

CYBER RISKS

FOR COMPANIES WITH REVENUE MORE THAN R500M & THOSE REQUIRING TECH PI COVER

PROPOSAL FORM

IMPORTANT NOTICE

- Answer all questions leaving no blank spaces.
- If you have insufficient space to complete any of your answers, continue on your company letter head.
- It is the intention of underwriters that any contract of insurance with the proposer shall be based upon the answers and information provided in this proposal form and any other additional information provided by the proposer. If a quotation is offered, it will be the intention of underwriters to offer coverage only in respect of those entities named in answer to question 1.
- Completion of this proposal form does not bind the proposer nor insurer to complete the insurance transaction.
- Please ensure that a copy of your latest DRP (Disaster Recovery Plan) or BCP (Business Continuity Plan) is submitted with your proposal form, should you require insuring agreement 4 | Data Recovery and Loss of Business Income.
- Please find the following annexures at the end of the proposal form:
 - Annexure A - Glossary of Terms
 - Annexure B - Biometric Data
 - Annexure C - Operational Technology and Supply Chain Software
 - Annexure D - PCI DSS (Payment Card Industry Data Security Standard)

SECTION 1 | GENERAL INFORMATION

Details of entities to be insured (the “Proposer”):

Proposer’s Name	
Trading Name (if different from above)	
Registration / ID Number	
VAT Number	
Company Legal Constitution	<input type="checkbox"/> Partnership / <input type="checkbox"/> Private Company / <input type="checkbox"/> Public Company / <input type="checkbox"/> Close Corporation / <input type="checkbox"/> Non-profit Organisation / <input type="checkbox"/> Government / <input type="checkbox"/> Sole Proprietor
Date Company Established / Services Commenced (As currently constituted)	
Date Company Established / Services Commenced (As initially constituted)	
Physical Address (incl. Area Code)	
Practice/Trading Address(es) (if different from above)	
Website Address	
Telephone Number	
E-Mail	

1. Have you been involved in any mergers and/or acquisitions within the last three years? (If Yes, please provide further details):

 Yes No

2. Do you have Subsidiaries? (If Yes, please provide further details):

 Yes No

Name	Shareholding %	Nature of Activities	Location	No. of Staff
	%			
	%			
	%			

3. Is your network interconnected with a holding company and/or any Subsidiary?

 Yes No

(a) If Yes, is this holding company and/or Subsidiary covered under this policy?

 Yes No

SECTION 2 | INSURANCE HISTORY

1. Are you presently or have you in the past been insured for the type of insurance now being proposed?

 Yes No

If Yes, please state: Insurers:

Limit of Indemnity	R
First Amount Payable	R
Premium	R
Date of Cover Expiry	R
Retroactive Date	

2. For the type of insurance now being proposed, has any Insurer ever:

(a) Required an increased premium or imposed special terms?

 Yes No

(b) Refused to accept or renew any insurance for the body corporate?

 Yes No

(c) Cancelled the insurance?

 Yes No

If Yes to any of the above 3 questions, please provide full details:

SECTION 3 | REQUIRED COVER

1. State the Limit of Indemnity and First Amount Payable required:

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

2. Please mark which sections of the Cyber Risk offering you wish to incorporate within your policy:

Insuring Agreement 1 (Technology) Professional Services (Tech PI)	<input type="checkbox"/>
Insuring Agreement 2 Multimedia Liability (With Tech PI only)	<input type="checkbox"/>
Insuring Agreement 3 (Network) Security and Privacy Liability	<input type="checkbox"/>
Insuring Agreement 4 Data Recovery and Loss of Business Income	<input type="checkbox"/>
Insuring Agreement 5 Privacy Regulatory Defence and Penalties	<input type="checkbox"/>
Insuring Agreement 6 Crisis Management Costs	<input type="checkbox"/>
Insuring Agreement 7 Data Extortion	<input type="checkbox"/>

SECTION 4 | PREVIOUS LOSSES / EXISTING CIRCUMSTANCES

1. Is any principal, AFTER FULL ENQUIRY, aware of any circumstance which might:

- (a) Give rise to a claim against the proposer, any predecessor or any past or present principal? Yes No
- (b) Cause any loss to the proposer, any predecessor or any past or present principal? Yes No
- (c) Otherwise affect the consideration of this proposal for insurance? Yes No

If **Yes**, please provide details:

--	--

2. In respect of ANY of the risks to which this proposal relates, has any claim been made (whether successful or not) against the proposer or any past or present principal?

