CYBER INSURANCE PROPOSAL FORM

Instructions

Completion of this application may require input from your organisation's risk management and information technology departments.

- Please answer **all** questions completely. Should any questions, or part thereof not be applicable please print "N/A" in the space provided.
- This form must be completed, dated and signed by an authorised representative from your organisation.

Underwriters will rely on all statements made in this application so please provide honest answers.

1. ORGANISATION INFORMATION:

Organisation name

Head office address

Primary contact phone number

Primary contact email address

Registration number

VAT number

Nature of business ____ If other, please specify: ____

Products and services offered

Average number of employees Permanent: ____ Temp: ____ Contractors: ____

Public facing URL addresses (websites and services such as file transfer facilities)

Subsidiary names (if applicable)

	Last year	Projected current year
Gross revenue	$	$
Gross e-business revenue	$	$
Approx. value of asset base	$	$

Geographical split of total gross revenue (%)

Zimbabwe	%	%
European Union	%	%
USA	%	%
SOUTH Africa	%	%

2. INSURANCE INFORMATION:

Have you ever had an insurance policy cancelled or been declined insurance cover?

If Yes, please provide additional information:

Have you sustained an unscheduled network outage over the past 24 months?

If Yes, please provide additional information (including duration of outage):

Are you, or any of the partners, directors or officers, aware of or are there any circumstances within the past 5 years that would have given, may give, or have given, rise to a claim against the organisation or against this insurance policy?

If Yes, please provide additional information:

Have you previously held similar cover to this application?

3. SURVEY POLICIES AND STANDARDS:

Have you implemented information security policies which have been approved by management?

Are security policies reviewed on an annual basis?

Please specify any information security certifications that you hold, e.g. PCI DSS

What is the minimum password length restriction applied to accounts?

How regularly are users required to change their passwords?

After how many failed authentication attempts are accounts locked out?

How long are accounts locked out for after failed authentication attempts?

Are users prevented from re-using their passwords for at least 5 changes?

Are password guidelines enforced on all sensitive systems, e.g. password parameters defined on active directory?

4. SURVEY REVIEWS AND ASSESSMENTS:

How frequently are your IT environments subjected to vulnerability or penetration testing? If possible, please attach the latest testing report.

5. MANAGEMENT OF SENSITIVE AND PRIVATE INFORMATION:

Which of the following data do you collect/store (own and 3rd party):

- Bank records or financial account details — Approx. # of records: _____
- Medical records or health information — Approx. # of records: _____
- Payment card details — Approx. # of records: _____
- Personal identity information (names, contact details, addresses) — Approx. # of records: _____
- Third party corporate confidential data — Approx. # of records: _____

Have your internet facing systems been configured so that no sensitive or personal data resides directly on them, but is instead stored behind a firewall on internal databases/systems? _____

Have you implemented encryption for the following:

- Data stored on portable devices (laptops, external storage devices, tablets, phones, etc.) _____
- Sensitive data transmitted outside your environment _____
- Sensitive data/backups stored outside your environment _____
- Sensitive data stored in your environment _____

If Yes, please provide additional information: _____

6. SECURITY IMPLEMENTATION:

Have you implemented anti-virus software on all computers and mission critical servers (where applicable)? _____

Have you implemented firewalls at all breakout points to external networks? _____

As part of system configuration do you ensure that all default vendor accounts are secured, via disabling/ deleting or changing the account password? _____

Do you actively in real time monitor sensitive/critical servers and applications? _____

Do you allow for remote access to your network? _____

Do you secure all computers and servers according to your technical security configuration standards? _____

Have you implemented controls to restrict unauthorised access to sensitive data via your wireless network? _____

7. PHYSICAL AND ENVIRONMENTAL SECURITY:

Have you implemented physical controls such as surveillance cameras or access control mechanisms to restrict access to your server room and other sensitive processing facilities? _____

Have you implemented physical security controls such as reception to screen visitors or access control mechanisms to restrict access to your offices? _____

Do your remote locations including disaster recovery and redundant processing sites have physical security that is at least aligned to the primary processing site? _____

8 SYSTEM and SECURITY LOGS:

For what period of time do you maintain logs? _____

9 SECURITY PATCHES AND VIRUS DEFINITIONS:

How frequently do you update virus definition files on computers and servers? _____

How long after release do you implement security related patches and updates on computers, servers and network appliances (routers, firewalls, etc.)? _____

10. THIRD PARTY SERVICE PROVIDERS:

Functions outsourced to 3rd party service providers	Outsourced to 3rd party service provider	3rd party service provider's name
Cloud data processing/storage	_____	_____
Data centre/hosting	_____	_____
Data processing (marketing/payroll)	_____	_____
Managed security services	_____	_____
Network implementation/maintenance	_____	_____
Off-site archiving, backup and/or storage	_____	_____
Payment processing	_____	_____
Software implementation/maintenance	_____	_____
Systems development, customisation and maintenance	_____	_____

Other (please specify) _____

_____

_____

What level of access do you grant to 3rd party service providers? _____

Do agreements with the 3rd party service providers require levels of security commensurate with your information security policies? _____

Do you review that 3rd party service providers are adhering to contractual and/or regulatory requirements regarding data protection? _____

Do you require indemnification from 3rd party service providers for any liability attributable to them (including data breach and system downtime)? _____

11. BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY:

Do you have documented and approved disaster recovery and business continuity plans? _____

Do you review, test and update disaster recovery plans on at least an annual basis? _____

How frequently do you generate backups? _____

Do you monitor for the successful generation of backups? _____

12 PERSONNEL SECURITY:

Do you conduct background checks on potential employees as part of the recruitment process? _____

Do you have a process implemented for granting, reviewing and disabling user accounts and privileges? _____

How long after termination of employment do you typically revoke user privileges? _____

Have employees been required to attend any security and data privacy training or awareness courses within the past 12 months? _____

Have you implemented controls to manage and/or restrict internet access and usage? _____

3. LIMIT

Limit of liability:	Requested deductible:

The undersigned persons declare that to the best of their knowledge the information provided herein is true and correct. In addition the undersigned agrees that, if between the date of this Form and the date of the actual Application or the effective date of the Policy, (1) any material change in the condition of the Applicant is discovered, or (2) there is any material change in the answers to the questions contained herein, notice of such change will be reported to the Insurer immediately and the Insurer may in its sole discretion modify or withdraw any quote. Any material misrepresentation, omission, concealment or incorrect statement of fact, in this Form or otherwise, may be grounds for the rescission of coverage provided to some or all of the Insureds, subject to and in accordance with the terms of this Policy. The undersigned agrees that this declaration shall form part of the agreement with the insurer and that they are properly authorised to sign this declaration.

Signing of this Form does not automatically bind coverage and acceptance of the risk is at the Insurer's discretion.

Applicant name: _____ Applicant signature: _____

Position: _____ Date: _____