# Zimbabwe Carbon Markets Authority

# Zimbabwe Carbon Registry: Security and Access Control Policy

# V1

# February 2026

---

## 1. OVERVIEW

**1.1.** This Policy outlines the security and access control policy of the Zimbabwe Carbon Registry (ZCR). It outlines the provisions put in place to ensure that the registry and all data processed through the Zimbabwe Carb0on Markets Authority (ZiCMA) platform is secure, and that all accounts and transactions are genuine.

**1.2.** For the purpose of this policy "Registered Account Holders" refers approved account holders registered by ZiCMA, and "Users" refers to all parties accessing the public pages of the ZiCMA web-platform and ZCR.

**1.3.** If any breach of these security provisions that affects any Registry Account Holder or registered units, ZiCMA shall notify all affected parties including the affected account holders and any international institutions as applicable (e.g., the UNFCCC and ICAO Secretariat).

## 2. Security Provisions

**2.1.** The ZCR maintains a layered set of statutory, technical, procedural and administrative security controls to protect the integrity of registry data, ensure authenticated and secure access, and safeguard all transactions carried out by registered account holders.

**2.2.** All data processed through the platform is protected through recognised encryption controls, including encryption at rest and in transit.

**2.3.** User passwords are stored in encrypted form, and secure session-token controls are used to manage authenticated access. Sessions are automatically terminated after 60 minutes of inactivity to reduce the risk of unauthorised access.

**2.4.** Critical records, events and document references are anchored to blockchain infrastructure to provide a tamper-evident layer and an independently verifiable evidentiary trail.

**2.5.** Documents issued through the platform are assigned unique cryptographic hashes, enabling the detection of any alteration. This supports the real time verification of authentic actions and maintains the integrity of all historical registry records and submissions.

**2.6.** The ZCR is administered with multiple security and trust layers. Application layer-controls govern user authentication, permissions, workflow restrictions, and approval paths. Storage and database layers support operational reliability, replication, and recovery. Blockchain and cryptographic validation layers provide integrity assurance independent of the primary application database.

**2.7.** The ensure continuous accessibility and reliability, the ZCR has no single points of failure. Data is replicated across multiple separated environments including databases across multiple cloud providers, replicated server clusters, S3-based storage, dedicated IPFS servers, and blockchain-linked validation layers.

**2.8.** Weekly offline backups are maintained to support full disaster recovery.

**2.9.** The ZCR is protected by infrastructure and network security measures including DDoS mitigation, DNS protection, malicious traffic filtering, and web-application firewall protections.

**2.10.** To provide a full audit trail, Full logging maintained for system actions, administrative actions, and technical support interventions.

## 3. Account Screening

**3.1.** In accordance with the Carbon Trading (General) Regulations (2025) ("the Regulations"), all legal and natural persons must register with the Authority and maintain an active account on the ZiCMA platform to perform any transactions pertaining to carbon credits/units held in Zimbabwe.

**3.2.** Accounts may be held by legal (e.g., registered companies and corporations) and natural persons (e.g., individuals).

**3.3.** In accordance with the Regulations, all applicants must evidence to the satisfaction of the Authority, compliance with all eligibility requirements for the account type for which registration is sought.

**3.4.** Registration requests not completed in accordance with the procedures outlined in the Regulations shall not be considered.

**3.5.** Accounts shall only be approved for natural and legal persons able to verify their identity and undergo a successful Know-Your-Customer (KYC) check carried out by an independent third party.

**3.6.** Users are notified when verification is taking place.

**3.7.** ZiCMA retains the right to request additional information as needed to satisfactorily determine and verify the identity of all applicants.

**3.8.** Account holders may be domiciled in Zimbabwe or Abroad. ZiCMA shall not discriminate based on the country of origin of any account registration request or account.

## 4. Access and Transaction Controls

**4.1.** Access to all registry and platform data is governed through a strict role-based access control framework.

**4.2.** Users are segmented by statutorily defined roles, including government administrators, auditors (registered verifiers and validator accredited and licensed by the Authority), buyers (general account holders), project developers, and unregistered platform users. Each kind of user is only able to access approved areas of the platform corresponding to the information and functionalities relevant to the role.

**4.3.** Administrative access is segmented across different privilege and access levels in accordance with ZiCMA and Government of Zimbabwe internal procedures. Access is ordered under a "least-privilege model" under which users and administrators are granted only those permissions necessary for their defined functions.

**4.4.** Access to all transactional functionalities is limited to registered account holders.

**4.5.** Additional procedural and statutory controls are applied to all sensitive activities, including project approval and authorisation in accordance with the Regulations and Ministry of Environment, Climate and Wildlife internal policy.

**4.6.** Multifactor authentication is supported for all registered user and transaction types.

**4.7.** IP address and access logs are recorded and made available to users, allowing them to verify access activity associated with their accounts and supporting the identification of anomalous activity.

**4.8.** For credit/unit transactions the platform presents two separate confirmation screens before the transaction is completed. The first requires the user to confirm they wish to proceed with the action, the second presents a summary of the transaction, including the relevant transaction details and associated fees.

**4.9.** Where multi-factor authentication has been enabled by a registered account holder, the user must enter a MFA token prior to unit transactions.

**4.10.** All material actions are attributable to a specific authenticated user or authorised operator, together with the relevant approval and system history associated with the event. The ZCR maintains audit and attribution controls to support non-repudiation. User actions, confirmations, approvals, and administrative interventions are logged with sufficient detail to support audit, review and investigation.

## 5. Regular Audit and Review

**5.1.** All security provisions outlined in this policy undergo regular audit and review. Where material changes are made to these provisions, and updated version will be made available on the ZiCMA portal.

**5.2.** All provisions outlined in this document are subject to ongoing maintenance, testing, and review in accordance with recognised international standards of best practice.

**5.3.** A complete audit and review of platform security features is completed every six months.

**5.4.** Regular system tests are completed quarterly.

**5.5.** The ZCR operates dedicated testing environments in which quality assurance processes are carried out prior to deployment to the live production environment. No production changes are introduced without prior testing and validating.

**5.6.** Dependencies and software components are patched and updated in with international standards of based practice.

**5.7.** All documents relevant to the administration of the ZCR and any units in relation to international compliance schemes including Article 6 and CORSIA shall be retained for a period of at least 5 years.

## 5.8.