

SCHEDULE R – INFORMATION SECURITY REQUIREMENTS

This document contains confidential and proprietary information of Eskom and is “Eskom Confidential Information” for the purposes of the non-disclosure agreement entered into between Eskom and the Supplier in relation to this Project. It is furnished for contract evaluation and award purposes only. Except with the express prior written permission of Eskom, this document and the information contained herein may not be published, disclosed, or used for any other purpose.

INSTRUCTIONS FOR RESPONDING TO THIS DOCUMENT:

General Guidelines

- These RFP documents contain the key legal terms and conditions that the Supplier will be required to comply with in relation to this Project.
- Eskom requires the Supplier to comply with the requirements as written, and compliance with these RFP documents will be a critical component of the Supplier’s response to the RFP.
- The Supplier must complete Schedule Q (Supplementary Terms), as it is a mandatory requirement. Non-compliance will result in the Supplier being disqualified from further evaluation.

1. INFORMATION SECURITY REQUIREMENTS

- 1.1. This Schedule R (Information Security Requirements) sets out the minimum information security, confidentiality, privacy, and cyber-resilience obligations that the Supplier must comply with in connection with the Services. The Parties acknowledge that the protection of Eskom Data, systems, and information assets is critical to the delivery of the Services and to Eskom's ability to meet its legal, regulatory, and operational obligations.
- 1.2. These requirements are intended to ensure that:
 - 1.2.1. Eskom Data and systems are safeguarded from unauthorised access, disclosure, alteration, destruction, or misuse;
 - 1.2.2. security measures are aligned to prevailing international standards and Good Industry Practice; and
 - 1.2.3. the Supplier's Subcontractors, agents, and Personnel implement equivalent standards of protection when handling Eskom Data or accessing Eskom systems.
- 1.3. The Supplier's obligations under this Schedule apply in addition to, and not in substitution of, the Supplier's general obligations under the Agreement (including the Terms and Conditions, Schedule Q (Supplementary Terms), and Schedule P (Operator Agreement). Where there is any inconsistency, the obligation that affords Eskom the greater degree of security and protection shall prevail.
- 1.4. Information Security management aims to ensure the confidentiality, integrity and availability of an organization's information, data and IT services.
- 1.5. Information Security management is led and overseen by Eskom's IT Security Services Team, which is responsible for the end-to-end coordination and comprehensive management of Information Security Services across Eskom and its subsidiaries.

2. SECURITY OBLIGATIONS

- 2.1. In performing the Services, the Supplier shall implement and maintain a comprehensive, risk-based information security programme that is consistent with Good Industry Practice and the requirements of this Schedule R (Information Security Requirements). Without limiting the generality of the foregoing, the Supplier shall:

- 2.1.1. establish, document, and enforce security policies, standards, and procedures designed to protect Eskom Data and systems;
- 2.1.2. ensure that such policies and procedures are kept up to date to address emerging threats and vulnerabilities; and
- 2.1.3. demonstrate compliance with these obligations through reporting, certification, and audit rights as required by Eskom.
- 2.2. These security obligations remain in effect throughout the entire Term, including any Transition, Transformation, or Exit Assistance periods, and extend to all Subcontractors and Third Parties engaged by the Supplier in connection with the Services.
- 2.3. All Eskom governance procedures, including but not limited to, architectural submissions and related requirements, must be complied with prior to implementation of any solution.
- 2.4. In addition to the above, the Supplier shall:
 - 2.4.1. maintain compliance with applicable information security frameworks, standards, and controls, including ISO 27001, SOC 2, the NIST Cybersecurity Framework, or any equivalent framework approved by Eskom;
 - 2.4.2. comply with Eskom's security policies for user access and identity management, and enforce multi-factor authentication (MFA) and role-based access control (RBAC) for all administrative and user accounts;
 - 2.4.3. comply with Eskom's Privileged Access Control mechanisms in line with Eskom's Privileged Access Management solution;
 - 2.4.4. adhere to all relevant privacy regulations, including POPIA;
 - 2.4.5. perform annual penetration testing and quarterly vulnerability scans, covering infrastructure, applications, and APIs;
 - 2.4.6. provide Eskom with remediation reports and confirm closure of high and critical vulnerabilities within the defined SLAs;
 - 2.4.7. specify and implement encryption standards for data at rest, in transit, and during processing, in line with post-quantum cryptography and the Eskom Encryption Standard. The Supplier is expected to demonstrate readiness or provide a roadmap aligned with NIST IR 8547;

