SIBANYE STILLWATER SHARED SERVICES OPERATOR AGREEMENT

1. RECITALS

Sibanye Stillwater Shared Services ("the Responsible Party")

and

Endleleni Marketing (Pty) Ltd
_____ ("the Operator"),

Vendor number _____

entered into an agreement where the Operator's scope of work includes the Processing of Personal Information, requiring an Operator Agreement to be entered into.

2. DEFINITIONS

2.1. **Binding Corporate Rules** means the Personal Information processing policies, within a group of undertakings, which are adhered to by a Responsible Party or Operator within that group of undertakings when transferring Personal Information to a Responsible Party or Operator within that same group of undertakings in a foreign country;

2.2. "**Data Subject**" means the person to whom the Personal Information relates;

2.3. "**Operator**" means the person who processes personal information for the Responsible Party in terms of a contract or mandate, without coming under the direct authority of the Responsible Party. For purposes of this Agreement means the Operator as defined and any authorised subcontractor of that party;

2.4. **"Main Contract"** means the primary supply agreement between the Operator and the Responsible Party

2.5. "**Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including:

2.5.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.5.2. dissemination by means of transmission, distribution or making available in any other form; or

2.5.3. merging, linking, as well as restriction, degradation, erasure or destruction of Personal Information, the details of which are set out in Schedule 1;

2.6. "**Processing Instructions**" means any actions relating to the Processing of Personal Information by the Operator, in relation to the services of the Operator;

2.7. "**Responsible Party**" is the party defined on the cover page and who alone or in conjunction with others determines the purpose of and means for processing personal information; and

2.8. "**Security Compromise**" occurs where there are reasonable grounds to believe that Personal Information of a Data Subject has been accessed or acquired by an unauthorised person with reference to the Operator's Processing of the Personal Information.

3. OPERATOR CLAUSE

3.1. Processing by the Operator

3.1.1. The Operator will Process Personal Information strictly in accordance with this Operator Agreement and Processing Instructions.

3.1.2. The Operator acknowledges and agrees that the Responsible Party retains all right, title and interest in and to the Personal Information and that the Personal Information shall constitute the Responsible Party's Confidential Information.

3.1.3. Unless required by law, the Operator shall Process the Personal Information only:

3.1.3.1. In compliance with the Main Contract; and

3.1.3.2. This Operator Agreement.

3.1.4. In the event where the Operator is unsure as to the parameters or lawfulness of the instructions issued by the Responsible Party, the Operator will, as soon as reasonably practicable, revert to the Responsible Party for the purpose of seeking clarification or further instructions.

3.1.5. The Operator shall co-operate and assist the Responsible Party with consultations with or notifications to relevant regulatory authorities and/or Data Subjects that the Responsible Party considers are relevant pursuant to POPIA in relation to the Personal Information.

3.1.6. The Operator shall treat all Personal Information as confidential and shall not disclose it without the prior written consent of the Responsible Party, unless required to do so by law.

3.1.7. Without limiting the Operator's obligations under this Contract, the Operator shall comply with the Responsible Party's data privacy and protection policies, applicable industry or professional rules and regulations, in relation to the safeguarding of Personal Information.

3.2. Security

3.2.1. The Operator undertakes to Process Personal Information in accordance with the POPIA requirements.

3.2.2. The Operator shall secure the integrity and confidentiality of Personal Information provided by the Responsible Party by taking appropriate, reasonable technical and organisational measures to prevent:

3.2.2.1. loss of, damage to or unauthorised destruction of Personal Information; and

3.2.2.2. unlawful access to or processing of Personal Information.

3.2.3. The Operator must take reasonable measures to:

3.2.3.1. identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

3.2.3.2. establish and maintain appropriate safeguards against the risks identified;

3.2.3.3. regularly verify that the safeguards are effectively implemented; and

3.2.3.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

3.2.4. The Operator must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

3.2.5. Within 5 (five) Business Days of a request from the Responsible Party, the Operator shall provide to the Responsible Party a written response and full details of the technical and organisational measures taken by or on behalf of

the Operator to demonstrate and ensure compliance with this Operator Security clause 2.2.