Yes No

If **Yes**, please provide details (including loss date, amount claimed and a brief description):

--	--

3. If **Yes**, to questions 1 or 2 above, what steps have been taken to prevent a recurrence?

--	--

4. Please indicate if any of the following has occurred over the past (5) years:

- | | | |
|---|------------------------------|-----------------------------|
| (a) Have you or any past or present principal, partner, director, or employee been disciplined for mishandling data or otherwise tampering with your computer network? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| (b) Have you or any past or present principal, partner, director, or employee been subject to any disciplinary action or governmental action or investigation as a result of professional activities? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| (c) Have you sustained any unscheduled network outage or interruption? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| (d) Have you suffered an intentional breach of IT security, network damage, system corruption or loss of data? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| (e) Have you sustained a material or significant system intrusion, tampering, virus or malicious code attack, loss of data, hacking incident, data theft or similar incident or situation? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| (f) Has any customer or other person or entity alleged that their personal information was compromised? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| (g) Have you notified customers that their information was or may have been compromised? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

If **Yes**, please provide details:

SECTION 5 | ACTIVITIES OF PROPOSER

What are your main services / activities?

--

SECTION 6 | FINANCIAL INFORMATION

1. Please provide the following figures and the respective financial year-end dates to which they refer:

	Previous Financial Year	Current Financial Year	Forthcoming Fin. Year
Date:	/ /	/ /	/ /
Gross Annual Revenue:	R	R	R
Net Income/Loss Before Tax:	R	R	R
Total Assets:	R	R	R

2. Value of gross annual revenue accounted for by sales or operations on your website:	R
---	---

3.	Number of annual transactions paid for by debit/credit card monthly			
4.	Are you compliant with the Payment Card Industry Data Security Standards (PCI DSS)?	N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
	If Yes, to what level?	1 <input type="checkbox"/>	2 <input type="checkbox"/>	3 <input type="checkbox"/>
	If applicable, please complete Annexure C at the end of the proposal form.			
5.	Average transaction value:	R		
6.	Percentage of last year's gross annual revenue generated from:			
	Client subject to RSA laws	%	Clients subject to USA/Canada laws	%
			Clients anywhere else in the world	%
	a) If revenue is generated from outside RSA and not subject to USA/Canada law, please indicate the countries from which revenue is generated			
	1. If revenue is generated from the USA/Canada, please state the percentage of revenue generated from each state			
7.	Estimate of total annual IT system budget:	R		
8.	Please confirm your total number of Employees:			
	Previous Financial Year	Current Financial Year		

SECTION 7 | ERRORS & OMISSIONS COVERAGE (TECH PI)

Please complete the following section only if applying for (Technology) Professional Services / Errors and Omissions cover. Alternatively go straight to Section 8 | Network Dependency.

1. Percentage of gross annual revenue, by services performed in the current and previous financial years:

		Current Financial Year	Previous Financial Year
Hardware	Maintenance	%	%
	Installation	%	%
	Sale of own brand	%	%
Software Product Services	Shrink wrapped / off-the-shelf software	%	%
	Own customisable software	%	%
	Third-party customisable software	%	%
Software Services	Installation including configuration (no code changes)	%	%
	Customisation (including code changes)	%	%
	Development bespoke application	%	%
	Maintenance	%	%
Services	Consultancy	%	%
	Data processing	%	%
	Cabling	%	%
	Project management	%	%
	Provision of contract staff	%	%
	Facilities management	%	%
	Training	%	%
	Web design	%	%
	Internet / application service provision (excluding web hosting)	%	%
	Web hosting	%	%
	Telecommunications	%	%
Other work (please provide details)		%	%
		%	%
Total must add up to 100%		%	%

2. Details of your three largest contracts which have been undertaken in the last three years:

	Client / Business	Services Provided	Total Contract Value	Contract Length
1.			R	
2.			R	
3.			R	

