AFRO-ASIAN®
INSURANCE SERVICES LTD
Broker at LLOYD'S

Cyber Risk Application

General Information

Company/Trading Name (inc any subsidiaries to be included on the policy):

Business activity:

Operating countries:

Website:

Date established:

Financial / Employee Information

	US Revenue	Non-URevenue	Total Revenue
1. a) Revenues of last completed financial year			
b) Net profit of last completed financial year			
c) Projected revenues of current financial year			

	Additional Comments
2. a) Are any acquisitions or significant changes to the size, activities of the company or number of employees anticipated within the next year?	

b) Total Number of employees:

c) What position in your organisation is responsible for information security?

d) What position in your organisation is responsible for privacy issues?

Data Assessment

3. a) Please identify the type and volume of information you store

Consumer Data	**No. of records**
Personally Identifiable Information (PII)	
General PII (Name, address, phone no.)	
PHI	
FAI	
Unique/Government ID (SSN/Driving licence etc/passport)	
Biometric data	
Other	
Please estimate the maximum number of unique individual records held within a single database?	

Payment Card Data	**No. of records/transactions**
Transactions processed annually	
Credit card data stored on your systems	
Please confirm which format payment card data is stored in (tokenised, hashed, last four numbers etc)	

4. a) Do you have a data classification program that governs the access, transmission and storage of data? Yes □/No □

b) Do you have a data retention and destruction policy? Yes □/No □

c) Do you complete a regular purging of all legacy data? Yes □/No □

d) Do you segment sensitive data from the rest of your network? Yes □/No □

Monitoring

5. a) Are you operating a Security Operations Centre (SOC)?

b) Is this running 24x7?

c) Is this operated in-house or outsourced?

d) Are logs aggregated in a SIEM?

6. a) Are database queries involving sensitive data monitored?

b) If so, is there a formal notification procedure in place when a typical database query occurs?

Internal / External Assessment

7. a) When was the last 3rd party security assessment of your network performed?

b) Did this include a network penetration test?

c) Have all critical and high risk recommendations been remediated?

d) How often are such assessments performed?

Employee Management

	Additional Comments
8. a) Are staff trained in security and privacy matters such as phishing?	Yes □/No □
b) Are access controls employed using the principle of least privilege? -How regularly is this reviewed?	Yes □/No □
c) Is USB write access disabled by default?	
d) Are all passwords on your system set to a different password to the manufacturer/ vendor default?	Yes □/No □
e) Are passwords required to meet standards in complexity and length?	Yes □/No □
f) Are regular password change requirements enforced for all user and administrator accounts?	Yes □/No □

Privileged User & Remote Access

	Additional Comments
9. a) Do you require the use of two-factor authentication for admin accounts?	Yes □/No □
b) Do you require the use of two-factor authentication for all remote access?	Yes □/No □
c) Are remote sessions monitored for anomalous activity?	Yes □/No □

Security Systems

	Additional Comments
10 a) Do you have anti-virus deployed across your network?	Yes □/No □
b) Are firewalls deployed at all external connection points?	Yes □/No □
c) How often are firewall rules reviewed and updated?	
d) Do you have web application firewalls in place for all web servers?	Yes □/No □
e) Do you have intrusion detection and/or intrusion prevention systems running?	Yes □/No □
f) Do you have a Data Loss Prevention solution implemented?	Yes □/No □
g) Do you perform web application testing?	Yes □/No □

Patch management and software support

	Additional Comments
11. In what timeframe are security critical patches implemented?	
12. Are you scanning your network for unpatched systems and how regularly is this conducted?	
13. a) Do you operate any unsupported software or legacy systems for e.g. Windows XP?	
b) If so, is PII/PHI or any sensitive information stored on these systems?	Yes □/No □
c) Please provide details of compensatory controls in place to isolate these from: - the rest of your network - remote access/ internet	

