	▪ Provides strategic oversight and final approval for all major asset-related decisions, including acquisitions, inter-departmental transfers, and disposals. ▪ Ensures that asset management practices align with organizational goals, donor expectations, and legal compliance. ▪ Authorizes exceptions to standard asset procedures where necessary and justified. ▪ Reviews periodic asset reports and audit findings to ensure operational and financial integrity.
Finance and Administration Manager	▪ Has overall responsibility for implementing and monitoring the Asset Management Policy. ▪ Maintains and updates the central **Asset Register**, ensuring completeness, accuracy, and timely entry of asset-related data. ▪ Monitors compliance with asset management procedures and coordinates asset verifications and audits. ▪ Ensures that asset depreciation, impairment, and write-offs are accurately reflected in the financial statements. ▪ Reports on asset-related issues to management and donors, including theft, loss, damage, and disposals.
Procurement Officer	▪ Ensures that all asset acquisitions follow the approved procurement policy, donor procurement guidelines, and value-for-money principles. ▪ Verifies that procured items meet the required technical specifications, quality standards, and warranty provisions. ▪ Facilitates the tagging and labeling of assets upon delivery and ensures all necessary documentation is shared with the Finance and Administration Department.

	▪ Works closely with the Finance team to ensure that all new assets are properly recorded in the Asset Register at the point of acquisition.
Project Managers/Department Heads	▪ Oversee the proper use, allocation, and condition of assets assigned to their respective departments or projects. ▪ Assign custodians for departmental assets and ensure they understand and fulfill their responsibilities. ▪ Conduct internal checks on asset usage and condition as part of routine project or departmental monitoring. ▪ Report any incidents involving asset loss, damage, or misuse promptly to the Finance and Administration Manager. ▪ Participate in annual asset verification exercises and support timely reconciliations.
Custodians	• Are directly responsible for the safekeeping, appropriate usage, and routine care of assets assigned to them. • Must ensure that assets are used strictly for official CEMA activities and in line with organizational and donor policies. • Are required to report any asset malfunction, damage, loss, or theft immediately to their supervisor and the Finance and Administration Department. • Assist in asset verification exercises and support inventory updates by making assets available for inspection. • May be held accountable for negligent use or failure to report changes in the condition or location of the asset.

6. Asset Acquisition

The Centre for Environment and Migration Assistance (CEMA) is committed to ensuring that all asset acquisitions are justified, transparent, cost-effective, and aligned with organizational and donor priorities. This section outlines the procedures and requirements for acquiring new assets—whether through purchase, donation, or lease.

6.1 Procurement Process

- All asset purchases must follow CEMA's **approved procurement procedures** and, where applicable, the procurement guidelines of funding partners or donors.
- Requests for asset acquisition must be initiated by the relevant department or project and supported by a justification that includes the purpose, estimated cost, and funding source.
- The Procurement Officer, in collaboration with the requesting department, must obtain quotations or bids, evaluate suppliers, and ensure compliance with value-for-money and quality standards before purchase decisions are made.
- Approval thresholds must be observed, with the Executive Director approving all major capital asset purchases in line with CEMA's financial delegation matrix.

6.2 Recording and Registration

Immediately upon acquisition of any asset, the following steps must be completed:

- **Entry into the Asset Register:**
  The Finance and Administration Department must record the asset in the official Asset Register. Details to be captured include:
    - Description and category of the asset
    - Date of acquisition
    - Serial number or model
    - Purchase price or valuation
    - Source of funding
    - Custodian and department
    - Estimated useful life and depreciation schedule
    - Physical location
- **Asset Identification Number:**
  A unique **Asset Identification Number (AIN)** must be generated and assigned to each asset to facilitate tracking and accountability. This number must be consistent across the register, labels, and documentation.
- **Asset Tagging:**
  All tangible assets must be **physically labeled** with a durable, tamper-proof **asset tag** bearing the AIN. Tags must be affixed in a visible and appropriate location on the asset. Tagging must be completed before the asset is deployed for use.

6.3 Donated and Leased Assets

- **Donated Assets:**
  Assets received through donation (whether from individuals, organizations, or development partners) must be:
    - Supported by a written **donation agreement** or letter of donation, clearly indicating ownership, terms of use, and any restrictions.
    - Accompanied by a **valuation certificate** or credible assessment to establish fair market value for accounting and insurance purposes.

    - Registered and tagged following the same procedures as purchased assets.
- **Leased Assets:**
  Leased or rented assets used by CEMA on a long-term basis must be documented through a formal lease agreement and included in the Asset Register for tracking and reporting, even though ownership remains with the lessor.

---

7. Asset Register

The **Asset Register** is a central and authoritative tool for managing CEMA's physical and intangible assets. It is designed to ensure that all assets owned, leased, or donated to the organization are properly recorded, monitored, and accounted for throughout their lifecycle. The register forms a key component of CEMA's internal control system and supports transparency, audit readiness, and strategic resource planning.

7.1 Purpose of the Asset Register

The primary purpose of the Asset Register is to:

- Track the acquisition, location, condition, and use of assets.
- Provide reliable data for financial reporting and audits.
- Support routine verification, maintenance planning, and insurance coverage.
- Serve as a reference point for asset transfers, disposals, and replacements.

7.2 Minimum Information to be Captured

Each asset entered into the Asset Register shall include, at a minimum, the following details:

- **Asset Identification Number (AIN):**
  A unique code assigned to each asset for easy tracking and reference across records and labels.
- **Description and Specifications:**
  A brief summary of the asset, including type, model, serial number, color, and any relevant technical specifications.
- **Date of Acquisition:**
  The date on which the asset was received, delivered, or became available for use.
- **Supplier or Donor Information:**
  The name of the vendor, supplier, or donor from whom the asset was acquired or received, including reference to procurement or donation documentation.
- **Location:**
  The physical location (office, region, department) where the asset is deployed or stored.