3.3. Security Compromise

3.3.1. The Operator shall notify the Responsible Party in writing immediately and in any event, no later than 24 (twenty-four) hours if there has been a Security Compromise. A Security Compromise notification can be sent to privacy@sibanyestillwater.com.

3.3.2. The Operator shall immediately upon becoming aware of the Security Compromise investigate the Security Compromise and furnish the Responsible Party with:

3.3.2.1. a preliminary report within 48 (forty eight) hours from its initial notification to the Responsible Party in terms of clause 2 above setting out the details, if available, of the Data Subjects affected by the Security Compromise and the nature and extent of the Security Compromise, details of the identity of the unauthorised person, if known, who may have accessed or acquired the Personal Information; and

3.3.2.2. daily reports on progress made at resolving the compromise.

3.3.3. The Operator shall take reasonable steps to mitigate the effects of the Security Compromise and to minimise any damage resulting from the Security Compromise and assist the Responsible Party in remediating or mitigating any potential damage from the Security Compromise to the extent that such remediation or mitigation is within the Operator's control as well as reasonable steps to prevent a recurrence of such a Security Compromise, including disciplinary proceedings against employees responsible for the Security Compromise and the removal of responsible employees from the performance of Services for the Responsible Party.

3.4. Operator Employees

The Operator shall:

3.4.1. restrict the dissemination of the Personal Information to only those of its employees who are actively involved in activities for which use of the Personal Information is authorised and then only on a "need to know" basis and the Operator shall initiate, maintain and monitor internal security procedures

reasonably acceptable to the Responsible Party to prevent unauthorised disclosure by its employees;

3.4.2. Ensure that its Employees will not Process Personal Information:

3.4.2.1 except in accordance with the provisions of the Main Contract; and

3.4.2.2 procure that its Employees are contractually obligated to maintain the security and confidentiality of any Personal Information and this obligation continues even after their engagement ends;

3.4.3. Take all reasonable steps to ensure the employees Processing Personal Information receive adequate training on compliance with this Operator Agreement and POPIA requirements applicable to the Processing of Personal Information.

3.5. Access Requests

3.5.1. The Operator shall provide the Responsible Party with full co-operation and assistance in relation to any requests for access to, correction of or complaints made by the Data Subjects relating to their Personal Information.

3.5.2. The Operator shall notify the Responsible Party in writing:

3.5.2.1. Within 3 (three) Business Days of receipt thereof, of any request for access to or correction of the Personal Information or complaints received by the Operator relating to the Responsible Party's obligations in terms of POPIA and provide the Responsible Party with full details of such request or complaint; and

3.5.2.2. Promptly of any legally binding request for disclosure of Personal Information or any other notice or communication that relates to the Processing of the Personal Information from any supervisory or governmental body.

3.6. Audit Rights

The Responsible Party's audit, compliance or ICT personnel may review the security safeguards of the Operator periodically or when there is a reasonable suspicion that the Operator is not complying with the provisions of this Operator Agreement or Main Contract or where there is a reasonable suspicion that the confidentiality, integrity and accessibility of Personal Information is likely to be compromised. The cost, or an audit will be for the account of the Operator unless it is a periodic audit. Such audit

rights shall include the right of access to systems, procedures and software, and inspection of the physical security of the Operator's premises.

3.7. Separation of Personal Information

The Operator shall Process the Personal Information in relation to the Services separately from Personal Information, data and property relating to the Operator or any third party and may not be combined or merged with information of another party unless otherwise agreed to in writing by the Responsible Party.

3.8. Return and Retention of Personal Information

3.8.1. The Responsible Party may, at any time on written request to the Operator, require that the Operator immediately return to it any Personal Information and may, in addition, require that the Operator furnish a written statement to the effect that upon such return, it has not retained in its possession or under its control, whether directly or indirectly, any such Personal Information or material.

3.8.2. Alternatively, the Operator shall, as and when required by the Responsible Party on written request, destroy all such Personal Information and material and furnish the Responsible Party with a certificate of destruction to the effect that the same has been destroyed, unless the law prohibits the Operator from doing so. In that case, the Operator agrees that it will maintain the confidentiality of the Personal Information and will not actively Process the Personal Information any further.

