

END USER LICENSE AGREEMENT (EULA)

IMPORTANT: READ CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE.

This End User License Agreement ("Agreement") is a legally binding contract between **Maestro IT (Pty) Ltd** ("Licensor") and you ("Licensee" or "User") installing and using the **Machuzu NextGen Application** ("Software"). By downloading, installing, running the launcher file, or using the Software, you agree to be bound by these terms. **If you do not agree, do not install or use the Software.**

1. Scope of Agreement & Third-Party Exclusions

- **Strict Licensing Scope:** This Agreement applies **exclusively** to the proprietary application file `Machuzu-Next-Gen.jar` and its companion execution batch file `LaunchMachuzuNextGen.bat`.
- **Absolute Third-Party Product Exclusion:** This license explicitly **excludes** any and all third-party software, utilities, packages, and runtimes required to configure the execution environment.
- **Separate Terms Apply:** Third-party components—including but not limited to **Java 17, OpenJFX 17, SQLite command-line tools, and ImmuDB**—are downloaded by the User from their respective provider sources. Maestro IT (Pty) Ltd holds no ownership over, provides no warranties for, and assumes zero liability for the installation, functionality, licensing compliance, or performance of these independent third-party applications.

2. Technical Environment & Setup Obligations

- **User Directory Management:** The Licensee is solely responsible for establishing the file environment (e.g., creating the `MachuzuNextGen` folder) and acquiring external prerequisites. The application requires explicit operating system file read/write access to its execution path to process crypto files, map internal configurations, and manage network keys.
- **Launcher Modifications:** Users are permitted to edit configuration parameters inside `LaunchMachuzuNextGen.bat` using standard plain text editors (such as Notepad) solely to align JavaFX environment paths with their local machine's installation directory.

3. Technology Risks & Architecture Disclosures

The Machuzu NextGen core application is designed to operate alongside localized database frameworks and peer-to-peer cryptographic structures. The Licensee explicitly acknowledges and assumes the specific technical risks inherent to this architecture:

- **Data Encryption Tiers (Free vs. Premium Versions):**
 - **The Freely Available Version:** Licensee explicitly acknowledges that **the free tier of the Software does not encrypt all data** transmitted between the local computer, the cloud node (`://machuzu.com`), and other network nodes running on external computers. Broadcasted information, transaction details, or cleartext files may be visible across these transit paths. Users are advised not to process highly sensitive or confidential information on this tier.
 - **The Premium Version:** In contrast to the free tier, **the Premium Version of the application explicitly encrypts all data** transmitted between the local computer, the cloud node (`://machuzu.com`), and all other network nodes on external computers. Upgrading to the Premium tier ensures comprehensive end-to-end data encryption across the entire network topology.
- **Cloud Certificate Security Mechanism:** To validate and protect transactions, the local computer establishes a secure transport layer by leveraging the official cloud certificate (`machuzu.com`) stored locally within the application's `/crypto` folder. The application accesses this keystore to securely sign outbound payloads, perform mutual authentication, and establish encrypted handshakes with the centralized cloud node. This cryptographic binding verifies that all local application activities are securely tied to the authorized domain structure.
- **Local Immutability Risks:**
 - **Local Inception of Immutability:** Structural data permanence begins locally on the host machine within the integrated ImmuDB database layer.
 - **Permanent Records:** Once a blockchain record—such as a user identity or a sovereign trace record—is saved to the local ledger, those records cannot be altered, overwritten, or deleted by any administrative privilege level. Users assume full responsibility for data entry accuracy, as faulty or erroneous identity entries are permanent.
- **Distributed Network Transparency & Decentralisation Benefits:**
 - **Shared Ledger Architecture:** Saved data records are intentionally shared, replicated, and synced across all participant nodes or active members belonging to a network.
 - **Benefits of Decentralisation:** This distributed design removes single points of failure, ensuring that network operations remain uninterrupted even if individual host computers disconnect. Replicating identity and trace records across all nodes ensures high system availability, transparent peer validation, and resilience against malicious database modification attempts on any single terminal.
- **Peer-to-Peer Key Exchange:** Because network expansion relies on the manual sharing of system-generated alphanumeric keys (e.g., via external email pipelines), the user assumes all risks associated with the interception, misuse, or unauthorized distribution of active peer keys.