3. Do you typically undertake contracts which are longer than 2 years in duration? Yes No
4. Do you use outside consultants/contractors, or subcontract work to others? Yes No
If Yes, indicate what percentage of last year's gross annual revenue it represented %
5. Do you normally require consultants/contractors to hold their own Professional Indemnity (PI) cover? N/A Yes No
6. Do you enter into written contracts with all clients? Yes No
7. Please provide a copy of your standard client contract conditions, containing the clauses / provisions detailed in question 8 below.
8. Do your written contracts with clients contain the following clauses/provisions:
- a) Limitations of liability, including consequential damages Yes No
- b) Disclaimer or warranties Yes No
- c) Arbitration clause Yes No
9. What value do you cap liability at in your standard contract terms? R
10. How many clients have unlimited liability?
11. What percentage of your clients are on standard terms? %
12. a) Please indicate the average value of a client contract R
b) Please indicate the value of your largest single client contract R
13. Do you ensure that changes to the original contract are agreed to by both parties and documented in writing, which is then incorporated into the main contract? Yes No
14. Are all contracts reviewed by legal counsel prior to commencing any work? Yes No

15. Are variations to contracts reviewed by legal counsel? Yes No

16. Do you have quality control procedures in force to test all software and products prior to release? Yes No

17. Is the failure of your products or any of your services likely to result in any of the following outcomes:

a) Damage or destruction to physical property? Yes No

b) Death or bodily injury? Yes No

c) Immediate and significant financial loss? Yes No

d) Insignificant financial loss? Yes No

18. Have there been any significant changes in the nature or size of your business in the past 12 months? Yes No

19. Do you anticipate any change in the nature or size of your business over the next 12 months? Yes No

If Yes to (15) or (16) above, please provide full details (on a separate sheet if necessary):

20. Have you released or introduced new products, software and/or services within the past 12 months? Yes No

21. Do you plan on releasing or introducing new products, software and/or services within the next 12 months? Yes No

If Yes to (17) or (18) above, please provide full details (on a separate sheet if necessary):

22. Have you ever had to recall any of your electronic products or software for any reason? Yes No

If Yes, please provide full details (on a separate sheet if necessary):

23. Over the past three years, have any customers refused to pay or requested a refund or invoked contract penalty clauses outside the normal course of business?

Yes No

If Yes, please provide full details (on a separate sheet if necessary):

24. Do you have a formal process in place for resolving disputes with clients?

Yes No

25. Have you ever instituted adversarial proceedings against a client in order to recover unpaid fees?

Yes No

SECTION 8 | NETWORK DEPENDENCY

1. Do you outsource the management or any part of your IT operations?

Yes No

If Yes, please provide details in the table below:

Name Third Party Service Provider	Outsourced Operation	Access To Your Network
	Cloud data processing / storage	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Data centre / hosting	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Data processing (marketing / payroll)	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Managed security services	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Network implementation / maintenance	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Off-site archiving, backup and/or storage	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Payment processing	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Software implementation / maintenance	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Systems development, customisation, and maintenance	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>
	Other (specify)	Full <input type="checkbox"/> / Restricted <input type="checkbox"/> / No Access <input type="checkbox"/>

2. Please indicate whether your third party service provider(s) that assists you with either of the following outsourced operations, holds the relevant compliance certificate(s). e.g., ISO27001.

a) Cloud storage or processing service provider(s)

N/A Yes No

b) Data hosting or processing service provider(s)

N/A Yes No

3. Indicate the time after which the inability of your staff to access your computer network/databases would have a significant impact on your business:

Immediately <input type="checkbox"/>	After 6 hrs <input type="checkbox"/>	After 12 hrs <input type="checkbox"/>	After 24 hrs <input type="checkbox"/>	After 48 hrs <input type="checkbox"/>	Never <input type="checkbox"/>
--------------------------------------	--------------------------------------	---------------------------------------	---------------------------------------	---------------------------------------	--------------------------------

4. Indicate the time after which the inability of customers to access your website would have a significant impact on your business:

Immediately <input type="checkbox"/>	After 6 hrs <input type="checkbox"/>	After 12 hrs <input type="checkbox"/>	After 24 hrs <input type="checkbox"/>	After 48 hrs <input type="checkbox"/>	Never <input type="checkbox"/>
--------------------------------------	--------------------------------------	---------------------------------------	---------------------------------------	---------------------------------------	--------------------------------

5. Please provide brief details of the effect on your business should your internal network and/or applications fail or be disrupted (including commercial relations, revenues and reputation).

SECTION 9 | BUSINESS CONTINUITY

1. Please provide the latest copy of your DRP (Disaster Recovery Plan) or BCP (Business Continuity Plan). This is required for Data Recovery and Loss of Business Income cover to be considered.