3.8.3. The Operator shall comply with any request in terms of this clause within 7 (seven) days of receipt of such request.

3.9. Subcontracting

3.9.1. The Responsible Party has the right to request at any time a copy, of the data processing agreements the Operator entered into with any subcontractor to process Personal Information in relation to this Operator Agreement.

3.9.2. The Responsible Party may require the Operator in writing to cease or suspend the processing of Personal Information by a subcontractor if, in the Responsible Party's reasonable opinion, the subcontractor is unable to comply with the terms of the subcontractor's agreement with the Operator or this Agreement.

3.10. Transborder Information Flow

3.10.1. In the event of any transborder information flow, the Operator hereby warrants and undertakes in favour of the Responsible Party that:

3.10.1.1. It shall procure the third party's compliance with all the obligations of this Operator Agreement insofar as the Processing of Personal Information by the third party is concerned;

3.10.1.2. The Operator shall at all times be responsible to the Responsible Party for fulfilment of all the Operator's obligations under this Operator Agreement and remain the Responsible Party's sole point of contact regarding the Services, including with respect to payment;

3.10.1.3. The third party is prevented from further transferring Personal Information to other third parties;

3.10.1.4. It shall ensure that the third party has implemented the appropriate technical and organisational security measures in the relevant jurisdiction in which the Personal Information is being transferred, as contained in Schedule 2; and

3.10.1.5. It has implemented and taken technical and organisational security measures to safeguard the security of the Personal information in-transit.

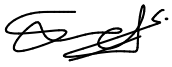
3.10.2. Where the Operator rely on its binding corporate rules as the lawful bases for transborder information flow, the Operator must demonstrate to the Responsible Party, evidence that the Operator is part of a group of undertakings as well as evidence of the group's binding corporate rules.

3.10.3. The Operator hereby agrees that the Responsible Party shall solely hold it responsible for the fulfilment of all obligations under this Operator Agreement and it hereby indemnifies and holds the Responsible Party harmless from any and all losses arising from any claim or action brought against the Responsible Party by any party, including by any regulator, arising from or due to the Operator's or any other party appointed by the Operator breach of the obligations contained in this Operator Agreement in relation to the lawful Processing of Personal Information in South Africa or anywhere else in the world.

3.11. Indemnity

Any limitation of liability set out in this Operator Agreement shall not apply to any breach of this Operator Clause.

SIGNED by the Parties and witnessed on 29 June 2025 **(date) at** Roodepoort **(place).**

On behalf of:	Name:	Designation:	Signature:	Date:
Sibanye-Stillwater: ***(Duly authorised hereto)***				
Witness 1:				
The Operator: ***(Duly authorised hereto)***	Kasaven Govender	Director		29 Jun 2025
Witness 2:	Sharon Naidoo	Personal Assistant		29 June 2025

Schedule 1 DETAILS OF THE PROCESSING PERSONAL INFORMATION

Purpose of Processing

1. Purpose [**Drafting note: Please insert the purpose for Processing the Personal Information.**]

2. Manner of processing [**Drafting note: Please insert the manner of processing the Personal Information.**]

The Personal Information Processed concern the following Data Subjects:

1. [**Drafting note: Please insert a list of the categories of Data Subjects.**]

    a. Staff – Existing and New recruits
    b. Suppliers – Existing and New Suppliers
    c. Clients – Existing and New that purchases core and non core products from Sibanye
    d. Optional – Community members
    e. Optional – Community Suppliers

2. Categories of data:-

    The Personal Information transferred concern the following categories of data:

    Business risk related

    Personal risk related

    Qualifications

    Certificates

    Memberships of organisations

    Drivers Licence

    Criminal – Fingerprints

    Medical

    Occupational Health & Safety

    Lifestyle Audits

    Physical Location

    RFP vetting

    Invoice Vetting

    [**Drafting note: Please insert a list of the categories of data which will be Processed.**]

3. Details of the Data Subject's Personal Information:

[**Drafting note: Please insert a list of the Personal Information data which will be Processed.**]

All verifications as per MIE schedule. Where MIE cannot source related check Endleleni Marketing has partnered with multiple suppliers.