- 2.4.8. ensure that its subcontractors and vendors meet the same security standards and comply with Eskom's security standards on third-party access management;
- 2.4.9. develop, implement, and maintain effective incident response procedures and protocols for the detection, reporting, management, containment, investigation, remediation, and closure of actual or suspected cyber incidents, security incidents, or security breaches;
- 2.4.10. notify Eskom within 24 (twenty-four) hours of becoming aware of any actual or suspected cyber incident, security incident, or security breach, and provide Eskom with an initial incident report;
- 2.4.11. provide further updates, evidence, remediation reports, and closure confirmation as reasonably required by Eskom and in accordance with Eskom's incident management process;
- 2.4.12. undergo Eskom's annual security assessments that may include penetration testing, vulnerability management assessment, and continuous monitoring assessments;
- 2.4.13. be liable for security breaches resulting from negligence and shall indemnify Eskom against any resulting damages;
- 2.4.14. establish and document procedures for the secure deletion of all Eskom Data, in full compliance with the applicable data retention policies upon contract termination;
- 2.4.15. comply with Eskom's cybersecurity policies, standards, and procedures;
- 2.4.16. educate employees on cyber threats, phishing, and cybersecurity best practices, and ensure cybersecurity training for personnel assigned to Eskom-related work, with emphasis on personnel handling Eskom-classified information;
- 2.4.17. ensure that its security monitoring services integrate with Eskom's Security Incident and Event Management solution;
- 2.4.18. provide Eskom with evidence and information required for investigations and intelligence services, in compliance with legal requirements;
- 2.4.19. ensure that any infrastructure and infrastructure components used by the Supplier to perform the Services for Eskom are secured to prevent security risks to the Eskom environment and are fully patched. Infrastructure refers to the essential

systems, assets, and technologies, both physical and digital, that are vital for the functioning of Eskom. If these systems are disrupted, it could cause significant harm to security, public safety, business operations, or national stability;

- 2.4.20. ensure data protection services that support secure data life-cycle management, data leakage prevention, and intellectual property protection for the services to be rendered to Eskom;
- 2.4.21. ensure that the security of the facilities hosting infrastructure used to deliver services to Eskom complies with Eskom's policies;
- 2.4.22. be responsible for promptly informing the Eskom Information Security Manager within 48 (forty-eight) hours of becoming aware of any risks or vulnerabilities, in accordance with Eskom's risk management process;
- 2.4.23. inform Eskom within 48 (forty-eight) hours if any personnel assigned to Eskom-related work resign, retire, or are suspended from their organisation;
- 2.4.24. ensure that all designated personnel complete a security screening or vetting process prior to commencing Services for Eskom or being deployed to an Eskom site, and that the results are shared with Eskom. The requirement for the vetting and screening process is set out in Annexure R-1 "Security Vetting and Screening";
- 2.4.25. develop and submit solution design documents to Eskom for architectural review and approval by the relevant governance committees;
- 2.4.26. provide the necessary personal information documents, including a signed Non-Disclosure Agreement, to Eskom to facilitate the registration of the Supplier's employees on the Eskom network; and
- 2.4.27. compile and deliver a monthly report outlining the cybersecurity posture and the status of related services.

Annexure R-1: Security Vetting and Screening

1. To ensure timeous access, as required by Eskom, the Supplier is responsible for performing its own screening, as well as preparing for and supporting the Vetting Fieldwork Unit's requirements described in this clause and within the scope of Services. This includes security vetting and/or screening of any individuals under the Supplier's control or employment who execute the Services from time to time during the Term.
2. The Supplier shall submit all required documents, certificates, and records for security vetting to Eskom's Vetting Fieldwork Unit or the State Security Agency relating to its business, owners, directors, executives, members, subcontractors, employees, and any individual requiring access to Eskom's sites, systems, or information. The Supplier acknowledges that additional or updated documentation may be requested at any time in response to security concerns and risk assessments.
3. The Supplier shall ensure that any criminal record verification certificates submitted are issued by a reputable screening entity accredited by the South African Police Service and are not older than four weeks at the time of submission and remain valid for the entire duration of the individual's access. The Supplier is responsible for submitting all criminal record verification certificates or outcomes to Eskom's Vetting Fieldwork Unit for authenticity verification. If any criminal record verification certificate or outcome is found to be fraudulent, cancelled, withdrawn, invalidated, amended, expired, or if a criminal conviction, including one under appeal, is identified against any individual requiring access, Eskom, upon recommendation from its Vetting Fieldwork Unit, reserves the right to instruct the Supplier to immediately remove and/or block such individual from accessing any Eskom site, installation, system, or information, and to ensure that the individual has no further involvement with the Services.
4. The Supplier shall be solely responsible for all costs associated with obtaining and submitting identifying documents, certificates, and any other records specified in this clause and in the scope of the Services, as may be required for security vetting and/or screening and clearance processes, including any updated or additional documents requested.
5. If the outcome of the vetting and/or screening investigations is unfavourable, or if security clearance is denied, the Supplier shall have the right to lodge an appeal against the outcome within 60 (sixty) days from the date on which notification of the outcome is received.