Block G First Floor | The Palms Office Park | 391 Main Avenue|
Ferndale | Randburg | 2194 | South Africa
Website: www.mukfin.co.za | Email: admin@mukfin.co.za

CYBER ENTERPRISE RISK MANAGEMENT INSURANCE PROPOSAL FORM

Please Note

1. Please answer **ALL** questions in full. If there is insufficient spaces on the form please continue on the company letterhead.
2. The latest audited Financial Statements / Annual Report / Interim Report **MUST** be attached.
3. This form may be used for new applications or new renewals. In the case of renewals the underwriters **MUST** receive a completed, signed and dated proposal form, financials/reports and acceptance of renewal terms prior to renewal date, failing which, no cover exists after said date.
4. It is the intention of underwriters that any Contract of Insurance with the Proposer shall be based upon the information provided in this Proposal Form as well as any attachments included. If a quotation is offered it will be the intention of the underwriters to offer cover **ONLY** in respect of the entities named under Particulars of Proposer.

NB: (No insurance is in force until the Proposal has been accepted by the Company and the premium paid, except as provided by an official Covering Note issued by the Company)

If MUKFIN agrees to issue a cyber enterprise risk management policy, all of the information, which the company provides, will become part of and shall form the basis of any policy issued to the Company by Mukoma Financial Services.

1. IDENTIFICATION OF THE APPLICANT COMPANY

Company Name .....
Address .....
.....
Postal Address .....
.....
Contact Person .....
Phone Number .....
Fax Number .....
Cell Number .....
E-Mail Address .....
Website .....
Type Of Organisation .....
VAT Number .....
Date Established .....
Number of employees .....
Annual Gross Margin .....
Annual Turnover .....

2. PROFILE OF THE COMPANY/COMPANIES TO BE INSURED

2.1 Business Operations

Please describe the main business operations of the company/companies to be insured. If these activities include e - commerce, please indicate the percentage of turnover generated.

2.2 Scope

The companies and subsidiaries to be insured. If the company has subsidiaries outside of South Africa, please provide the details.

2.3 Criticality of the Information Systems

Please assess the outage period over which your company will suffer significant impact to its business.

Application/Activity	Maximum Outage Period Before Adverse Impact On Business				
	Immediate	>12h	>24h	>48h	>5 Days

3. INFORMATION SYSTEMS

	<100	101-1000	>1000
Number of Information Systems users			
Number of Laptops			
Number of Servers			

Do you have an e-commerce or an online service website? ☐Yes ☐No

If yes:

What is the revenue share generated or supported by the website? (estimate) ……(% or ME)

4. INFORMATION SECURITY

4.1 Security Policy and Risk Management

1. An IS policy is formalised and approved by company management and/or security rules are defined and communicated to all staff and approved by the staff representatives. ☐Yes ☐No
2. Formalised awareness training on the IS is required of all staff at least annually. ☐Yes ☐No
3. You identify critical information systems risks and implement appropriate controls to mitigate them. ☐Yes ☐No
4. Regular audits of the IS are conducted and resulting recommendations are prioritised and implemented. ☐Yes ☐No
5. Information resources are inventoried and classified according to their criticality and sensitivity. ☐Yes ☐No
6. Security requirements that apply to information resources are defined according to classification. ☐Yes ☐No

4.2 Information Systems Protection

1. Access to critical information systems requires dual authentication. ☐Yes ☐No
2. Users are required to regularly update passwords. ☐Yes ☐No
3. Access authorisations are based on user roles and a procedure for authorisation management is implemented. ☐Yes ☐No
4. Secured configurations references are defined for workstations, laptops, servers and mobile devices. ☐Yes ☐No
5. Centralised management and configuration monitoring of computer systems are in place. ☐Yes ☐No
6. Laptops are protected by a personal firewall. ☐Yes ☐No
7. Antivirus software is installed on all systems and antivirus updates are monitored. ☐Yes ☐No
8. Security patches are regularly deployed. ☐Yes ☐No