No	ItemTypeName	EntityType
1	XDS Comprehensive	Person
2	Amended Summary of Findings	Person
3	Approved Fingerprint	Person
4	Assessment Feedback	Person
5	Asylum Seeker and Refugee Permit	Person
6	Bank Account Verification	Person
7	Basic Sales Screening Assessment	Person
8	Call Centre Customer Service Simulation Assessment	Person
9	Character Reference	Person
10	Citizenship	Person
11	Competency Assessment - Entry Level	Person
12	Competency Assessment - Executive Level	Person
13	Competency Assessment - Graduate Level	Person
14	Competency Assessment - Managerial Level	Person
15	Competency Assessment - Professional / Specialist Level	Person
16	Competency Assessment - Supervisory Level	Person
17	Comprehensive Sales Assessment	Person
18	Consumer Trace	Person
19	Criminal by AFIS - Premium Search	Person
20	Criminal by AFIS - Priority Search	Person
21	Criminal by AFIS - Standard Search	Person
22	Date of Naturalization	Person
23	Death Certification	Person
24	Department - Matric Symbol Match	Person
25	Digital Identity Verification	Person
26	Directorship Search	Person
27	Dofa Premium	Person
28	Dofa Standard	Person
29	Driver Accident History	Person
30	Drivers Licence	Person
31	Drivers Licence and Professional Drivers Permit	Person
32	Drivers Licence History	Person
33	Employment Confirmation	Person
34	Employment Recommendation	Person
35	Employment Reference - Executive	Person
36	Employment Reference - Standard	Person

37	Executive Level Individual Coaching	Person
38	Financial Sector Conduct Authority Approved Qualification	Person
39	Fingerprint Zone - Candidate Contact - Host	Person
40	Fingerprint Zone - Candidate Contact - Host (Pieter)	Person
41	Fingerprint Zone - Candidate Contact - Premium - South Africa	Person
42	Fingerprint Zone - Candidate Contact - Premium & IDV-Biometric Verification - South Africa	Person
43	Fingerprint Zone - Candidate Contact - Priority - South Africa	Person
44	Fingerprint Zone - Candidate Contact - Priority & IDV-Biometric Verification - South Africa	Person
45	Fingerprint Zone - Candidate Contact - Standard - South Africa	Person
46	Fingerprint Zone - Candidate Contact - Standard & IDV-Biometric Verification - South Africa	Person
47	Fingerprint Zone - Walk-In - Standard - South Africa	Person
48	Firearm Competency	Person
49	Firearm License	Person
50	Fit and Proper Summary	Person
51	Fraud Check	Person
52	ID Number Validation	Person
53	ID Verification with Photo - South Africa	Person
54	IDV-Biometric Verification - South Africa	Person
55	Institution Accreditation	Person
56	Integrity (IMI) – Answer Sheet (Entry level)	Person
57	Integrity (IP200) - Online link (Mid-Manage up)	Person
58	Junior Level Coaching	Person
59	Junior Level Individual Coaching	Person
60	Layered Voice Analysis Test	Person
61	Lifestyle & Conflict of Interest Report	Person
62	Marital Trace	Person
63	Media Search	Person
64	Middle Level Coaching	Person
65	Middle Level Individual Coaching	Person
66	Middle Level Team Coaching	Person
67	MIE Fingerprint	Person
68	NQF Level Confirmation	Person
69	OFAC Check	Person
70	OPQ32r – Occupational Personality Questionnaire (All levels)	Person
71	Passport Verification	Person
72	Permanent Residence Permit	Person
73	Professional Drivers Permit	Person
74	PSIRA Registration	Person
75	Qualification - Other	Person
76	Qualification General	Person
77	Qualification Matric	Person
78	Qualification Membership	Person
79	Quality Assurance	Person
80	Realtime ID Verification - South Africa	Person
81	Realtime ID Verification Snapshot - South Africa	Person
82	Revised Fit and Proper Summary	Person

