ANNEXURE A

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

During the subsistance of the contract, the Service Provider will be entrusted with the Road Accident Fund's (RAF) confidential, private, personal or sensitive information ('referred to herein as files, data and or documents).

The Service Provider shall have such policies in place to comply with RAF requirements as well as the provisions of the Protection of Personal Information Act, 4 of 2013.

The Service Provider shall therefore implement the following measures *inter alia*:

1.1 Document Handling and Transportation

The Service Provider must have protocols in place to ensure proper handling and transport of files to and from the Service Provider 's premises. The Service Provider must have a secure transportation system (lockable) to transfer files to and from the premises.

1.1.1 Security Measures

During handling and transportation, the files must be kept in lockable containers or packaging to prevent loss, theft, or damage of whatsoever nature.

1.1.2 Record Keeping

The Service Provider should maintain accurate records of each document stored, including its location, access history, and retention schedule. The records should be organised in a way that allows for easy and accurate tracking of each document.

1.2 Document Retrieval and Handling

1.2.1 Secure Retrieval

The Service Provider should use secure protocols for retrieving the documents, including verifying the identity of the requester and ensuring that the documents and records are transported securely.

1.2.2 Record Keeping

The Service Provider should maintain a detailed record of all retrieval activities, including the date and time of the activity, the identity of the requester, and the reason for the activity.

1.2.3 Secure Storage

The physical documents and records should be stored in lockable cabinets to prevent unauthorised access or tampering.

1.2.4 Access Control

The physical documents and records should be accessible only to authorised personnel, and the Service Provider should have policies and procedures in place to ensure that access is controlled and monitored.

1.2.5 Fire Suppression

The Service Provider's premises should have a fire suppression system or similar in place, fire extinguishers with carbon dioxide, to prevent damage or loss of documents and records in the event of a fire.

1.3 Security including secure facility.

The Service Provider 's premises should have a secure perimeter with controlled access and or surveillance systems. The premises should have secure doors, locks, and alarms to prevent unauthorised access.

1.3.1 Physical Security

The Service Provider must have physical security measures in place to ensure the safety and security of the documents, including controlled access points, surveillance cameras, and or 24/7 security monitoring. The Service Provider must always ensure the physical security of records in their possession. All document storage facilities must be adequately protected against unauthorised access. Should there be any real, attempted, or suspected breach of physical security the Service Provider will be obliged to inform the RAF and provide any CCTV footage, police report and linked alarm system records of the incident.

1.3.2 Document Access Control

Access to the documents and records must be controlled, with only authorised personnel permitted to handle, view, or transport the documents.

1.3.3 Access Monitoring and Control

The Service Provider must have access monitoring and control procedures in place to ensure that only authorised personnel are granted access to the documents and records and the storage facility.

Initial here

1.3.4 Network Security

The digital document storage systems must have appropriate technical security measures in place, such as firewalls, intrusion detection, and encryption, to protect against unauthorised access or attacks.

1.3.5 Access Control

- Grant access on a need-to-know basis.
- Use strong authentication methods to control access to systems and data.
- Regularly review and update access permissions.

1.3.6 Data Protection Obligations

- The Service Provider must handle and process personal and sensitive data in compliance with applicable data protection laws and regulations.
- Implement measures to safeguard data against unauthorised access, disclosure, alteration, and destruction.
- Inform the RAF immediately of any data breaches or incidents that may impact the security of the information.
- The Service Provider shall implement appropriate measures designed to ensure the confidentiality of personal, confidential and sensitive date, including by imposing confidentiality obligations on any of its agents or subcontractors, or any third party who has received records.

  Comply fully with the respective legislative and regulatory frameworks in the processing of personal information.
- Third-party service providers that handle PII on behalf of the organization should be screening or vetted for their data protection policies and procedures and should be required to sign a data protection agreement.
- Raf reserve the right to conduct security screening or vetting for company directors and resources provided.

1.3.7 Cybersecurity Standards:

- The Service Provider is required to implement robust cybersecurity measures to protect against cyber threats, including but not limited to malware, phishing, and unauthorised access.
- Use encryption for data in transit and at rest to ensure the confidentiality of sensitive information. Utilise encryption protocols and algorithms that comply with industry standards.

Initial here

- Regularly update and patch systems, software, and applications to address security vulnerabilities.

1.3.8 Incident Reporting and Response:

- The Service Provider must have a documented incident response plan to address and mitigate data breaches promptly.
- The Service Provider must report any security incidents or data breaches to RAF in a timely manner.

1.3.9 Subcontractors and Third-Party Oversight

- If subcontractors are engaged, the Service Provider must ensure that they also adhere to the same data protection and cybersecurity standards outlined in this policy.
- The Service Provider is responsible for the actions and compliance of any sub-contractors or third parties engaged in providing services to the RAF.

1.3.10 Audit and Monitoring

- The RAF reserves the right to audit and monitor the Service Provider ’s compliance with this policy.
- The Service Provider must cooperate with any audits or assessments conducted by RAF to evaluate compliance with data protection and cybersecurity standards.

Initial here