9. A Disaster Recovery Plan is implemented and updated regularly. ☐Yes ☐No
10. Data backups are performed daily, backups are tested regularly and a backup copies are placed regularly in a remote location. ☐Yes ☐No

4.3 Network Security and Operations

1. Traffic filtering between the internal network and internet is updated and monitored regularly. ☐Yes ☐No
2. Intrusion detection/prevention system is implemented, updated and monitored regularly. ☐Yes ☐No
3. Internal users have access to Internet web site browsing through a network device (proxy) equipped with antivirus and website filtering. ☐Yes ☐No
4. Network segmentation is implemented to separate critical areas from non-critical areas. ☐Yes ☐No
5. Penetration testing is conducted regularly and a remediation plan is implemented where necessary. ☐Yes ☐No
6. Vulnerability assessments are conducted regularly and a remediation plan is implemented where necessary. ☐Yes ☐No
7. Procedures for incident management and change management are implemented. ☐Yes ☐No
8. Security events such as virus detection, access attempts, etc…, are logged and monitored regularly. ☐Yes ☐No

4.4 Physical Security of Computing Room

1. Critical systems are placed in at least one dedicated computer room with restricted access and operational alarms are routed to a monitoring location. ☐Yes ☐No
2. The data centre hosting critical systems has resilient infrastructure including redundancy of power supply, air conditioning, and network connections. ☐Yes ☐No
3. Critical systems are duplicated according to Active/Passive or Active/Active architecture. ☐Yes ☐No
4. Critical systems are duplicated on two separate premises. ☐Yes ☐No
5. Fire detection and automatic fire extinguishing system in critical areas are implemented. ☐Yes ☐No
6. The power supply is protected by a UPS and batteries which are both maintained regularly. ☐Yes ☐No
7. Power is backed up by an electric generator which is maintained and tested regularly. ☐Yes ☐No

4.5 Outsourcing

[Please fill in if a function of the information system is out sourced.]

1. The outsourcing contract includes security requirements that should be observed by the service provider ☐Yes ☐No
2. Service Level Agreements (SLA) are defined with the outsourcer to allow incident and change control and penalties are applied to the service provider in case of non compliance with the SLA ☐Yes ☐No
3. Monitoring and steering committee(s) are organised with the service provider for the management and the improvement of the service ☐Yes ☐No
4. You have not waived your rights of recourse against the service provider in the outsourcing contract ☐Yes ☐No

What are the outsourced Information Systems functions?	Yes/No	Service Provider (Outsourcer)
Desktop management	☐Yes ☐No	
Server management	☐Yes ☐No	
Network management	☐Yes ☐No	
Network security management	☐Yes ☐No	
Application management	☐Yes ☐No	
Use of cloud computing	☐Yes ☐No	
If Yes, please specify the nature of cloud services: ……..		
Software as a Service	☐Yes ☐No	

Platform as a Service	☐Yes ☐No	
Infrastructure as a Service	☐Yes ☐No	
Other, to: ……...		

5. The outsourcing contract contains a provision requiring the service provider(s) to Maintain professional indemnity or errors and omissions insurance ☐Yes ☐No

5. PERSONAL DATA HELD BY THE ORGANISATION

5.1 Type and Number of Records

The Number of personal information records held for the activity to be insured: Total: ……...

Categories of personal data collected/processed	Yes/No	Number of Records
Commercial and marketing information	☐Yes ☐No	
Payment Card or financial transactions information	☐Yes ☐No	
Health information	☐Yes ☐No	
Other, to specify please: ……		
Do you process data for:	☐ Our own purpose?	☐On behalf of third party?