4. Customisation & Multijurisdictional Alignment

- **Tailored Regulatory Integration:** Licensee acknowledges that the core Software framework can be extensively customized, modified, and reconfigured by Licensor to meet the specific requirements of potential enterprise clients.
- **Legal Alignment:** Upon formal commercial engagement, Maestro IT (Pty) Ltd can structurally align the application's data retention, cryptographic protocols, identity modules, and compliance workflows with the national, local, or international laws governing a client's specific jurisdiction. This includes, but is not limited to, cross-border data transfer limitations, specialized localized privacy acts, and regional financial or electronic record keeping standards.

5. Privacy, Hosting & Regulatory Compliance (Eswatini Data Protection Act)

- **Secure Cloud Hosting Environment:** Maestro IT (Pty) Ltd declares that all application data routed to or interacting with the cloud node (`://machuzu.com`) is hosted within a highly secure, professional web hosting environment equipped with enterprise-grade logical controls and boundary defenses.
- **Absolute Third-Party Non-Disclosure:** In accordance with strict confidentiality protocols, **no user data processed by the Software or hosted on the cloud node shall be sold, shared, leaked, or disclosed to any third party.** This restriction applies universally, **regardless of whether the data is encrypted on the Premium version** or running unencrypted on the free tier.
- **Eswatini Statutory Alignment:** This privacy policy and all data handling operations executed by the proprietary software are structured to maintain complete alignment with the **Eswatini Data Protection Act, No. 5 of 2022**. Licensor operates as a responsible custodian of information, implementing technical security measures to safeguard data subject rights, protect lawful processing paths, and prevent unauthorized access or disclosure in full compliance with the laws of the Kingdom of Eswatini.
- **Sovereign Record Privacy Notice:** Because the core architecture utilizes permanent distributed ledgers, the User acknowledges that identity and sovereign trace records saved to the network cannot be structurally deleted or wiped. Users must ensure they have obtained explicit valid consents from data subjects before compiling or distributing any third-party personal information across peer nodes.

6. Integrity Commitment & Reputation Assurance

- **No Damaging Files:** Maestro IT (Pty) Ltd proudly reaffirms its status as a highly **upstanding, ethical corporate entity.** The company maintains an unyielding commitment to software safety and product security.
- **Reputation Shield:** Licensor shall under no circumstances compromise its commercial standing, brand equity, or public reputation by deliberately compiling,

introducing, or distributing malicious files, spyware, ransomware, or damaging code within `Machuzu-Next-Gen.jar` Or `LaunchMachuzuNextGen.bat`.

7. Limitation of Liability & Warranty Disclaimer

- **"As-Is" Provision:** THE COVERED SOFTWARE (`Machuzu-Next-Gen.jar` and `LaunchMachuzuNextGen.bat`) IS PROVIDED ON AN "AS-IS" AND "AS-AVAILABLE" BASIS, WITH ALL FAULTS. This clause represents a standard allocation of legal risk; it does not indicate or imply that the software contains active errors, defects, or malicious components.
- **Liability Exclusions:** TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL MAESTRO IT (PTY) LTD BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES WHATEVER, INCLUDING BUT NOT LIMITED TO LOSS OF DATA, INTERCEPTED DATA TRANSMISSIONS ON THE FREE TIER, SYSTEM DOWNTIME, OR SYSTEM CONFLICTS ARISING FROM THE ACQUISITION, UPGRADE, OR FAILURE OF EXTERNAL THIRD-PARTY UTILITIES.

8. Monitoring, Security Operations & Incident Reporting

- **Strange Occurrences:** If you experience any system anomalies, unauthorized network breaches, unencrypted traffic exposure on the free tier, or wish to submit support questions regarding your setup, you must immediately contact our technical operations gateway.
- **Dedicated Contact Portal:** All structural incident reports, operational feedback, bug tracking logs, and general administrative communications must be routed directly via email to:

wandile@machuzu.com