- **Assigned Custodian:**
  The name or position of the staff member or unit responsible for the use and care of the asset.
- **Cost and Depreciation:**
  The original purchase cost or fair market value (for donations), and a record of depreciation calculations based on the asset's expected useful life.
- **Condition/Status:**
  The current physical or operational condition of the asset (e.g., new, good, under repair, obsolete, damaged, lost).
- **Insurance Details (if applicable):**
  Information about any insurance policy covering the asset, including policy number, insurer, and expiry date.

Additional optional fields may include: warranty expiration dates, funding source, maintenance history, or barcode scan ID (if digital systems are in use).

7.3 Updating and Maintenance

- The Asset Register shall be maintained by the **Finance and Administration Department** and stored in both digital and hard-copy formats, with adequate backup and access controls.
- The register must be **updated quarterly** to reflect any changes in asset status, such as new acquisitions, changes in custodian or location, repairs, transfers, or disposals.
- Immediate updates must be made in the event of significant changes, such as loss, theft, damage, or insurance claims.
- The Asset Register shall be reviewed annually during the asset verification exercise and aligned with physical counts and audit findings.

Maintaining a complete and current Asset Register ensures that CEMA can make informed decisions regarding asset planning, replacement, and risk management while meeting internal and external accountability standards.

---

8. Asset Use and Maintenance

CEMA recognizes that the proper use and maintenance of organizational assets are essential for ensuring their longevity, functionality, and value for money. This section outlines the expectations and procedures governing how assets should be utilized and maintained to support operational effectiveness and reduce the risk of loss or premature deterioration.

8.1 Authorized Use

- All assets must be used strictly for **official CEMA business** and programmatic activities. Personal use of organizational assets is **prohibited**, unless explicitly authorized by the Executive Director under exceptional circumstances.

- Staff must adhere to ethical and professional standards when using organizational assets, avoiding negligence, abuse, or misuse that may result in damage or loss.
- Assets shall only be operated or handled by individuals who are **authorized and trained**, particularly in the case of technical equipment and vehicles.

8.2 Custodial Responsibilities

- Each asset shall be assigned to a designated **custodian**, typically a staff member or department head, who is responsible for its day-to-day use, security, and care.
- Custodians are expected to:
    - Ensure that assets are stored securely when not in use.
    - Handle and operate assets responsibly in accordance with manufacturer guidelines and CEMA's operational policies.
    - Immediately report any faults, losses, or damages to the Finance and Administration Department for follow-up.
    - Support asset verification, tagging, and relocation processes as needed.

8.3 Use and Management of Vehicles and Motorcycles

- All vehicles and motorcycles must be operated in compliance with **CEMA's Transport Policy**, which outlines procedures for trip authorization, safety checks, driver conduct, and logbook management.
- Drivers and authorized users must maintain **accurate fuel and mileage logs**, which are subject to regular review by project managers and the Finance and Administration Department.
- Unauthorized passengers, off-route travel, or private use of vehicles without written approval is strictly prohibited.
- All motor vehicles and motorcycles must undergo scheduled **preventive maintenance**, and only approved garages or service providers may be used for repairs.

8.4 Maintenance and Repairs

- All assets, particularly ICT equipment, vehicles, and machinery, must be maintained regularly to prevent breakdowns and ensure optimal performance.
- Routine and preventive maintenance schedules shall be developed and monitored by the responsible departments or custodians, with oversight by the Finance and Administration Manager.
- **All maintenance and repairs must be documented** and attached to the asset file, including:
    - Date of service
    - Nature of the issue
    - Service provider
    - Cost of repair
    - Confirmation of restored functionality
- Major repair costs must be approved in advance by the Executive Director or Finance and Administration Manager, in line with financial approval thresholds.

8.5 Insurance and Risk Mitigation

- Where applicable, assets such as vehicles, buildings, and high-value equipment must be covered by appropriate **insurance policies**.
- Staff are expected to take all reasonable precautions to **minimize risk**, including locking up assets after use, avoiding risky storage environments, and ensuring proper electrical protection for electronic devices.

By enforcing responsible asset use and consistent maintenance, CEMA aims to protect its investments, reduce operational disruptions, and ensure that assets serve their intended purposes throughout their useful life.

9. Asset Movement and Transfer

The movement and transfer of assets within or between locations or custodians is a critical process for maintaining proper control and accountability. This section outlines the procedures for the authorized movement of assets to ensure that all transfers are documented, tracked, and that assets remain secure during transit.

9.1 Authorization for Asset Movement

- The movement of assets between locations or departments, or from one custodian to another, must be **authorized in writing.** This written authorization serves as a record of the transfer request, the reason for the move, and the specific asset(s) involved.
- The request for transfer must be initiated by the **current custodian** or department head, who will submit a transfer request form to the **Finance and Administration Department** for approval.
- The transfer request must include the following details:
  - Asset ID number and description
  - Current location and custodian
  - New location and custodian
  - Reason for the transfer (e.g., relocation, departmental change, maintenance)
  - Date of transfer
- The **Finance and Administration Manager** is responsible for reviewing and approving the transfer request before assets are moved.

9.2 Documentation and Update of the Asset Register

- Once the asset transfer is approved and completed, the **Asset Register** must be updated to reflect the new location and custodian. This ensures that the organization maintains accurate, real-time information on asset status and location.
- **Documentation of transfer** must be kept on file, including:
  - Transfer request form, signed by both the outgoing and incoming custodians.

    - A confirmation of the transfer that includes the date and signatures of both custodians, ensuring that the new custodian accepts responsibility for the asset.
- In cases of significant asset movement (e.g., across locations or between offices), the Asset Register must be updated immediately upon completion of the transfer.

9.3 Custodian Responsibilities During Transfer

- The **outgoing custodian** is responsible for ensuring that the asset is in proper working condition before the transfer and that all relevant documentation (e.g., maintenance history, warranties, manuals) is handed over.
- The **incoming custodian** is responsible for verifying the asset's condition and ensuring that all required documents are received. They must formally acknowledge receipt by signing the transfer form.
- Both custodians must ensure that the asset is securely packed, labeled, and protected during the transfer process. The Finance and Administration Department should be informed immediately in the event of any damage or loss that occurs during the asset's movement.

