Description of Request	Request to purchase Multimedia software subscription licenses for a period of 5 years

1. High level background

Multimedia software is a suite of tools designed to enable users to view, edit, and combine multiple forms of digital media into cohesive outputs. It encompasses applications for graphic design, video editing, photography, animation, audio production, and web development, providing a versatile platform for creative and professional work. The primary purpose of multimedia software is to enhance communication, storytelling, and productivity by integrating diverse media types into a single deliverable.

Multimedia software enhances organizational competitiveness by empowering teams to produce professional, high-quality outputs that reinforce brand image, improve stakeholder engagement, and sustain customer trust in a dynamic business environment.

To maximize efficiency and accessibility, a **concurrent license model** would be preferable, allowing multiple users to leverage the software as needed without being restricted to individual device-based licenses.

2. Scope of work/Business requirements

Detailed description and volumes of the product/service requested:

50 x Multimedia software subscription for:

- File editing and conversion (video and photo)
- Web design/development
- Graphic design
- Cloud integration (can be disabled)
- MS Office integration/export (example: PowerPoint)

2.1. Security Requirements

2.1.1. The Tenderer shall have a valid International Organization for Standardization (ISO) 27001 certificate

2.1.2. The solution shall be able to integrate with existing Eskom's identity providers (IdP's) such as Microsoft (MS) Active Directory (AD), Entra Identity (ID) and shall support Security Assertion Markup Language (SAML) 2.0, Open Authorization (OAuth) 2.0 and OAuth 2.1 to enable Multi-Factor Authentication (MFA) and Single Sign-On (SSO)

2.1.3. The solution shall employ Role-based access control (RBAC) mechanism

2.1.4. The solution shall be able to onboard privileged accounts onto Privileged Access Management (PAM) tools, such as CyberArk but not limited to onboard privileged accounts to securely manage, rotate passwords, monitor, record sessions, control, enforce access to privileged accounts, auditing and reporting capabilities

2.1.5. Data at rest to be encrypted using at minimum Advanced Encryption Standard (AES)-256 and in transit (or in motion) using at minimum Transport Layer Security (TLS) 1.3 or later version

2.1.6. Data shall be secured at minimum using a Secure Hash Algorithm (SHA)-256 for data integrity, securing transactions, and messages

2.1.7. Audit trails, logs, user administration and user activity logs shall be enabled, encrypted, and securely kept with limited access to administrators

2.1.8. Sensitive information such as personal identifiable information (PII) data in non-production environments shall be masked

2.1.9. Incremental daily back-ups shall be done, encrypted, and securely kept offsite only for all critical systems

2.1.10. Real-time data synchronization or data replication to a secondary or disaster recovery (DR) site, located in different regions, shall be employed only for critical systems

2.1.11. Disaster Recovery Plan (DRP) shall be defined, annually tested, and such DRP test results shall be shared with the Eskom Cybersecurity team only for critical systems

2.1.12. A back-up Restore Plan and Procedure shall be defined, annually tested, and such test results shall be shared with Eskom's Cyber Security team

2.1.13. Patch Management Process shall be defined. The software updates and patches shall be tested in a non-production environment before being deployed into the production (PROD) environment

2.1.14. The database shall be placed behind the perimeter firewall

2.1.15. The solution shall support the prevailing enterprise services bus (ESB), application programmable interfaces (API's) and Integration Platform as a Service (iPaaS) platforms for security, logging and monitoring

2.1.16. The on-premises System and Cloud Service shall be able to integrate with Security Information and Event Management (SIEM) standard technologies such as Syslog, Windows event logging, Simple Network Management Protocol (SNMP) and Application Programming Interface (API) but not limited to these technologies listed

2.2. Solution Testing

The solution will undergo comprehensive testing following Eskom's standards to ensure its completeness and authenticity. The testing team is responsible for gathering testing requirements, creating test cases, and executing the tests to thoroughly evaluate the solution for deployment within Eskom's IT environment.
Please note that the following:

- All testing, except unit testing, will be carried out by the Eskom testing team. The tenderer is responsible for conducting unit testing.
- All testing (including unit testing) must be performed within Eskom's test management systems, such as Application Lifecycle Management (ALM), LoadRunner (for performance testing), and Unified Functional Tester (UFT). The implementation team must coordinate with the testing team to ensure sufficient time is allocated for testing, and that all testing activities are incorporated into the project schedule.
- Before the official test cycle begins, the development team must provide unit test results, adhering to the entry and exit criteria outlined in the master system test plan. A signed-off test closure report is required before marking any test milestone as complete.

The following tests and milestones must be completed:

- **Unit Testing (Development Environment):** Results provided by the tenderer's development team.
- **System Integration Testing & Functionality Testing (QA Environment):** This includes end-to-end functional testing and integration testing, ensuring the solution works with other systems and meets all requirements. The Eskom testing team will lead and execute this testing, while the tenderer's team must provide necessary inputs.
- **User Acceptance Testing (Pre-Prod Environment):** Facilitated by the testing team but executed by Eskom's customer/business team to verify that the system meets the requirements defined in the BRS for completeness and authenticity.
- **Non-Functional/Performance Testing (Pre-Prod Environment):** Led and executed by the performance tester.
- **Disaster Recovery Testing (for the on-premise option).** Led and executed by the Disaster recovery team.

All testing requirements must cover all identified interfaces that have been identified. The testing team must adhere to the Testing Centre of Excellence (TCoE) standard document provided as part of the RFP documentation

2.3. Training/Transfer of skills:

Online Browser Training
Internal application help/training (example: similar to MS Office)

3. Service Level Agreement requirements

The contract is license-only, performance is monitored through license entitlement verification, usage review, and commercial reconciliation, this approach can support Audit compliance.

- Verification that the contracted number of licenses is provisioned and accessible
- Confirmation that licensed features listed in the Scope of Work are available
- Periodic license usage and consumption reporting
- Reconciliation of invoices against active licenses and entitlements
- Review of vendor standard availability commitments as published in the subscription terms