83	Revised Summary of Findings	Person
84	SARS Individual Tax Clearance	Person
85	Screening History Overview	Person
86	Senior Level Individual Coaching	Person
87	Senior/Executive Level Coaching	Person
88	Senior/Executive Level Team Coaching	Person
89	Sequestration	Person
90	Sexual Offenders Clearance	Person
91	Sigma Combined Credit Check	Person
92	Sigma Combined Sequestration	Person
93	Sigma Comprehensive	Person
94	Sigma Notices	Person
95	Skills Assessment - Administrative	Person
96	Skills Assessment - IT	Person
97	Skills Assessment - Software	Person
98	Skills Assessment - Technical	Person
99	Social Media - Driver Verification	Person
100	Social Media Screening - Basic	Person
101	Summary of Findings	Person
102	Transunion Comprehensive	Person
103	Transunion Notices	Person
104	UMALUSI - Matric Symbol Match	Person
105	UN Security Sanction Check	Person
106	Vaccine Certificate Verification	Person
107	Vehicle Licence (Disk) Verification	Person
108	Visa Verification	Person
109	Voter Registration Status	Person
110	Work Permit	Person
111	World Check	Person
112	XDS Detailed Credit Check	Person
113	XDS Sequestration	Person

4. Details of the Data Subject's Special Personal Information:

[**Drafting note: Please insert a list of the Special Personal Information which will be transferred, this includes information relating to a person's race, religion, alleged criminal behaviour. Please note that special Personal Information has to be processed with the data subject's express consent.**]

As per MIE schedule aligned to Sibanye requirements. Where MIE cannot source related vetting Endleleni Marketing has partnered with multiple suppliers

Schedule 2 TECHNICAL SECURITY MEASURES

TECHNICAL QUESTIONNAIRE

Response:

1. **Not Applicable – based on service provided**
2. **Yes**
3. **Partially**
4. **No**

A. Operator confirmation	**Response**
1. Will accommodate an onsite visit from the Responsible Party for a security audit with 24 hours' notice.	**Yes**
2. Will store all personal information within South Africa - including backups. If "No", provide countries where the personal information is housed in the Response field.	**Yes if applicable**
3. Maintains an audit log of the location of all personal information and related backups.	**Yes**
4. Will not access the Responsible Party's personal information from outside of South Africa.	**Yes**
B. Policies, Standards and Procedures	**Response**
1. Has formal written Information Security Policies.	**Yes**
2. Will provide copies of the Information Security Policies to the Responsible Party on request.	**Yes**
3. Can provide results of a third-party external Information Security assessment conducted within the past 2 years (SAS-70, penetration. test, vulnerability assessment, etc.).	**Yes**
4. Maintains incident response procedures.	**Yes**
5. Has a policy to protect personal information against unauthorised access; whether stored, printed, spoken or transmitted.	**Yes**
6. Has a policy that prohibits sharing of individual user accounts and passwords.	**YEs**

7. Has a policy that implements the following Information Security concepts: need to know, least privilege and checks and balances.	**Yes**
8. Requires system administrators to be educated and qualified.	**Yes**
9. Implements AAA (Authentication, Authorisation, Accounting) for all users.	**Yes**
10. Performs background checks for individuals handling confidential information.	**Yes**
11. Has termination or job transfer procedures that would immediately protect unauthorised access to the Responsible Party's personal information.	**Yes**
12. Provides customer support with escalation procedures.	**Yes**
13. Has documented change control processes.	**Yes**
14. Requires sub-contractors, contractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer agreements.	**Yes**
15. Maintains a routine user Information Security awareness program.	**Yes**
16. Has a formal routine Information Security risk management program for risk assessments and risk management.	**Yes**
C. Architecture	**Response**
1. Will provide a network topology diagram/design.	**Yes**
2. Implements network firewall protection.	**Yes**
3. Implements web application firewall protection.	**Yes**
4. Implements host firewall protection.	**Yes**
5. Maintains routers and Access Control Lists (ACLs).	**Yes**
6. Provides network redundancy.	**Yes**
7. Has IDS/IPS technology implemented.	**Partially**
8. Uses DMZ architecture for Internet systems.	**Partially**

9. Adheres to the practice that web applications, which 'face' the Internet, are on a server different from the one that contains the database.	**Yes**
10. Uses enterprise virus protection on all systems.	**Yes**
11. Follows a program of enterprise patch management.	**Yes**
12. Provides dedicated customer servers to segregate data from other customer data. If not, then how is this accomplished in a secure virtual or segmented configuration.	**Yes**
13. Implements controls to restrict access to data from other customers.	**Yes**
14. Ensures that remote access is only possible over secure connections.	**Yes**
15. Uses separate physical and logical development, test and production environments and databases.	**Yes**
16. Secures development and test environments using, at a minimum, equivalent security controls as the production environment.	**Yes**
17. Has managed, secure access points on its wireless network.	**Yes**
D. Configurations	**Response**
1. Has implemented encryption for confidential information being transmitted on external or Internet connections with a strength of at least AES 256 bit or uses TLS 1.0, preferably TLS 1.1.	**Yes**
2. Has implemented encryption for confidential information at rest with a strength of at least AES 256 bit.	**Yes**
3. Has password-protected screen savers that activate automatically to prevent unauthorised access when idle, for computers used by system's support users.	**Not Applicable**
4. Removes all unnecessary services from computers.	**Not Applicable**
5. Uses file integrity monitoring software on servers (such as tripwire, etc.).	**Not Applicable**
6. Changes or disables all vendor-supplied default passwords or similar "published" access codes for all installed operating systems, database	**Yes**

management systems, network devices, application packages, and any other commercially produced Information Technology (IT) products.	
7. Uses passwords that are a minimum. of 8 characters, expire at least bi-annually and have complexity requirements.	**Yes**
8. Ensures that passwords are never stored in clear text or are easily decipherable.	**Yes**
9. Checks all systems and software to determine whether appropriate security settings are enabled.	**Yes**
10. Manages file and directory permissions following least privilege and need-to-know practices.	**Yes**
11. Implements redundancy or high availability for critical functions.	**Yes**
12. Authenticates all user access with either password, token or biometrics.	**Yes**
13. Formally approves, tests and logs all system changes.	**Yes**
14. Does not use production data for both development and testing, unless it has been declassified by the Company.	**Yes**
15. Uses artificial data in both development and test environments.	**Partially**
16. Limits access to development and test environments to personnel on a need to know basis.	**Yes**
17. Sets the account lockout feature for successive failed logon attempts on all system's support computers.	**Yes**
18. Prohibits split tunnelling when connecting to customer networks.	**Yes**
E. Product Design	**Response**
1. Ensures that if the product integrates with portable devices, confidential information is encrypted when stored on these portable devices and requires password access.	**Not Applicable**
2. Ensures that access to confidential information, across a public connection, is encrypted with a secured connection and requires user authentication.	**Yes**

3. Implements protections for Common Vulnerabilities and Exposures (CVEs) in a timely manner to protect from exploits.	**Yes**
4. Audits the application against the OWASP Top 10 Application Security Risks.	**Yes**
5. Ensures that application server and database software technologies are kept up-to-date with the latest security patches.	**Yes**
6. Uses threat modelling in their software development lifecycle (SDL).	**Yes**
7. Performs security code reviews as part of their Software Development Lifecycle (SDL).	**Yes**
8. Conducts OWASP code reviews for the Top 9 source code flaw categories as part of their SDL.	**Yes**
F. Application Security	**Response**
1. Uses industry standard best practices for application security (e.g. OWASP).	**Yes**
2. Will provide certificates of reviews applicable certification.	**Yes**
G. Access Control	**Response**
1. Immediately removes, or modifies access, when personnel terminate, transfer, or change job functions.	**Yes**
2. Achieves individual accountability by assigning unique IDs and prohibiting password sharing.	**Yes**
3. Ensures that critical data, or systems, are accessible by at least two trusted and authorised individuals, in order to limit having a single point of service failure.	**Yes**
4. Ensures that users have the authority to only read or modify those programs, or data, which are needed to perform their duties.	**Yes**
H. Monitoring	**Response**
1. Reviews access permissions monthly for all server files, databases, application, etc.	**Yes**