9.4 Asset Movement Between Locations or Offices

- For assets moved between physical locations (e.g., regional offices, field stations, or external storage), additional precautions must be taken to ensure that the transfer is securely completed. This includes:
    - Proper packaging and labeling to prevent damage during transit.
    - Confirmation of receipt by the receiving office or department.
    - A record of transport logistics, such as the courier service or vehicle used for the transfer.

9.5 Unauthorized Asset Movement

- Any unauthorized movement of assets is prohibited. Movement without proper documentation and approval may result in disciplinary action, as it undermines internal controls and accountability.
- If assets are found to be missing or misplaced due to unauthorized movement, the custodian responsible for the last known location of the asset may be held liable.

9.6 Temporary Transfers or Loaned Assets

- Temporary transfers or loans of assets (e.g., for project use, personal development, or training) must follow the same procedures as permanent transfers. A **temporary asset loan agreement** must be signed by both parties, with clear timelines, usage terms, and return conditions.
- The Asset Register should note the expected return date and any special terms of the loan.

10. Asset Security

Ensuring the security of assets is fundamental to protecting CEMA’s resources from theft, damage, or misuse. This section outlines the measures that must be taken to safeguard organizational assets—both physical and digital—by implementing preventive, protective, and responsive strategies.

10.1 Secure Storage

- **Assets must be stored securely** when not in use. All physical assets (e.g., furniture, equipment, vehicles, and supplies) should be kept in locked, controlled environments when not actively being used.
- Storage areas should be well-organized to ensure easy access and to reduce the risk of asset misplacement or damage.
- High-value or sensitive assets (e.g., computers, medical equipment, or vehicles) should be stored in **designated secure areas** with restricted access, such as locked rooms or cabinets.
- Inventory storage locations must be monitored periodically by the custodian or relevant department to ensure that the assets are safe and well-maintained.

10.2 Digital Asset Security

- **ICT assets** (e.g., computers, smartphones, printers, and storage devices) must be secured using **password protection** and **access controls** to prevent unauthorized use or data breaches.
  - All computers and electronic devices should have **strong passwords** that are regularly updated according to CEMA’s **ICT Security Policy**.
  - Systems should use encryption software to protect sensitive data on devices and during transmission over networks.
  - Access to assets such as software, databases, or confidential information should be restricted to **authorized personnel** based on their role and the principle of least privilege.
  - Anti-virus and anti-malware software must be installed and updated regularly on all ICT assets to defend against potential cyber threats.
  - Devices should automatically lock after a set period of inactivity to prevent unauthorized access.

10.3 Physical Security of Office Premises

- CEMA’s office premises must have **adequate physical security** measures to protect all assets, particularly those that are highly valuable or sensitive.
  - **Locks and Security Systems:** All offices and storage areas where assets are kept must have **appropriate locks** on doors and windows. Where possible, **alarm systems** should be installed, particularly in areas where high-value assets are stored.

  - **Security Personnel:** In high-risk environments, the organization should consider employing **security guards** or other personnel to monitor access points and ensure that assets are not tampered with or stolen. Guards should be trained to follow the organization's security protocols and respond appropriately to security threats.
  - **Surveillance:** Security cameras, where feasible, should be installed in key areas (e.g., entrances, storage rooms) to monitor activities and provide evidence in case of any security incidents.
  - **Visitor Management:** Strict procedures should be followed for granting access to visitors. Visitors must be logged in and out of the premises, and they must be escorted by a staff member when accessing areas where assets are stored.
  - **Emergency Procedures:** CEMA must establish emergency protocols for asset protection in case of natural disasters, theft, fire, or other unforeseen events. These procedures should be regularly reviewed and communicated to all staff.

10.4 Vehicle and Equipment Security

- **Vehicles** used for official business must be securely parked when not in use. Vehicles should be locked at all times, and keys must be kept in a secure location when not in use.
  - If vehicles are being used for travel, an approved travel log should be maintained, detailing the trip, vehicle condition, and driver information.
  - Vehicles should be parked in well-lit, secure areas, particularly in high-risk locations or after hours.
- **Sensitive Equipment:** High-value equipment such as cameras, projectors, and laptops should not be left unattended in public spaces or in easily accessible areas. When not in use, such items should be securely locked away in offices or storage rooms.

10.5 Incident Reporting and Response

- Any **security breaches**, such as theft, damage, or unauthorized access, must be reported immediately to the **Executive Director** and the **Finance and Administration Manager** for investigation and action.
- **Incident reports** should be completed by the affected custodian or department, detailing the nature of the incident, the assets involved, and any mitigating actions taken.
- CEMA will investigate the cause of any security incidents, identify preventive measures to avoid recurrence, and ensure appropriate action is taken, including disciplinary procedures if necessary.
- In the case of theft or significant loss, a report should be filed with the **local authorities**, and the insurance provider should be notified for possible claims.

10.6 Insurance Coverage

- CEMA shall ensure that its assets are adequately covered by insurance policies against risks such as theft, fire, natural disasters, or accidents, depending on the asset type and its use.
- Regular insurance audits and reviews should be carried out to ensure that all high-value assets are included in the coverage, and that the organization's needs are met.

---

11. Asset Verification and Audit

Regular asset verification and audit processes are essential to ensure the accuracy of asset records, safeguard organizational resources, and identify potential risks such as loss, theft, or damage. This section outlines the procedures for conducting asset verification and audits, along with the responsibilities of staff in supporting these activities.

11.1 Annual Asset Verification

- **Physical verification of all assets** must be conducted at least once annually. This process ensures that the assets recorded in the **Asset Register** physically exist, are in good condition, and are being used appropriately.
- The asset verification should be carried out by a team comprising the **Finance and Administration Department** and designated staff from relevant departments or custodians.
    - The team will conduct a **physical count** of assets at all CEMA locations, including offices, storage facilities, and field offices.
    - Each asset's condition, location, custodian, and any signs of damage or deterioration should be noted during the verification process.
    - Assets should be checked against the **Asset Register** to ensure that all information is accurate and up-to-date.
    - Any discrepancies, such as unaccounted-for assets, damaged equipment, or missing items, should be documented and investigated promptly.