5.2 Personal Information Protection Policy

1. A privacy policy is formalised and approved by management and/or personal data security rules are defined and communicated to the concerned staff. ☐Yes ☐No
2. Awareness and training are provided at least annually to the personnel authorised to access or process personal data. ☐Yes ☐No
3. A personal data protection officer is designated in your organisation. ☐Yes ☐No
4. A confidentiality agreement or a confidentiality clause in the employment contract is signed by the concerned staff. ☐Yes ☐No
5. The legal aspects of the privacy policy are validated by a lawyer/legal department. ☐Yes ☐No
6. Monitoring is implemented to ensure compliance with laws and regulations for the protection of personal data. ☐Yes ☐No
7. Your personal information practices have been audited by an external auditor within the past two years. ☐Yes ☐No
8. A Data Breach Response plan is implemented and roles are clearly communicated to the functional team members. ☐Yes ☐No

5.3 Collection of Personal Data

1. You have notified to the Personal Data Protection Commission (PDPC) the personal data processing involved by your company and you have obtained the applicable PDPC authorisation. ☐Yes ☐No
2. A privacy policy is posted on your website which has been reviewed by a lawyer/legal department. ☐Yes ☐No
3. Consent of individuals is required before collecting their personal data and the concerned persons can access and if necessary correct or delete their personal data. ☐Yes ☐No
4. Recipients are provided with a clear means to opt out of targeted marketing operations ☐Yes ☐No
5. You transfer Personal Data to third parties. ☐Yes ☐No
   If Yes, answer the following questions:
   a) The third party (e.g. processor) has a contractual obligation to process personal data only on your behalf and under your instructions. ☐Yes ☐No
   b) The third party has a contractual obligation to set up sufficient security measures to protect personal data ☐Yes ☐No

5.4 Personal Information Protection Controls

1. Access to personal data is restricted to only those users who need it to perform their task and access authorisations are reviewed regularly. ☐Yes ☐No
2. Personal data is encrypted when stored on information systems and personal data backups are encrypted. ☐Yes ☐No
3. Personal data is encrypted when transmitted over the network. ☐Yes ☐No
4. Mobile devices and laptop hard disks are encrypted. ☐Yes ☐No
5. IS policy prohibits the copying of non-encrypted personal data to removable storage devices or transmitting such data via email transmission ☐Yes ☐No

If personal records held contain payment card information (PCI), please answer the following:

Your PCI DSS level is: Level 1: ____ Level 2: ____ Level 3: ____ Level 4: ____

(Please refer to definitions page at the end of this document)

The payment processor (yourself or third party) is PCI DSS compliant ☐Yes ☐No

If **No**:

PCI is stored encrypted or only a part of payment card numbers is stored ☐Yes ☐No

PCI retention time does not exceed the duration of payment and legal/regulatory requirements ☐Yes ☐No

Payment card data processing is externalised ☐Yes ☐No

Please indicate payment processor name, PCI retention time and any additional security measures:

5.5 Incidents

Please provide a description of any information security or privacy incidents that have occurred in the last 36 months. Incidents include any unauthorised access to any computer, computer system, database, intrusion or attacks, denial of use of any computer or system, intentional disruption, corruption, or destruction of data, programs, or applications, any cyber extortion event(s); or any other incidents similar to the foregoing including those that have resulted in a claim, administrative action, or regulatory proceeding.

Date	Description of the incident
Comment	

No person or entity proposed for cover is aware of any fact, circumstance or situation which he or she has reason to suppose might give rise to any claim that would fall within the scope of the proposed coverage.

None ☐ Or, except: _____

DECLARATION

I/We declare that the above statements are true and complete.

At the present time, other than as stated above, I / We have no reason to anticipate any claim being brought against me/s that would constitute a claim under the insurance now being renewed or applied for.

I / We declare that in the event of this being a renewal of a policy, there have been no material alterations to the risk as submitted to the underwriter originally, and if a new application that all material facts have been disclosed.

I/We agree that this declaration shall form, together with the proposal form, the basis of the contract between me/us and the Insurers, and that I/We are properly authorised to sign this declaration.

Full name:

Capacity:

Signature:

Date:
