Cyber Risk Assessment Form – SME

Client Information	
Name of Organization:	EASTERN CAPE PARKS & TOURISM AGENCY
Company Website:	www.visiteasterncape.co.za
Principle Address:	17-25 FLEET STREET, EAST LONDON
Date of Establishment:	Last Year
Annual Revenue (ZAR):	Last Year
IT Security Spend (ZAR):	Last Year
Number of Employees:	
Business Description:	Accommodation, Tours & Activities, Hunting & Fishing
Business Type:	Public Sector

Are there any Joint Ventures (JVs) in place?	☐ Yes ☑No
Details of JVs:	
Were there any mergers and/or acquisitions in the past 5 years?	☐ Yes ☑ No
Details of M&A activity:	
Are you planning any M&A in the next year?	☐ Yes ☑ No
Details of proposed M&A:	
Are you a parent or subsidiary entity?	Subsidiary Entity
Provide details	

Data Security & Exposure		
Do you have a Chief Privacy Officer or equivalent?	☑Yes	☐ No
Do you have a group wide privacy policy?	☑Yes	☐ No
Do you have a data classification policy with associated security for sensitive data?	☑Yes	☐ No
Are sensitive data access & controls continuously monitored?	☑Yes	☐ No
What are the Frequency of your company backups?	Daily	
Please state which of the following you are required to be compliant with ☐ PCI-DSS ☐ FACTA ☐ HIPAA ☐ HITECH ☐ Gramm-Leach Act ☐ Other		
Please state what other data governance regulations you are required to be compliant with? • Protection of Personal Information Act (POPIA) • Public Finance Management Act(PFMA)		
Please state the number of Personal Identifiable Information Records currently stored/processed?		
Please state the number of Payment Card Information Records currently stored/processed?		
Please state the number of Protected Health Information Records/Medical Records currently stored/processed?		
Please state which of the following you are required to be compliant with? ☑South Africa ☐ USA ☐ Europe ☐ Canada ☐ Australia ☐ Other		
Please state other countries not listed above?		
Are you sharing data with any 3rd party?	☑ Yes	☐ No
Please provide details of 3rd parties whom you share data with?		

What are the data regulations of your shared parties? POPI POPIA

Security Policies		
Do you maintain any certified IT security standards?	☐ Yes	☑No
Please specify the applicable standards (e.g. NIST, ISO 27001)?		
Do you have a cyber threat intelligence function?	☑Yes	☐ No
Is regular penetration testing done by a 3rd party?	☑Yes	☐ No
Is there a process to remediate penetration test findings?	☑Yes	☐ No
Approximate date of last assessment?		
What were the remediation points identified?		
Are you doing any background verification tests on employees and/or 3rd party employees/users?	☑Yes	☐ No
Does your company accept card payments?	☑Yes	☐ No
Do your point-of-sale (POS) systems have anti-tampering?	☐ Yes	☑ No
Describe the encryption and tokenization process of data flow through the POS network:		
What is the frequency of 3rd party assessment of POS systems?	Choose an item.	
Are the POS and Corporate Network segregated?	☐ Yes	☑ No

Physical Security		
Do you have critical systems in dedicated rooms with restricted access and relevant alarms/protections?	☑Yes	☐ No
Does your data center hosting have resilient infrastructure for redundancy of power supply, air-con etc.?	☑Yes	☐ No
Are critical systems duplicated off-site?	☑Yes	☐ No

Are there fire detection and automatic fire suppression in critical IT areas?	☑Yes ☐ No
Is power supply protected by UPS/batteries and are they maintained regularly?	☑Yes ☐ No
Is a generator in place and maintained regularly?	☑Yes ☐ No
Third Party Exposure	
Please provide a list of third-party service providers? • SKG • Microsoft	
Did you conduct due diligence on these third parties?	☑Yes ☐ No
Please provide details on your due diligence practices for third parties?	
Do you regularly audit third party service providers?	☐ Yes ☐ No
Are on-demand services data stored on the cloud?	☑Yes ☐ No
Do you have contractual indemnities in place for a breach or network interruption?	☐ Yes ☐ No
Please provide details of contractual indemnities currently in place. • Service provider may not disclose any information they encounter while they do their work within the ECPTA. • The service providers must follow all the policies governing the ECPTA. • They must disconnected from the network after completing their work	
Does the existing Business Continuity Management (BCM)/Disaster Recovery (DR) plan factor third party service providers failure?	☑Yes ☐ No
Business Resilience	
Is there an impact to profit due to computer system failure?	☑Yes ☐ No
What is the downtime required to impact profit?	Days
Do you have a formal BCM/DR plan in place?	☑Yes ☐ No
What is the frequency of testing of BCM/DR plans?	Monthly
What are the Recovery Time Objectives (RTOs) for system restoration?	Hours
Do you log all security breaches?	☑Yes ☐ No
Does the incident response plan describe team roles and responsibilities?	☑Yes ☐ No
Have you suffered a cyber incident in the past 5 years?	☑Yes ☐ No

Please provide details of incidents experienced and remedial actions?	
Digital Media	
Is there a formal review process for offline & online content?	☑Yes ☐ No
Does the company make any use of copyrighted material provided by others?	☑Yes ☐ No
Does the company post on online forums?	☑Yes ☐ No
Is the company active on social media?	☑Yes ☐ No
Remote Working	
Do you provide formalized training for staff at least annually on Information Security?	☑Yes ☐ No
Are users required to regularly update passwords?	☑Yes ☐ No
Is the access authorization based on user roles?	☑Yes ☐ No
Is there a management procedure in place for user role access authorization?	☑Yes ☐ No
Do you have configuration preferences segmented by equipment (e.g. laptops, servers, mobile devices)?	☑Yes ☐ No
Are remote workers required to use a VPN to access the corporate network?	☑Yes ☐ No
Does remote access into the corporate network require multifactor authentication?	☑Yes ☐ No
Are security patches regularly deployed?	☑Yes ☐ No
Do you make use of internal & external firewalls?	☑Yes ☐ No
Do you make use of intrusion detection?	☑Yes ☐ No
Do you make use of proactive vulnerability scanning?	☑Yes ☐ No
Do you make use of anti-virus & anti-malware software?	☑Yes ☐ No
Does your password policy make provisions for complexity, length and avoiding re-use of used passwords?	☑Yes ☐ No
Do you have a patch management procedure?	☑Yes ☐ No
Do you use any unsupported systems and/or software?	☐ Yes ☑No
Does the change management policy include risk assessment, testing, authorization, roll back etc.?	☑Yes ☐ No
Do you allow Bring-Your-Own-Device?	☐ Yes ☑No

How is the BYOD process managed?	
Are USB privileges restricted?	☑Yes ☐ No

Overview of IT assets in the environment		
Asset count	**Type of Assets**	**Comments**
50	Internal Network Server's (server's and application server's)	All servers 50 servers are hosted on 3 different hosts
220	Desktop / Laptop's (Workstations)	All laptops are running on Windows 2010.
1	DMZ Server's (Servers and Application Servers, etc.)	We have a DMZ within our HQ firewall
6	Network Shared resources (File shares, Printers)	6 Leased Konica Minolta printers
12	Wireless Network and Wired Network Equipment (Network devices)	Running WPA3, Network Access 802.11
1	IPS / IDS and Antivirus Services	Antimalware services are installed on all client devices
1	Firewall	
0	Proxy Server	We do not make use of a proxy server. We make us of a reverse proxy for HTTPS traffic to specific web applications
0	SIEM Network Monitoring	
3	Web Portals	Secured through Azure MFA and permissions are generally located using the least use privileges
1	BYOD Network / Guest Network	Separate network that allows limited internet access
1	Security Systems (camera system)	Controlled and recorded on an NVR system. All devices are within a separate subnet.
0	Specialised Equipment connected to network	
0	ICS / SCADA Systems	

1	Cloud Based Systems	M365,Email,Communication tools Azure DR

Declaration & Notice
It is declared that to the best of the knowledge and belief of the client, after inquiry, that the statements and responses set out herein are true and accurate. You understand that you are under a duty to make a fair presentation of the risk to the insurer, and that all material circumstances that you are or ought to be aware of have been disclosed to the insurer, or failing that, sufficient information to put a prudent insurer on notice that further inquiries are needed. You understand that non-disclosure or misrepresentation of a material fact or matter may impact the terms of the policy or impact whether the policy responds in whole or in part to a claim. You undertake to inform the Insurers of any material alteration to the information provided herein or any new fact or matter that arises which may be relevant to the consideration of the proposal for insurance. You acknowledge and understand that we gather data (including Personal Information) from you for (i) the delivery of the Services; (ii) the management of our relationship with our clients, including the marketing of products or services to you which may be of interest to you, invoicing, the settlement of disputes and associated business administration; and (iii) the development of Aon Group's products and services (for example conducting benchmarking, market research, data analysis). You acknowledge that we may need to disclose your Personal Information to Insurers, their agents and consultants, other third parties and due to the global nature of services provided by us, Personal Information may be transmitted, used, stored and otherwise processed outside of the country in which it was submitted. You acknowledge that we may transfer your Personal Information outside the borders of South Africa for the purposes of rendering the Services. You hereby consent to the disclosure and transfer of your Personal Information as set out in this clause The undersigned is authorized by the applicant and declares that the statements set forth herein and all written statements and materials furnished to the underwriters in conjunction with this application are true.

Name of Director/Principal:	
Position:	
Date Completed:	
Digital Signature:	

This supplemental questionnaire is incorporated into and made part of any application for Cyber Risk coverage by the applicant. All representations and warranties made by applicant in connection with such application also apply to the information provided in this supplemental questionnaire.

Disclaimer

The information contained here in and the statements expressed should not be considered or construed as insurance broking advice and are of a general nature. The information is not intended to address the circumstances of any particular individual or entity. Accordingly, the information contained herein is provided with the understanding that Aon, its employees and related entities are not rendering insurance broking advice. As such, this should not be used as a substitute for consultation with an Aon Broker or Consultant.

Although we endeavour to provide accurate and current information and we use sources we consider reliable, Aon does not warrant, represent or guarantee the accuracy, adequacy, completeness or fitness for any purpose of the information and can accept no liability for any loss incurred in any way by any person who may rely on it. You should not act on such information without appropriate professional advice after a thorough examination of the particular situation. Aon reserves the right to change the content of this document at any time without prior notice. Descriptions, summaries or highlights of coverage do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy. This document has been compiled using information available to us at date of publication.

For further information on our capabilities, please visit: www.aon.co.za or www.aon.com

Aon South Africa (Pty) Ltd, an Authorised Financial Services Provider, FSP # 20555
Aon Re Africa (Pty) Ltd, an Authorised Financial Services Provider, FSP # 20658
Aon Limpopo (Pty) Ltd, an Authorised Financial Services Provider, FSP # 12339