2. Is this plan tested and updated at least annually?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

3. Have you recently carried out an IT security audit or Vulnerability scan?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

If Yes, who performed the IT audit and when did it occur?

Audited by:		Date:	/	/
--------------------	--	--------------	---	---

a) If Yes, were there any serious concerns raised?

N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	------------------------------	-----------------------------

b) If Yes, have all the recommendations been implemented?

N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	------------------------------	-----------------------------

4. Have you had an external Penetration Test carried out?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

If Yes, who performed the Penetration Test and when did it occur?

Conducted by:		Date:	/	/
----------------------	--	--------------	---	---

c) If Yes, were there any serious concerns raised?

N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	------------------------------	-----------------------------

d) If Yes, have all the recommendations been implemented?

N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	------------------------------	-----------------------------

5. Please provide the following in respect of your network backup:

Managed Third Party Service Provider	And / Or	Managed Locally By An Employee	
Name of third party service provider		Job title	
Is the third party ISO2007 compliant?	Yes <input type="checkbox"/> / No <input type="checkbox"/>	What backup software is used?	
Is the backup application stored on all company devices/assets with critical data?	Yes <input type="checkbox"/> / No <input type="checkbox"/>	What media is used to store the backup? (tape / hard drive / USB)	
Are these backup applications secured to prevent being tampered with? (MFA / password protected / PAM / Encryption)	Yes <input type="checkbox"/> / No <input type="checkbox"/>	How many backup versions are stored?	
Can backups be cancelled or stopped?	Yes <input type="checkbox"/> / No <input type="checkbox"/>	Where is the media stored? (offsite / onsite / secure safe)	
How often are backups conducted?		How often are backups conducted?	
How many backup versions are stored?		How often are restorations tested?	
How often are restorations tested?			

6. Do you use any operational technology or supply chain software?

Yes No

If Yes, please complete the additional questions at the end of the questionnaire.

SECTION 10 | NETWORK SECURITY

1. Do you employ an Information Officer, who is responsible for meeting your worldwide obligations under privacy and data protection laws?

Yes No

2. Do you provide mandatory Employee Awareness Training on security, data and privacy risks?

Yes No

3. Do you use any of these servers:

a) Microsoft Azure

Yes No

b) Amazon Web Services

Yes No

c) Microsoft Office 365

Yes No

d) Google G-Suite

Yes No

4. Do you utilise least Privileged Access Management (PAM)?

Yes No

5. Do you have strict user revocation procedures on user accounts and inventoried recovery of all information assets following employment termination?

Yes No

6. Do you ensure compliance of employees, contractors & others to your company policies?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
7. Do you have antivirus software on all computer devices, servers and networks?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
8. Do you have advance Endpoint Protection and Response (EDR) tools implemented on your network?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
9. Do you have firewalls with Intrusion Detection/Prevention Software to prevent and monitor unauthorised access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
10. Do you have a Patch Management process that ensures all updates are implemented within 14 days?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If No to the above, within how many days are critical security, anti-virus and malware patches, received from commercial software vendors, implemented on all physical		
11. Do you have access control procedures and hard drive encryption to prevent unauthorised exposure of data on all laptops, PDAs, smartphones and home-based PCs?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
12. Have you configured your network to ensure that access to sensitive data is limited to properly authorised requests?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
13. Do all your wireless networks have WPA2 or WPA3 Encryption?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
14. Please indicate if you have Encryption implemented on the below data and if applicable, which Managed Service Provider or program is used for this:		
a) All sensitive information that is physically removed from the premises by tape, disk hard drive or other means?	N/A <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
b) All sensitive information and confidential information that is transmitted within and from your organisation using industry grade mechanisms?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If Yes		
c) All sensitive and confidential information stored on your databases, servers and data files?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If Yes		
If No to any of the above, please provide details describing the nature of unprotected information and what security measures are in force to protect this information in the absence of encryption:		

15. Do you have Multi-Factor Authentication (MFA) implemented in the follow areas?

a) All admin/privileged accounts

Yes No

b) Access to critical data

Yes No

c) Access to backups

Yes No

d) Remote access

Yes No

16. Do you filter all incoming emails and communications for malicious links, spam, malware, and attachments?

Yes No

17. Do you employ a Sender Policy Framework (SPF)?

Yes No

18. Please provide your email domain name e.g., @camargueum.co.za

19. Is your network segmented?

Yes No

If **Yes**, please provide details of how your network is segmented

20. Do you make use of any unsupported/end-of-life software or operating system?

Yes No

If **Yes**, please provide further details on the function of the software/operating system in your network and whether is it segmented/isolated from your main network.