11.2 Investigation of Discrepancies

- Any discrepancies identified during the asset verification (e.g., **loss**, **theft**, **damage**) must be thoroughly **investigated**. The investigation will be led by the **Finance and Administration Department**, with support from the relevant custodian or department head.
    - The investigation should focus on determining the cause of the discrepancy (e.g., failure to follow proper asset management procedures, negligence, or malicious intent).

    - The custodian or department responsible for the asset should provide any necessary information or explanations to assist in the investigation.
    - Following the investigation, a report outlining the findings, causes of the discrepancies, and recommended corrective actions must be submitted to the **Executive Director** and other relevant management staff.
    - If the discrepancy involves theft or significant damage, CEMA may need to report the incident to **donors**, **regulatory bodies**, or **local authorities** as required.

11.3 Reporting of Discrepancies

- **Discrepancies must be reported promptly** to CEMA's **Executive Director**, **Finance and Administration Manager**, and any other relevant parties, such as project managers or department heads.
- If required by donor agreements or funding requirements, discrepancies involving assets may need to be communicated to donors in a formal report. This includes:
    - A detailed description of the asset(s) involved.
    - A summary of the discrepancies (e.g., loss, damage, theft).
    - Findings from the investigation and any corrective measures taken or planned.
    - The steps taken to prevent recurrence and ensure better accountability moving forward.

11.4 Reconciliation of Asset Register with Accounting Records

- At least annually, the **Asset Register** must be reconciled with **CEMA's accounting records**. This process ensures that the value of assets in the financial statements matches the actual assets held by the organization.
    - The reconciliation should compare the total value of assets in the **Asset Register** with the corresponding amounts recorded in the **general ledger** and **financial statements**.
    - Any discrepancies between the asset records and the accounting entries should be promptly addressed and corrected. These discrepancies could include issues such as misclassifications of assets or unrecorded depreciation.
    - The reconciliation process should be signed off by both the **Finance and Administration Manager** and the **Executive Director**, ensuring transparency and accountability in the asset management and financial reporting systems.

11.5 Audit of Assets

- **External and internal audits** of assets must be conducted periodically to assess the adequacy of asset management practices and compliance with relevant policies and regulations.

    - External audits should be performed annually or as required by CEMA’s funding agreements or statutory regulations.
    - Internal audits should be carried out regularly by CEMA’s internal audit team to evaluate asset management practices, identify potential areas of risk, and recommend improvements.
    - Audit findings and recommendations should be documented in an **audit report**, which will be reviewed by senior management and used to implement improvements in asset management procedures.

11.6 Corrective Actions and Improvements

- Any issues identified during the asset verification, investigation of discrepancies, or audits should be addressed through corrective actions. These may include:
    - Improving asset tracking and labeling systems.
    - Reinforcing asset security measures to prevent theft or damage.
    - Providing additional training to staff on asset management procedures and responsibilities.
    - Updating the Asset Register or accounting systems to correct errors or omissions.
- Regular reviews of asset management processes should be conducted to ensure continuous improvement in line with CEMA’s overall organizational goals and compliance requirements.

---

12. Asset Insurance

Asset insurance is a crucial component of CEMA's asset management strategy, ensuring that high-value and risk-prone assets are protected from potential loss, damage, or theft. This section outlines the guidelines for insuring CEMA’s assets, ensuring that the organization is adequately covered while minimizing financial risks associated with asset loss or damage.

12.1 Insurance Coverage for High-Value and Risk-Prone Assets

- **High-value assets**: Assets with significant monetary value, including but not limited to vehicles, ICT equipment, medical equipment, office furniture, and machinery, must be insured against common risks such as **fire**, **theft**, **vandalism**, **natural disasters**, and **accidents**.
    - The value threshold for high-value assets to be considered for insurance coverage will be determined by CEMA’s Finance and Administration Department and should be based on the current market value or replacement cost of the asset.
- **Risk-prone assets**: In addition to high-value assets, any assets deemed to be **high-risk** (such as vehicles, generators, or electronic devices) must also be insured. These assets are considered risk-prone due to their frequent use, exposure to the elements, or susceptibility to damage or theft.

- The following assets are generally considered high-risk or high-value and must be insured:
    - **Vehicles**: Cars, motorcycles, and any transport equipment owned or leased by CEMA.
    - **ICT Equipment**: Computers, laptops, smartphones, tablets, and other critical technological equipment.
    - **Medical Equipment**: Health-related assets, especially those used in the delivery of services in the field.
    - **Office Equipment and Furniture**: Assets such as printers, projectors, photocopiers, and high-quality office furniture.
    - **Machinery**: Specialized tools or machinery that are essential to project implementation or operations.

12.2 Types of Insurance Coverage

- **Comprehensive Coverage**: This type of insurance should cover a wide range of potential risks, including theft, fire, natural disasters (e.g., earthquakes, floods), vandalism, and accidental damage. It is particularly important for assets used in high-risk environments or frequently transported.
- **Third-Party Liability Coverage**: For vehicles and transport-related assets, CEMA should ensure third-party liability insurance is in place to cover any damages or injuries caused to others in the event of an accident.
- **Fire and Theft Coverage**: For assets such as equipment, machinery, and office furniture that are stored in secure but potentially vulnerable areas, fire and theft insurance is crucial to mitigate risk.
- **Travel and Field Work Insurance**: When assets are used in the field or during travel (such as vehicles or portable ICT equipment), CEMA should consider specific insurance coverage for fieldwork risks, including coverage for loss or damage during transportation.

12.3 Insurance Policy Management

- **Annual Review of Policies**: All insurance policies covering CEMA's assets must be **reviewed annually** by the **Finance and Administration Department** to ensure they provide adequate coverage based on asset values, current risks, and operational needs.
    - During the annual review, the Finance and Administration Department should assess any changes in asset values (e.g., new acquisitions, disposals, depreciation) and update insurance policies accordingly.
    - The review should also consider any changes in risk exposure, such as the introduction of new assets, expansion into new locations, or changes in the operating environment (e.g., higher risk of theft or natural disasters in a given area).
- **Renewal and Claims Process**: Insurance policies must be renewed on time to ensure continuous coverage. The **Finance and Administration Manager** is responsible for overseeing the timely renewal of insurance contracts, and for managing the claims process in the event of asset loss or damage.

