Camargue

SME Cyber Risks

For companies with revenue between R1bn and R4bn

DECLARATION

I hereby declare that I am authorized to complete this application on behalf of the Proposer and that after due inquiry, to the best of my knowledge and belief, the statements and particulars in this application are true and complete and no material facts have been misstated, suppressed or omitted. I undertake to inform the Insurer of any material alteration or addition to these statements or particulars which occurs before the commencement of or during the period of insurance. I also acknowledge that this Application (together with other information supplied to Underwriters) shall be the basis of such contract. I understand that Underwriters will rely on the statements that I make on this form. In this context, any Insurance Coverage that may be issued based upon this form will be void if the form contains falsehoods, misrepresentations or omissions.

Privacy Statement

I/We consent to Camargue Underwriting Managers processing my/our personal information as per the Privacy Statement which may be accessed at https://www.camargueum.co.za/legal

NAME | **CAPACITY**

SIGNATURE OF THE PROPOSER | **DATE** DD/MM/YYYY

BROKER DETAILS

Broker:

Contact Person: Tel:

Email:

Camargue

SME Cyber Risks

For companies with revenue between R1bn and R4bn

GENERAL INFORMATION

Details of entities to be insured (the "Proposer"*):

Proposer's Name:

ID Number (if sole trader):

Physical Address:

Postal Code:

Company Registration Number: **VAT Number:**

Website:

Annual Revenue: **Number of Employees:**

Is 100% of Annual Revenue generated from South Africa?

If not, please advise percentage split per territory:

Main Business Description:

Please confirm the total number of Data Subjects that are retained within your networks, databases, and cloud-based servers at any one point in terms of employees, customers, and contractors/vendors:

** The "Proposer" means the prospective named insured and in answering the below questions and declaration, the "Proposer" means the named insured and all subsidiaries to be covered under the policy.*

REQUIRED COVER

State the Limit of Indemnity and First Amount Payable required:

Limit of Indemnity:	R	R	R
First Amount Payable:	R	R	R

Camargue

SME Cyber Risks

For companies with revenue between R1bn and R4bn

BUSINESS ACTIVITIES

1. **Is the Proposer:**

1.1	**A platform/app provider (or developer) for any of the following: Money/funds/securities transfer, cryptocurrencies/blockchain, crowd-funding, fundraising, political lobbying, direct/ targeted marketing, social media, dating, gaming, file sharing or content streaming?**	**YES**		**NO**
1.2	**Involved in: Adult entertainment, debt collection or the processing, storage or distribution of cannabis products?**	**YES**		**NO**

****If the Proposer has answered YES to either of the above, please note that these activities fall outside of our risk appetite, and we are not able to provide a quotation.****

SECURITY, CONTROLS AND RISK MANAGEMENT

1.	**Does the Proposer use Google Workspace, Microsoft 365 or other similar cloud-based infrastructure with the four network security best-practice guidelines listed in Question 2 enabled? (If YES, continue to Question 3)**	**YES**		**NO**

2. **Which of the following security best-practice guidelines does the Proposer have enabled on its network(s):**

2.1	**Filtering all incoming emails and communications for malicious links, spam, malware and attachments?**	**YES**		**NO**
2.2	**Multi-Factor Authentication for all user accounts?**	**YES**		**NO**
2.3	**Sender Policy Framework?**	**YES**		**NO**
2.4	**Endpoint Monitoring and anti-virus capability (If NO, answer below:)**	**YES**		**NO**
2.4.1	Does the Proposer use cloud security monitoring tooling/dashboards to ensure a secure configuration is being used? (If NO, answer below):	**YES**		**NO**
2.4.2	Please provide full details of compensatory controls:			

3. **Does the Proposer have the following protocols in place:**

3.1	**All system configuration and data is either (i) subject to regular Back-ups (at least weekly) via secure cloud or (ii) maintained in offline copies disconnected from the organisation's network?**	**YES**		**NO**
3.2	**Multi-Factor Authentication settings are enabled for access to Back-up files?**	**YES**		**NO**
3.3	**Data is encrypted while it is in transit?**	**YES**		**NO**
3.4	**Data is encrypted while at rest?**	**YES**		**NO**
3.5	**Data is encrypted at rest on portable devices?**	**YES**		**NO**
3.6	**Alerts from endpoint monitoring tools are reviewed at a regular cadence?**	**YES**		**NO**

4. Does the Proposer have processes in place to implement, within 14 days, critical security, anti-virus and malware patches/signatures received from commercial software vendors onto all of its servers, laptops, desktops, routers, firewalls, phones and other physical devices? (If NO, answer below:)

YES		NO	

4.1 Within how many days are critical security, anti-virus and malware patches received from commercial software vendors implemented on all physical devices?