SECTION 11 | INFORMATION AND DATA MANAGEMENT

1. Does your password policy include the following:

a) Minimum length of 8 characters with at least two special characters, an upper case and a lower case letter?

Yes No

b) Passwords are all changed within a period of 90 days?

Yes No

c) User is locked out if the system after a maximum of 5 failed attempts?

Yes No

d) Test for trivial passwords such as password123?

Yes No

If **No** to any of the above, please describe the controls in place to manage your system security:

2. Do you have a Data Classification Policy (e.g., public, internal user only, confidential)? Yes No
3. Do you post a Privacy Policy on your website which has been reviewed by a qualified lawyer? Yes No
4. Do you have an Information Asset Inventory that lists the owners and sources of all data? Yes No
5. Do you have procedures in force for honouring the specific marketing 'opt-in' and 'opt-out' requests of your customers that are consistent with the terms of your published Privacy Policy? N/A Yes No
6. Do you have a Data Retention and Destruction Policy? Yes No
7. Is all information held in physical form (paper, disks, CDs etc.) disposed of or recycled by confidential and secure methods which are recognised throughout the organisation? N/A Yes No
8. Do you have a procedure in place to record security breaches and incidents? Yes No
9. Please confirm the total number of Data Subjects that are retained within your networks, databases, and cloud-based servers at any one point in time in terms of employees, customers, and contractors/vendors.
10. Have you in the past 5 years or are you currently collecting biometric data from employees, consumers and/or vendors? Yes No
- If Yes, please complete our Biometric Annexure B on page 19 of this proposal form.
11. Do you track data by use of tracking tools? Yes No
12. Do you inform visitors of your website(s) that you track data (e.g., by cookies)? Yes No
13. Do you have a policy and associated procedure(s) to ensure that wrongful tracking and collection of data is avoided effectively? Yes No

SECTION 12 | GENERAL QUESTIONS

1. Have you or any of the proposer’s principals, partners, directors, risk managers, or employees:

a) Been convicted of or is any prosecution pending for any offence involving dishonesty of any kind (including but not limited to an offense involving fire, fraud, theft or handling stolen goods)?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

b) Been declared bankrupt, the subject of bankruptcy proceedings or of any voluntary or mandatory insolvency or winding up procedures?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

If **Yes** please provide full details, on a separate sheet if necessary:

2. Confirm the following with respect to COVID-19 impact:

a) Please provide commentary on the impact of COVID-19 and the current financial market volatility to your income and balance sheet.

b) Please advise of any inability to offer your services or product as a result of the COVID-19 business disruption (or potential disruption).

c) Please advise of any impact to your supply chain or inventory (including any impairments to inventory valuations).

d) Were any of your business controls (including but not limited to transfer controls) impacted by any COVID-19 business disruption or potential disruption?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

e) Please provide details of any communications made to your shareholders concerning the implications (or potential implications) of COVID-19.

DECLARATION

Signing this proposal form binds neither the proposer to complete this insurance, nor does it bind the insurer to accept the proposal. It is agreed that all written statements and attachments furnished to the insurer in conjunction with this proposal are hereby incorporated by reference into this proposal and made part thereof. It is understood and agreed that the insurer has relied upon this proposal and attachments, which shall be the basis of the insurance contract.

The undersigned is an authorised signatory of the proposer and certifies that reasonable inquiry has been made to obtain the answers herein which are true, correct and complete to the best of his/her knowledge and belief. The proposer undertakes to inform the insurer of any material alteration to these facts, whether occurring before or after completion of the insurance contract.

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>

We, the Directors and Management of the Company, declare that to the best of our knowledge the statements set forth herein are true. It is agreed that this form shall be the basis of the Contract should a Policy be issued.	
Signature of the Proposer	
Name of Signatory	
Capacity of Signatory (duly authorised)	
Name of Company	
Date	
Place	

BROKER'S DETAILS

Name of Company	
Contact Person	
Telephone Number	
E-Mail	

ANNEXURE A | GLOSSARY OF TERMS

Biometric Data

A technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

Data Classification Policy

A process of organising data into categories that make it is easy to retrieve, sort and store for future use.