    - In the event of asset loss, theft, or damage, the **Finance and Administration Department** must immediately initiate the claims process with the insurance provider. This includes documenting the incident, submitting necessary forms, and providing evidence of loss or damage (e.g., incident reports, photographs).
    - The organization should keep a record of all claims filed and track the outcome of each claim to ensure that insurance proceeds are appropriately allocated.

12.4 Documentation and Reporting

- **Insurance Documentation**: All insurance policies, certificates, and related documents must be **properly filed and easily accessible** for audit purposes. The **Finance and Administration Department** is responsible for maintaining the insurance documentation, including:
    - Policy numbers, renewal dates, and the scope of coverage.
    - Evidence of premium payments and policy amendments.
    - Claims documentation, including communication with the insurance company and any payments received.
- **Insurance Reporting**: Insurance details, including policy coverage and any claims made, should be reported to CEMA's **Board of Directors** and relevant stakeholders on an annual basis. This reporting ensures transparency and keeps leadership informed about the organization's risk management strategy.

12.5 Exclusions and Limitations

- Insurance policies may include certain **exclusions** or **limitations** regarding the types of damages or losses covered. It is important for CEMA to review the **terms and conditions** of each policy to understand any restrictions.
    - For example, insurance may not cover losses due to negligence, improper use, or unauthorized access to assets.
    - If an asset is involved in an incident that is excluded from coverage, CEMA may need to bear the financial responsibility for the loss.
- To mitigate these risks, all staff must be **trained** on asset protection practices to prevent damage or theft that could void the insurance coverage.

12.6 Insurance Costs and Budgeting

- The cost of insurance premiums must be included in CEMA's annual budget. The **Finance and Administration Manager** should work with the accounting department to ensure that adequate funds are allocated for asset insurance coverage.
    - The cost of insurance should be weighed against the value of the assets being covered, and the potential risks to which those assets are exposed.

    - Insurance premiums should be monitored to ensure that they remain reasonable and that the coverage provided is proportional to the value of the assets insured.

---

13. Asset Disposal

Asset disposal is an essential process in managing CEMA's resources, ensuring that assets that are no longer useful, obsolete, or beyond repair are appropriately removed from the organization's inventory. This section outlines the guidelines and procedures for the disposal of assets, ensuring transparency, accountability, and compliance with organizational policies and donor requirements.

13.1 Reasons for Asset Disposal

Assets may be disposed of under the following circumstances:

- **Obsolescence**: When an asset is no longer useful due to technological advancements or changes in operations. For example, outdated computers, software, or equipment that cannot meet current needs.
- **Damage Beyond Repair**: When an asset is damaged beyond repair and cannot be restored to a functional condition, such as broken machinery, vehicles that are no longer operable, or equipment with severe faults.
- **No Longer Needed**: When an asset is no longer required for the organization's activities. This could be due to changes in program focus, project completion, or an excess of a certain asset type (e.g., surplus furniture or equipment).

13.2 Disposal Methods

CEMA may choose from several methods to dispose of assets, depending on the asset's condition, value, and relevance to the organization's needs.

- **Sale (via Competitive Bidding)**:
    - When an asset has value and can be sold, it should be disposed of through a **competitive bidding process**. This ensures that the asset is sold at fair market value and that CEMA receives the maximum possible return.
    - A public notice or advertisement should be issued to invite bids from potential buyers, with clear guidelines on the minimum price, asset condition, and the terms of sale.
    - The sale process must be transparent and conducted in compliance with CEMA's procurement and financial policies. The **Procurement Officer** will oversee this process, ensuring that all bids are reviewed fairly.
    - The **Finance and Administration Manager** must document the outcome of the sale and deposit the proceeds in CEMA's account.
- **Donation (with Prior Approval)**:

    - If an asset is still usable but no longer required by CEMA, it may be donated to another organization, community group, or charitable cause. However, donations must be approved in advance by the **Executive Director** to ensure that they are in line with CEMA's strategic goals and donor agreements.
    - The organization receiving the donation must be clearly identified, and a **Donation Agreement** should be drawn up, outlining the asset description, transfer conditions, and any stipulations about the use of the asset.
    - The **Asset Register** must be updated to reflect the donation, and documentation of the donation must be kept for reporting purposes.
- **Write-off (with Justification):**
    - If an asset is deemed completely unusable, damaged beyond repair, or obsolete, it may be written off the books. A **write-off** is appropriate when the asset has no residual value or is unlikely to be repaired or repurposed.
    - The **Finance and Administration Manager** must ensure that a clear **justification** for the write-off is provided, which could include a report on the condition of the asset, the reason for disposal, and any financial implications.
    - Write-offs should be reviewed and approved by the **Executive Director** and documented in the **disposal register** for audit and compliance purposes.

13.3 Disposal Approval and Documentation

- **Approval Process**: All disposals of assets must be **approved by the Executive Director**. Before any asset is sold, donated, or written off, the approval process must be followed to ensure that disposal is in the best interest of the organization and complies with financial and regulatory requirements.
    - A **Disposal Request Form** should be submitted by the department responsible for the asset, detailing the asset in question, the reason for disposal, the proposed disposal method, and an estimated value (if applicable).
    - The **Executive Director** must review the request and approve or reject it based on operational, financial, and strategic considerations.
- **Disposal Register**: All asset disposals must be documented in a **Disposal Register**, which is maintained by the **Finance and Administration Department**. The register should include:
    - Asset ID and description
    - Date of disposal
    - Method of disposal (sale, donation, write-off)
    - Approval signatures (Executive Director, relevant department heads)
    - Details of any proceeds from sales (amount and deposit details)
    - Recipient organization (if donated)
    - Justification for write-off (if applicable)

This register will serve as the official record of all disposals and will be reviewed during asset audits to ensure proper adherence to disposal procedures.