No of days:	

5. Does the Proposer scan the external perimeter of the network?

YES		NO	

5.1 What is the frequency of the Vulnerability Scanning?

Daily		Weekly		Monthly		Quarterly		Other	

6. Does the Proposer have separate Administrative Accounts for tasks that require elevated privileges (such as TIER 0 and equivalents) with internet access restricted?

YES		NO	

7. Does the Proposer have a defined Incident Response process that would be triggered following an IT or cyber incident?

YES		NO	

8. Does the Proposer confirm that:

8.1 **None of its directors or officers are aware of any claims or circumstances that may give rise to a claim or loss under this proposed insurance, or would have given rise to a claim or loss under this proposed insurance had it been in force at the time, including any computer system intrusion, tampering, virus or malicious attack, loss of data, hacking incident, alleged data theft, unplanned outage or similar circumstances, which has exceeded R100,000 in total costs?**

YES		NO	

8.2 **It provides all employees with anti-fraud training at least annually (including but not limited to detecting social engineering, phishing simulation and security and privacy Awareness Training, business email compromise and other similar exposures); and before processing funds transfers and/or third-party account detail changes, confirm the transaction details with the requestor, through a "secondary means of communication"**?**

YES		NO	

***A "secondary means of communication" is different from the first means of communication. For example, if the request is received by telephone, a secondary communication may be an email.*

9. Only complete this question if the Proposer is involved in Manufacturing, Pharmaceuticals, Energy, Power, Rail, Transportation and Logistics, Mining or any other heavy industrial trade and if the Proposer has Operational Technology (OT).

9.1 **Does the Proposer operate any Operational Technology as part of their business operations? (If NO, do not complete this section)**

YES		NO	

9.2 **Is there a formal asset inventory for the OT environment?**

YES		NO	

9.3 **Are any OT assets directly accessible from the internet?**

YES		NO	

9.4 **Is there any remote access to the OT sites?**

YES		NO	

9.5 **What level of segmentation currently exists between IT and OT?**

VLAN		FW		DMZ		Data Diode		Air Gap		None/Other	

9.6 **When patches are applied is there a secure patching process in place?**

YES		NO	

9.7 **Are there Business Continuity Plans (BCP) in place for the business?**

YES		NO	

GLOSSARY OF TERMS

Administrative Accounts
A user account which has been assigned elevated administrative access rights, granting the user the authority to perform various administrative including the modification of critical systems settings, installation/uninstallation of software and change system configurations.

Awareness Training
A formal process for educating employees and stakeholders to understand, identify and avoid cyber threats.

Back-ups
A copy of data, files and programs made to facilitate recovery if necessary.

Data Subject
Any natural or juristic person who can be identified, directly or indirectly, via an identifier such as a name, ID number, address etc.

Encryption
A method by which information is converted into secret code that hides the information's true meaning.

Endpoint Monitoring
Endpoint monitoring involves the continuous observation and analysis of activities on endpoints, including user devices and servers, to identify and respond to security threats effectively.

Incident Response
Systematic and planned approach that organizations rely upon to identify, handle and recover from cyber threats.

Multi-Factor Authentication
A process in which a user authenticates themselves through two or more different means when gaining access to a computer system or web-based service. Typically use a password and a passcode, generated by a physical token device or software as the two factors.

Operational Technology
Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

Patch Management
Process of managing an IT network by regularly performing patch deployment to keep the network up to date. Each patch deployed is a set of changes to a computer program or its supporting data which is designed to update, fix or improve it to resolve vulnerabilities.

Sender Policy Framework (SPF)
An email authentication technique which is used to prevent spammers from sending messages on behalf of your domain.

Vulnerability Scanning
Formal description and evaluation of the vulnerabilities in an information system.

AUTHORISED FINANCIAL SERVICES PROVIDER, LICENCE NUMBER: 6344. APPROVED LLOYD'S COVERHOLDER PIN: 107824DRW
Camargue Underwriting Managers (Pty) Ltd. Co. Reg. No. 2000/028098/07.
33 Glenhove Road, Melrose Estate, 2196. Telephone: 011 778 9140, E-mail: camargue@camargueum.co.za, Website: **www.camargueum.co.za**.

UNDERWRITTEN BY THE LICENSED INSURERS:

Certain underwriters at **Lloyd's**

DATE SEP 2024