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.

Data Retention and Destruction Policy

A policy that establishes requirements and guidelines within an organisation for archiving, retaining, and destroying enterprise data. The policy should account for the personnel, processes and technologies required to ensure that enterprise data is archived and destroyed as needed, to meet business objectives and legal obligations

Disaster Recovery Plan (DRP) / Business Continuity Plan (BCP)

A set of policies, tools, and procedures to enable the recovery and/or continuation of critical business components following a natural or human- induced disaster. A DRP will contain more specific information pertain to technology infrastructure and systems. These plans will contain details of the various personnel involved in the recovery process and their respective responsibilities.

Employee Awareness Training

Training programs which provide employees with anti-fraud training at least annually (including but not limited to detecting social engineering, phishing training, business e-mail compromise and other similar exposures).

Encryption

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

Endpoint Protection and Response (EDR)

Software installed on individual computers (endpoints) that is an integrated endpoint security solution which combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

Incident Response Plan

Action plans for dealing with cyber incidents to help guide an organisation's decision-making process and return it to a normal operating state as quickly as possible.

Information Asset Inventory

A list of all IT hardware and devices an entity owns, operates, or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Information Officer

The person responsible for encouraging responsible persons to comply with the principles and conditions for the lawful processing of personal information and assisting data subjects to make requests and lodge complaints.

Intrusion Detection/Prevention System

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Managed Service Provider

A third party organisation that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

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.

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.

Payment Card Industry Data Security Standards (PCI DSS)

A set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

Penetration Tests

Authorised simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Privileged Access Management (PAM)

It is a combination of tools and technology used to secure, control, and monitor access to an organisation's critical information and resources. This process is done through limiting user access according to authority level and job function.

Sender Policy Framework (SPF)

An email authentication technique which is used to prevent spammers from sending messages on behalf of your domain.

Vulnerability Scan(s) / IT Audits

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

WAP2 / WAP3 Encryption

A type of encryption used to secure the vast majority of Wi-Fi networks. It provides unique encryption keys for each wireless client that connects to it. WPA3 provides a more secure connection than WPA2.

ANNEXURE B | BIOMETRIC INFORMATION

1. Please indicate, by way of tick, which data you are currently collecting or have collected, over the past 5 years, from employees / customers / individuals:

	Employees	Customers	Individuals
Retina Scan:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Iris Scan:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fingerprint:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Voiceprint:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hand Scan:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Face Geometry:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Do you obtain written consent from employees/customers/individuals prior to the collection of their biometric data?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

3. Do you clearly indicate to employees/customers/individuals how you will collect their biometric data, why the data is required, how it will be stored and when it will be destroyed?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

4. Do you sell, lease, trade or otherwise profit from an employees' / customers / individual's biometric data?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

5. What level of security have you applied to biometric data for access, storage and transmission?

6. Is biometric data stored separately/segmented from other types of data?

7. Do you have a biometric data retention and destruction schedule outlining for how long you will hold the biometric data?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

8. Have you received any complaints alleging the unlawful collection, use, dissemination, or sale of biometric data?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

ANNEXURE C | OPERATION TECHNOLOGY (OT) AND SUPPLY CHAIN SOFTWARE

1. Are the process control networks and IT network air gapped?

Yes No

If No, how are remote connections secured?

VPN MFA

2. Please describe your procedures for managing critical IT and non-IT vendors, e.g., Backup vendors / contingency plans?

3. Have you conducted a business impact analysis for downtime due to your computer network?

Yes No

If Yes, after what period of time will your revenue be affected?

--

4. Does your DRP (Disaster Recovery Plan), which is tested and updated annually, address downtime of your OT or supply chain software?

Yes No

5. Do you have an alternative method by which your business can be conducted should your OT or supply change software fail?

Yes No

If Yes, please provide further details of this method:

--

6. In the event of missed or delayed production, would you incur any costs associated with contractual penalties, liquidated damages and/or non-contractual compensation payments?

Yes No

If Yes, please provide further details of the costs incurred:

--

ANNEXURE D | PCI DSS (PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS)

SECTION 1 | GENERAL PAYMENT CARD INFORMATION

Please complete all applicable sections. If necessary, please use separate sheet to provide a full response.

1. How many transactions do you process each year:

Level 4 Fewer than 20,000	<input type="checkbox"/>
Level 3 20,000 to 1 million	<input type="checkbox"/>
Level 2 1 million to 6 million	<input type="checkbox"/>
Level 1 More than 6 million	<input type="checkbox"/>

2. How do you process payment card transactions (please check all that apply):

<input type="checkbox"/>	Strictly card-not-present transactions (e-commerce, mail/telephone):	
<input type="checkbox"/>	No electronic cardholder data storage	<input type="checkbox"/>
		With electronic cardholder data storage
<input type="checkbox"/>	Standalone dial-out terminals with no electronic cardholder data storage	
<input type="checkbox"/>	Web-based virtual terminals:	
<input type="checkbox"/>	No electronic cardholder data storage	<input type="checkbox"/>
		With electronic cardholder data storage
<input type="checkbox"/>	Payment applications connected to a computer network (including via embedded applications within point of sale systems)	
<input type="checkbox"/>	No electronic cardholder data storage	<input type="checkbox"/>
		With electronic cardholder data storage
<input type="checkbox"/>	Other (please specify):	

3. Are you required to adhere to the PCI DSS by a financial institution or credit processor as a part of the merchant's services agreement or otherwise?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

If **Yes**, are you required to submit a Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) to document compliance with the PCI Data Security Standards?

ROC	<input type="checkbox"/>	SAQ	<input type="checkbox"/>	Neither	<input type="checkbox"/>
-----	--------------------------	-----	--------------------------	---------	--------------------------

SECTION 2 | REPORT ON COMPLIANCE (ROC) OR A SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

If you are not required to complete an ROC or SAQ, please proceed to Section 3

1. When was your last ROC or SAQ report submitted?

2. Did your last SAQ or ROC indicate that you are in compliance?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

3. What was the date of the last quarterly network scan completed by an Approved Scan Vendor?

Did your last quarterly network scan by an Approved Scan Vendor result in a non-compliant scan report i.e., did the scan report any Level 5 ('Urgent'), Level 4 ('Critical'), or Level 3 ('High') vulnerabilities?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

If **Yes**, please indicate the report level and describe the remediation status for the identified vulnerabilities:

SECTION 3 | PCI PROCESSING ENVIRONMENT

If you process payment card transactions via payment applications connected to the Internet (including via embedded applications within points of sales systems), please complete the following. Otherwise, please skip this section.

1. Are all payment processing systems (hardware and software applications) certified as PCI DSS-validated?

Yes <input type="checkbox"/>	No <input type="checkbox"/>	Unknown <input type="checkbox"/>
------------------------------	-----------------------------	----------------------------------

If you are unsure, please list the name and version of software application(s) here:

2. Have all default and vendor supplied passwords for payment systems been modified?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

3. Were your payment processing systems installed and configured with the assistance of a systems integrator, reseller or consultant qualified by the PCI Security Standards Council Qualifies Integrators and Resellers (QIR)™ program?

Yes <input type="checkbox"/>	No <input type="checkbox"/>	Unknown <input type="checkbox"/>
------------------------------	-----------------------------	----------------------------------

4. a) Are all the devices, computers and servers that handle payment card transactions inside your network completely segmented by firewalls at each internet connection as well as from the remainder of your corporate network?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

b) Have you restricted access to and from the PCI environment to only necessary systems and ports inside your corporate environment?

Yes <input type="checkbox"/>	No <input type="checkbox"/>
------------------------------	-----------------------------

c) Do you restrict external traffic from “untrusted” networks and hosts?

Yes No

d) Have you prohibited direct public access between the Internet and all components inside your PCI environment?

Yes No

e) Is outbound traffic from the PCI environment restricted to specific external IP addresses?

Yes No

5. Do you monitor traffic from the PCI environment to external sources?

Yes No

6. Do you employ any of the following: tokenization or end-to-end encryption (including encryption of databases to protect payment card data?)

Tokenization

End-to-end encryption

SECTION 4 | NON-COMPLIANCE

If you answered NO to question 5 in relation to SAQ or ROC compliance, please complete this section.

1. Please provide a general description of the areas where you are not compliant.

2. Please describe your remediation efforts in order to attain compliance with the issues noted above:

3. Please describe any compensating controls that you have implemented:

4. By what date do you plan to attain compliance?