2. Implements system event logging on all servers and records at a minimum who, what, and when for all transactions.	**Yes**
3. Reviews and analyses after hours system accesses, at least monthly.	**Yes**
4. Review's system logs for failed logins, or failed access attempts monthly.	**Yes**
5. Reviews and removes dormant accounts on systems at least monthly.	**Yes**
6. Reviews web server logs weekly for possible intrusion attempts and daily for significant changes in log file size as an indicator of compromise.	**Yes**
7. Reviews network and firewall logs at least monthly.	**Yes**
8. Reviews wireless access logs at least monthly.	**Not Applicable**
9. Performs scanning for rogue access points at least quarterly.	**Not Applicable**
10. Actively manages Intrusion Detection- (IDS) and Intrusion Prevention Systems (IPS) and alert notifications have been implemented.	**Partially**
11. Performs vulnerability scanning at least quarterly. This is a mandatory requirement for all Small and Medium-sized Enterprises (SMEs).	**Yes**
12. Performs penetration testing at least annually, if the vendor manages any Personal Information on behalf of Company/Vendor. This is a mandatory requirement for all SMEs.	**Yes**
13. Checks routinely that password complexity is adhered to.	**Yes**
I. Physical Security	**Response**
1. Controls access to secure areas. E.g. key distribution management (both physical and electronic), paper/electronic logs, monitoring of facility doors, etc.	**Not Applicable**
2. Controls access to server rooms and follows least privilege and need-to-know practices for those facilities.	**Not Applicable**
3. Has special safeguards in place for computer rooms. e.g. cipher locks, restricted access, room access log, card swipe access control, etc.	**Not Applicable**

4. Shreds or incinerates printed confidential information.	**Not Applicable**
5. Prohibits or encrypts confidential information on laptops and mobile devices.	**Not Applicable**
6. Positions desktops, which display confidential information, in order to protect from unauthorised viewing.	**Not Applicable**
7. Escorts all visitors in computer rooms or server areas.	**Not Applicable**
8. Implements appropriate environmental controls, where possible, to manage equipment risks. E.g. fire safety, temperature, humidity, battery backup, etc.	**Not Applicable**
9. Has no external signage indicating the content or value of the server room or any room containing confidential customer information.	**Not Applicable**
10. Provides an export copy of all of the customer's data in a mutually agreed upon format at the end of the contract.	**Yes**
11. Follows forensically secure data destruction processes for confidential data on hard drives, tapes and removable media when it's no longer needed and at the end of the contract term.	**Yes**
J. Contingency	**Response**
1. Has a written contingency plan for mission critical computing operations.	**Yes**
2. Has emergency procedures and responsibilities documented and stored securely at multiple sites.	**Yes**
3. Reviews and updates the contingency plan at least annually.	**Yes**
4. Has identified computing services that must be provided within specified critical timeframes, in case of a disaster.	**Yes**
5. Has identified cross-functional dependencies, so as to determine how the failure in one system may negatively impact another one.	**Yes**
6. Has written backup procedures and processes.	**Yes**

7. Tests the integrity of backup media quarterly.	**Yes**
8. Stores backup media in a secure manner and controls access.	**Yes**
9. Maintains a documented and tested disaster recovery plan.	**Yes**
10. Uses off-site storage and has documented retrieval procedures for backups.	**Yes**
11. Password protects and encrypts all backups.	**Yes**
12. Provides rapid access to backup data.	**Yes**
13. Labels backup media appropriately, to avoid errors or data exposure.	**Yes**
K. Operator's Business Associates (including sub-contractors)	**Response**
1. Operator makes use of the services of business associates (including sub-contractors) in execution of this contract.	**Yes**
2. Non-disclosure agreements have been signed before proprietary and/or confidential information is disclosed to the Operator's business associates ((including sub-contractors).	**Yes**
3. Operator's business associate (including sub-contractors) contracts, or agreements, are in place and contain appropriate risk coverage for customer requirements.	**Yes**
4. Operator's business associates (including sub-contractors) are aware of customer security policies and what is required of them.	**Yes**
5. Operator's business associate (including sub-contractors) agreements document the agreed transfer of customer's data when the relationship terminates.	**Yes**