13.4 Proceeds from Asset Sales

- **Proceeds from sales** of assets must be deposited directly into CEMA's official **bank account**. The sale of assets is an important source of funding for the organization and should be handled with financial transparency.
    - All proceeds must be **accounted for** and properly recorded in CEMA's financial system, ensuring that they are clearly identified as part of the asset disposal process.
    - Any revenue generated from the sale of assets should be used in accordance with CEMA's financial policies and may be allocated for reinvestment into the organization's activities or other operational needs.
- The **Finance and Administration Manager** is responsible for tracking the deposit of proceeds and ensuring that the sale is reflected in CEMA's financial records.

13.5 Environmental and Ethical Considerations

- When disposing of assets, particularly electronic or high-tech equipment, CEMA must consider **environmental and ethical standards** for disposal. This includes ensuring that assets are disposed of in a manner that does not harm the environment or violate any local laws.
    - Electronic waste (e-waste) should be disposed of through certified recycling centers that follow environmentally safe disposal methods.
    - When donating assets, CEMA should ensure that the receiving organization has the capacity to use the asset appropriately and that it will benefit the community or cause it is intended for.
- CEMA is committed to ensuring that all asset disposal practices are aligned with **sustainability principles** and **ethical standards**.

---

14. Intangible Assets

Intangible assets, which are non-physical but essential for the functioning of CEMA, must be carefully managed to ensure their value is protected, optimized, and compliant with applicable regulations and contractual agreements. This section provides guidelines on the management of **software**, **digital licenses**, and other intangible assets, ensuring that they are used responsibly and securely.

14.1 Software and Digital Licenses

- **Software Acquisition and Licensing**:
    - All software acquired by CEMA, whether through purchase, subscription, or donation, must be **licensed** in accordance with the

        terms and conditions set forth by the software provider. CEMA must ensure that it complies with the specific licensing agreements for each piece of software to avoid legal risks, including potential fines or penalties.
    - Licenses must be valid, up-to-date, and include details of the number of authorized users, any restrictions on use, and the duration of the license.
    - The **Procurement Officer** is responsible for verifying that software purchases are licensed correctly and that any licenses for software subscriptions are renewed in a timely manner.
- **License Management**:
    - **Software License Register**: A **Software License Register** must be maintained to track all software licenses owned or used by CEMA. The register should include the following details:
        - Software name and version
        - License type (e.g., single-user, multi-user, site-wide)
        - License expiry date (if applicable)
        - Number of users or devices covered by the license
        - Cost of the software and any recurring costs (e.g., annual maintenance or subscription fees)
        - License agreement terms (restrictions, conditions, etc.)
    - This register must be reviewed and updated **annually** or whenever new software is purchased, an existing license is renewed, or a license is terminated.
- **Compliance with License Agreements**:
    - Software must only be used within the boundaries defined by the license agreement. CEMA staff should be trained on the proper use of software and should understand that unauthorized copying, distribution, or use of software is strictly prohibited.
    - Any violation of the licensing agreements must be reported immediately to the **Finance and Administration Manager** and addressed in a timely manner.

14.2 ICT Systems Management

- **System Updates and Patches**:
    - To ensure the integrity, security, and functionality of CEMA's software, ICT systems (including operating systems, applications, and network systems) must be **regularly updated.** Updates should include security patches, bug fixes, and any new features that improve the system's performance or usability.
    - The **ICT Manager** (or designated IT staff) is responsible for regularly checking for software updates and applying them across CEMA's systems in a timely manner. This will help protect CEMA's systems from potential security vulnerabilities and performance issues.
- **Data Backup and Recovery**:
    - CEMA must implement a **data backup and recovery** plan to protect critical digital information, including documents, project data, financial records, and communications.

  - **Regular Backups**: All essential data, including software configurations, databases, and operating system files, should be backed up **daily** or **weekly**, depending on the frequency of changes to the data. This will ensure that critical information can be restored in the event of system failure, corruption, or loss.
  - **Cloud or Off-site Storage**: Backups should be stored in a secure off-site location, either through **cloud-based storage solutions** or physical external drives stored in a secure location. Cloud storage services should be selected based on **security features** such as encryption, multi-factor authentication, and compliance with relevant data protection laws (e.g., GDPR, if applicable).
  - **Backup Verification**: Periodic testing should be conducted to verify that backups are functioning correctly and that data can be restored when needed.
  - **Data Recovery Plan**: A clear and documented recovery procedure must be in place to guide staff on how to restore data in case of an emergency, such as a system failure or cyberattack.

14.3 Intellectual Property Rights

- **Protection of Intellectual Property (IP)**: CEMA must respect the intellectual property rights (IPR) of others when acquiring, using, or distributing software, content, or other digital assets. This includes ensuring that:
  - The organization does not violate the copyrights, patents, or trademarks of software developers, digital content creators, or other rights holders.
  - **Third-party software** is used only in accordance with licensing agreements and that CEMA does not engage in unauthorized distribution or modification.
- **CEMA's Own Intellectual Property**:
  - Any software, digital tools, or digital content created by CEMA (e.g., databases, reports, training materials) should be documented and protected under **CEMA's intellectual property policies**.
  - If CEMA develops proprietary software or other intellectual assets, proper documentation, licensing, and protection procedures should be followed to safeguard the organization's IP.

14.4 Security and Access Control

- **Access Control**:
  - To protect software, systems, and sensitive data, strict **access controls** should be implemented. This includes assigning appropriate levels of access based on staff roles and responsibilities.
  - **Role-based access**: Staff members should only have access to the software and data necessary for their work. The **ICT Manager** should ensure that access permissions are regularly reviewed and updated.

    - **Password Management**: All software, systems, and digital platforms should be protected by strong passwords, which should be regularly changed and follow best practices (e.g., minimum length, complexity).
- **User Training:**
    - Staff must receive ongoing training on **ICT security best practices** and the proper use of software. This training should cover topics such as:
        - Recognizing phishing and other security threats.
        - How to securely access and store data.
        - The importance of software updates and patches.
        - How to report any security incidents or vulnerabilities.