Portable Devices

		Additional Comments
14.	a) Do you utilise a Mobile Device Management system? If so, does this allow for remote wiping of devices?	Yes □/No □
	b) Do you require encryption of all mobile devices and laptops?	Yes □/No □
	c) In the absence of encryption, do unencrypted portable devices carry sensitive data which is accessible only through an encrypted VPN controlled by two factor authentication? **OR** d) If not, please advise compensating controls?	Yes □/No □

Physical Controls

		Additional Comments
15.	a) Are data centres owned or co-located?	
	b) What physical security is in place? (Tier of DC will suffice)	
	c) Is physical access monitored or reviewed for anomalous behaviour?	Yes □/No □
	d) Are hard copies of PII/PHI physically secured from receipt of such data to disposal?	Yes □/No □

Application Life Cycle (complete if you develop software/applications in-house)

			Additional Comments
16.	a) Do you have a formal change control process in place?	Yes □/No □	
17.	a) Are security measures built into all developed software?	Yes □/No □	
	b) Do you conduct pre-deployment testing on all applications (whether developed in-house or purchased through a 3rd party)?	Yes □/No □	
18.	a) Do you provide secure-code training to in-house software engineers?	Yes □/No □	
	b) Do you use production data in your test environments?	Yes □/No □	

Vendor Management

	Additional Comments
19. a) Are all third parties required to comply with the insured's security policy with regards to protecting sensitive information which the insured has shared with them?	Yes □/No □
20. a) Are vendor access rights periodically reviewed and updated?	Yes □/No □
21. a) Is 3rd party access on your network monitored?	Yes □/No □
22. a) Is access limited to dedicated time windows?	Yes □/No □
23. a) Is two-factor authentication required for vendor access to your network?	Yes □/No □

Compliance / Governance

	Additional Comments
24. a) Do you have a formal information security policy that is acknowledged by all staff?	Yes □/No □
25. a) Are all legal and regulatory requirements of all jurisdictions in which you operate embedded into company policies?	Yes □/No □
26. a) Please indicate security and privacy frameworks that your systems and policies are based upon? (ISO, NIST, etc)	
27. a) If you store Healthcare information please indicate whether you are HIPAA compliant b) Please advise the date and findings of your last externally conducted HIPAA audit	

Incident Response Plans

	Additional Comments
28. a) Do you have a formalised incident response plan?	Yes □/No □
b) What incidents does the plan cover?	
c) How often is this tested?	

Business Interruption

	Additional Comments
29. a) Do you have a documented Business Continuity Plan?	Yes □/No □
b) Do you have a documented Disaster Recovery Plan?	Yes □/No □
c) How frequently are they tested?	
d) What are your Recovery Time Objectives (RTOs) for critical systems?	
e) Have you performed a business impact analysis? f) How frequently do you backup mission critical data? g) How often are backups tested?	

Multimedia

	Additional Comments
30. a) Is there a procedure for responding to allegations that content created, displayed or published by the Applicant is libelous, infringing, or in violation of a third party's privacy rights?	Yes□/No□
b) Do you have take-down procedures in place to respond to allegations or requests from 3rd parties to remove infringing or offending content?	Yes□/No□
c) Does the Applicant have a process to review all content prior to posting on the Insured's Internet Site or on social media web pages created and maintained by or on behalf of the Insured?	Yes□/No□
d) Has the Applicant screened all trademarks used by the Applicant for infringement with existing trademarks prior to first use?	Yes□/No□

Claims/Circumstances

31. a) Have you had any claims or circumstances within the past 5 years that would have triggered the proposed policy?	
b) In light of any incident please provide details of any repeat attacks and remediation work that has been undertaken as a result	

I declare that after proper enquiry the statements and particulars given above are true and that I have not mis-stated or suppressed any material fact.

I agree that this proposal form, together with any other material information supplied by me shall form the basis of any contract of insurance effected thereon.

I undertake to inform underwriters of any material alteration to these facts occurring before the completion of the contract.

Signature	
Title	
Date	