14.5 Disposal of Intangible Assets

- When software or digital licenses are no longer needed, they must be properly disposed of according to the terms of the software license agreement. This may include:
    - **License termination**: Ensure that licenses are officially terminated or deactivated once they are no longer in use, particularly for subscription-based software.
    - **Secure data deletion**: When disposing of software or systems, any data associated with the software must be securely erased to prevent unauthorized access to sensitive information.
    - If software is transferred, donated, or sold, proper documentation should be kept to ensure compliance with licensing agreements.

14.6 Legal and Regulatory Compliance

- CEMA must ensure that its use of intangible assets, including software and digital content, complies with all applicable **national** and **international laws**, such as:
    - **Data protection laws**: Adhere to laws and regulations on the handling, storage, and protection of data (e.g., Uganda’s Data Protection and Privacy Act, 2019).
    - **Copyright laws**: Ensure that CEMA’s software use does not infringe upon copyright laws and that CEMA respects licensing agreements.
    - **Cybersecurity regulations**: Follow guidelines for securing ICT systems to protect against cyberattacks and data breaches.

15. Compliance and Sanctions

Compliance with the Asset Management Policy is essential for the effective and responsible management of CEMA's resources. All staff and stakeholders involved in asset management must adhere to the guidelines set out in this policy to ensure transparency, accountability, and the protection of CEMA's assets. This section outlines the consequences of non-compliance and the potential sanctions for failure to follow the policy, including actions related to theft, willful damage, or misuse of assets.

15.1 General Compliance Requirements

- All CEMA staff members, contractors, and volunteers must adhere to the principles and procedures outlined in this Asset Management Policy. This includes ensuring proper use, maintenance, security, and disposal of assets as specified in the policy.
- Compliance is the responsibility of all staff, particularly those in positions that involve the direct handling, procurement, or management of assets. Department heads, project managers, and custodians are expected to ensure that their teams are fully informed about the policy and follow the outlined procedures.
- Regular training and awareness programs will be provided to staff to ensure understanding and adherence to the Asset Management Policy, including updates on any changes to the policy.

15.2 Disciplinary Actions for Non-Compliance

Failure to comply with the policy may result in **disciplinary action** based on the severity of the violation. The specific disciplinary actions may include, but are not limited to, the following:

- **Verbal Warning**: For minor, unintentional violations of the policy, a staff member may receive a formal verbal warning. This is typically used for first-time offenses or minor lapses in adherence to asset management procedures.
- **Written Warning**: A formal written warning may be issued if a staff member continues to violate the policy after a verbal warning, or if the violation is deemed more serious (e.g., failure to maintain assets properly, failure to update the Asset Register).
- **Suspension**: For more serious violations, such as significant negligence in asset management or repeated violations despite warnings, the staff member may be suspended from their duties. The duration of the suspension will be determined by the severity of the offense and may be accompanied by a performance review.
- **Termination of Employment**: In cases of severe non-compliance, such as repeated violations, negligence, or failure to follow internal controls despite multiple warnings, the staff member may face termination of employment. This decision will be made in consultation with the **Executive Director** and **HR Department** based on an internal investigation and consideration of the facts.

15.3 Theft, Willful Damage, or Misuse of Assets

Theft, willful damage, or intentional misuse of CEMA’s assets is a serious violation of the organization’s policies and will not be tolerated. Such actions undermine the integrity of the organization and may lead to both internal sanctions and legal action.

- **Theft**: Any staff member found to have intentionally stolen or misappropriated CEMA assets will face immediate disciplinary action, which may include **termination of employment**. In addition, the staff member will be subject to legal proceedings in accordance with **Uganda's laws on theft**, as well as potential **civil liability** to recover the value of the stolen assets.
- **Willful Damage**: If a staff member is found to have intentionally damaged CEMA's assets (e.g., by neglecting maintenance responsibilities, tampering with equipment, or causing physical harm to assets), they will be subject to serious disciplinary action. This could include **suspension** or **termination** depending on the extent of the damage. In cases of significant financial loss, the staff member may be required to compensate for the damage caused.
- **Misuse of Assets**: Misuse of CEMA's assets refers to the improper or unauthorized use of assets for personal benefit or purposes unrelated to CEMA's operations. This could include:
    - Using CEMA vehicles, equipment, or ICT resources for personal use without proper authorization.
    - Allowing unauthorized individuals to use CEMA property.
    - Using digital systems, software, or licenses outside the scope of the agreed terms.

  Misuse of assets will result in disciplinary action, starting with a **written warning** and escalating to **termination** for repeated or severe violations. In cases where misuse leads to financial loss or reputational damage, the individual may be required to reimburse CEMA for the loss incurred.

15.4 Reporting Violations

All staff have a responsibility to **report violations** of the Asset Management Policy to their supervisors, department heads, or directly to the **Executive Director**. Reporting can be done through:

- **Direct communication** with supervisors or managers.
- **Anonymous reporting channels**, if available, to ensure confidentiality and protection for whistleblowers.

CEMA encourages an open and transparent environment where staff can report violations without fear of retaliation. All reports of non-compliance will be treated seriously, and investigations will be conducted promptly and fairly.

15.5 Investigation and Due Process

When a potential violation of this policy is identified, CEMA will follow due process to investigate the matter thoroughly. The investigation will be carried out by the **HR Department** or an appointed disciplinary committee, which will:

- Review the facts surrounding the violation.
- Interview the involved staff member(s) and any witnesses.
- Document the findings and determine the severity of the violation.
- Provide the staff member with an opportunity to explain their actions before any final decision is made.

Based on the investigation, appropriate action will be taken, including possible disciplinary measures or legal action.

15.6 Legal Action and Liability

In cases of theft, fraud, or other criminal acts related to asset misuse, CEMA reserves the right to take **legal action** against the responsible individual(s) in accordance with **Uganda's criminal laws**. Legal action may include:

- **Criminal prosecution** for theft, fraud, or other criminal behavior.
- **Civil litigation** to recover the value of stolen or damaged assets.
- **Fines or penalties** if the individual's actions have caused significant harm or financial loss to CEMA.

CEMA's legal team, in collaboration with law enforcement agencies, will take appropriate steps to ensure that any criminal or illegal activities related to asset misuse are pursued to the full extent of the law.

15.7 Ensuring a Culture of Compliance

To foster a culture of compliance, CEMA will:

- Regularly **train staff** on the Asset Management Policy and emphasize the importance of responsible asset use.
- Conduct **periodic internal audits** to ensure that asset management practices align with policy guidelines and identify any potential areas for improvement.
- Encourage **staff accountability** by promoting the principle that every employee is responsible for the proper use and safeguarding of CEMA's assets.

By ensuring that clear consequences exist for non-compliance and encouraging a culture of transparency, CEMA aims to protect its assets, uphold ethical standards, and maintain the trust of its donors, partners, and the communities it serves.

---

16. Review of the Policy

The Asset Management Policy is a living document that must evolve in response to changes in organizational needs, legal requirements, and best practices. Regular reviews of the policy are essential to ensure its continued relevance and effectiveness in guiding the management of CEMA's assets. This section outlines the review process, including the timing, scope, and responsibilities for conducting the review.

16.1 Frequency of Review

- **Biennial Review**: This policy will be formally reviewed at least once every **two years** to ensure it remains up-to-date with CEMA's operational needs, financial controls, and changes in asset management practices.
- **Trigger Events for Review**: In addition to the biennial review, the policy will be revisited whenever there are significant changes to the organization's operations, regulatory environment, or donor conditions. Specific events that may trigger a review include:
    - **Changes in Uganda's laws and regulations**: For example, amendments to the Uganda National Procurement Act, changes in asset taxation, or new data protection laws that may affect asset management.
    - **Donor requirements**: If CEMA receives new funding or engages with a new donor, that donor may have specific requirements related to asset management, which may necessitate updates to this policy.
    - **Internal structural changes**: When CEMA undergoes major organizational changes, such as the introduction of new departments, new types of assets, or changes to its operational scope (e.g., new geographic areas, programs, or project types), the policy will be assessed to ensure it covers these changes.
    - **Emerging best practices**: If new asset management technologies, software, or methodologies become available, the policy may be updated to reflect these innovations, enhancing the efficiency and effectiveness of asset management.

16.2 Review Process

- **Initiation of Review**: The review of the Asset Management Policy will be initiated by the **Finance and Administration Manager** or the **Executive Director** at the beginning of the review period or in response to the events outlined above. The decision to conduct a review will be formally documented, and an action plan for the review process will be developed.
- **Review Committee**: A review committee will be established to oversee the review process. The committee will include, at a minimum:
    - **Executive Director**: As the senior management representative, responsible for overseeing the review and ensuring alignment with organizational goals.
    - **Finance and Administration Manager**: To provide input on the financial aspects of asset management and ensure compliance with accounting standards and donor requirements.
    - **Procurement Officer**: To ensure that procurement practices are adequately reflected in the policy and aligned with current regulations and donor requirements.

    - **Project Managers/Department Heads**: To ensure that the policy reflects the needs of specific departments and project activities.
    - **HR Representative**: To assess any implications for staff roles and responsibilities related to asset management and ensure alignment with CEMA's personnel policies.
    - **ICT Manager**: To evaluate the management of intangible assets, particularly software and digital resources, and ensure that IT-related processes are covered in the policy.
- **Review Process Steps**:
    1. **Gather Feedback**: The review committee will gather feedback from staff involved in asset management to identify any challenges, inefficiencies, or areas of improvement. This feedback will be collected through interviews, surveys, and consultations with custodians, department heads, and other relevant personnel.
    2. **Analyze Changes**: The committee will analyze any external changes, such as new legal requirements, donor conditions, or technological advancements, that may impact the policy. It will also consider any internal operational changes that have occurred since the last review.
    3. **Assess Policy Effectiveness**: The effectiveness of the current policy will be assessed by reviewing audit reports, compliance with the policy, and any issues or breaches that have arisen during the previous period.
    4. **Update and Revise**: Based on the feedback and analysis, the committee will propose updates to the policy to address emerging needs or issues. Revisions may involve adding new sections, clarifying existing sections, or modifying processes to improve asset management practices.
    5. **Approval of Updated Policy**: Once the review committee has made its revisions, the updated policy will be submitted to the **Executive Director** for final approval. The Executive Director will ensure that the policy aligns with CEMA's strategic objectives and regulatory obligations before it is adopted.
    6. **Communication of Updates**: After approval, the updated policy will be communicated to all staff members and relevant stakeholders. A training session or refresher course may be conducted to ensure that all staff understand the revised policy and are aware of their roles and responsibilities regarding asset management.

16.3 Record-Keeping and Documentation

- **Policy Documentation**: All versions of the policy, including the initial policy and any revisions, will be archived and stored in a centralized repository, such as the organization's shared drive or document management system. Each version will be clearly labeled with the revision date and any significant changes made.
- **Audit Trail**: An audit trail of the policy review process will be maintained, documenting the steps taken, decisions made, and feedback received. This

ensures transparency in the review process and provides a record of the changes made to the policy over time.

16.4 Continuous Improvement

- **Ongoing Monitoring**: In addition to the scheduled biennial reviews, the policy will be continuously monitored for effectiveness. If any issues arise, such as non-compliance or operational inefficiencies related to asset management, immediate corrective action may be taken, and the policy may be revised outside the regular review cycle.
- **Stakeholder Engagement**: CEMA will regularly engage with external stakeholders, including donors, auditors, and other relevant organizations, to learn from their experiences and ensure that the organization's asset management practices remain aligned with global best practices.

16.5 Responsibility for Policy Review

The **Finance and Administration Manager**, with input from other key staff members, will be responsible for coordinating the review of the Asset Management Policy. However, the final approval and adoption of the revised policy will remain the responsibility of the **Board Chairperson**.

Prepared by:
Rita Kabagabu, Finance and Administration Manager

Reviewed by:
Abas Ruhweza, Executive Director

Approved by:
Rev. Moses Atuhaire, Board Chairperson