iTOO™

In association with Hollard.

PROPOSAL FORM
Cyber Insurance

Hollard.

Underwritten by The Hollard Insurance Co. Ltd,
an authorised Financial Services Provider

www.itoo.co.za | @itooexpert

ITOO is an Authorised Financial Services Provider. FSP No. 47230

Please answer **ALL** questions completely
Should any question or part thereof not be applicable, please state "N/A"
Should insufficient space be provided, please continue on your company letterhead

1. Name of Insured _____
2. Physical Address _____
3. Primary contact phone number _____
4. Primary contact email address _____
5. Registration Number _____
6. VAT Number _____

7. Choose an item which closely matches primary nature of business — Choose an item >>

If other please specify

8. Products and services offered

9. Subsidiary names (if applicable)

10. Have you been involved in any mergers/acquisitions within the past 3 years — Choose an item >>

11. Do you have any planned mergers/acquisitions within the next 12 months — **Yes** ☐ **No** ☐

12. Revenue

Annual Turnover/ Gross Revenue	Last year		Current year	
Gross e-business revenue	Last year		Current year	

13. Geographical split of gross revenue by region

South Africa	Last year	%	Current year	%
Europe	Last year	%	Current year	%
USA	Last year	%	Current year	%
Other	Last year	%	Current year	%

For countries outside South Africa, please specify the countries

13. Number of employees

Permanent		Contractors		Temporary	

14. Number of employees with system administration privileges

Permanent		Contractors		Temporary	

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

16. Approximate number of external IP addresses on your network — Choose an item >>
17. Approximate number of servers (including virtual machines) on your network — Choose an item >>
18. Number of locations where are servers located — Choose an item >>
19. Approximate number of laptops utilised — Choose an item >>
20. Approximate number of employees receiving company emails to privately owned devices — Choose an item >>

SECURITY POLICIES AND STANDARDS

1. Do you have a dedicated individual responsible for Information Security — Choose an item >>
2. Have you implemented information security policies/procedures and communicated these to employees — Yes / No
3. Are your security policies reviewed on at least an annual basis — Yes / No
4. Do you comply with privacy and data protection legislation applicable to all jurisdictions and industry standards in which you operate — Yes / No
5. Do you have a data classification policy including security requirements for sensitive data — Yes / No
6. Please specify any security certifications you hold (for example PCI DSS)
7. Do you enforce a "strong password policy" across all accounts, including: — Choose an item >>
   - Minimum password length restriction — Yes / No
   - Use of passwords which cannot within reason be deemed easily guessable — Yes / No
     - Do you perform any testing for known trivial passwords such as p@ssword1
   - Account lockout as a result of failed authentication attempts — Choose an item >>

*If **No** to any of the above, please provide additional information on controls to manage authentication security*

8. For sensitive servers and devices do you actively maintain:
   - System activity logs — Yes / No — and for what period of time: Choose an item >>
   - Security logs — Yes / No — and for what period of time: Choose an item >>
9. How regularly do you review the logs: Choose an item >>
10. Do you investigate all violations, intrusions and irregularities noted in the logs: Yes / No

SECURITY REVIEWS AND ASSESSMENTS

1. How frequently are your IT environments subjected to penetration testing: Choose an item >>
   Please attach the latest testing report
   - Were any serious concerns raised at your last test and have these been addressed: Choose an item >>
2. How frequently are your IT environments subjected to third party security assessments, including vulnerability scanning: Choose an item >>
   Please attach the latest testing report
   - Were any serious concerns raised at your last test and have these been addressed: Choose an item >>

   If all serious concerns have not been implemented, please provide details of outstanding items with remediation actions to be taken and associated timelines

3. Did the scope of the testing performed include both your internal and external IT environment: Yes / No
4. Do you perform penetration testing and/or secure code reviews on all new systems/software prior to deployment: Yes / No

SENSITIVE AND PRIVATE INFORMATION

1. Do you collect/store/process any of the following ***EMPLOYEE & CLIENT*** data

Bank records or financial account details	Approx. # of records	
Medical records or health information	Approx. # of records	
Payment card details	Approx. # of records	
• Do you store the card number		Yes / No
• Do you store the card expiry date		Yes / No
• Do you store the card validation codes (CVV number)		Yes / No
Personal identity information (names, ID numbers, contact details, addresses)	Approx. # of records	
Third party corporate confidential data	Approx. # of records	

2. Do you make use of or provide any web application functionality: Choose an item >>

3. 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 — Yes / No
4. Have you configured your network and externally visible applications and services to ensure that access to sensitive data is restricted to properly authorised requests — Yes / No
5. Have you implemented data retention and secure destruction policies for physical and electronic data and assets — Yes / No

*If **No**, please provide additional information on controls to manage data retention and destruction, considering both hard copy and electronic data*

6. Have you disabled employee write access to USB devices — Yes / No
7. Have you implemented encryption for the following:
   - Data stored on portable devices (laptops, external storage devices, tablets, phones, etc.) — Yes / No
   - Sensitive data transmitted outside your environment — Yes / No
   - Sensitive data/backups stored outside your environment — Yes / No
   - Sensitive data stored in your environment (data at rest) — Yes / No

*If **YES**, please provide additional information*

PAYMENT CARD DATA

Please complete this section only if you store or process payment card data

1. What level PCI merchant have you been certified as — Choose an item >>
2. What is your estimated number of payment card transactions processed per year
3. Are you fully compliant with the EMV card processing standards — Yes / No
4. Does a third party process payment card data on your behalf — Yes / No

   *If **YES**, please provide the name of the payment processor*

   *If **YES**, has the payment processor provided you with evidence that they are PCI certified* — Yes / No
5. Is payment card data encrypted or tokenised at all times — I don't know / Yes / No
6. Are your point of sale (POS) terminals designed to be tamper proof — Yes / No
7. Do you segregate your payment network from your normal network — N/A / Yes / No

8. Are POS terminals standalone or integrated with your systems — Choose an item >>
9. How frequently are you POS devices scanned for malware or skimming devices — Choose an item >>
10. How frequently is your payment network subjected to third party testing — Choose an item >>
    - At your last test were any serious concerns raised — Choose an item >>

SECURITY IMPLEMENTATION

1. Please indicate which of the following you have implemented (please select all that apply):
    - Anti-virus / malware which is updated in accordance with vendor recommendations — Yes
    - Firewalls at all breakout points to external networks — Yes
    - Firewalls to segment and protect sensitive data and resources within the network — Yes
    - Web application firewalls (WAF) — Yes
    - Intrusion detection or prevention systems (IDS / IPS) — Yes
        - Do you update signatures within a month of release — Yes
    - Security information and event management (SIEM) solutions — Yes
    - Cyber threat intelligence (CTI) function — Yes
    - Data loss prevention (DLP) tools — Yes
    - Access control and remote device wipe for mobile devices — Yes
    - Access control and remote device wipe for BYOD devices — Yes / NO BYOD
2. As part of system configuration do you ensure that all default installation and vendor accounts are secured via changing the account password and where possible disabling, deleting or renaming the account — N/A / Yes / No
3. Do you manage access permissions, including application of the principles of least privilege and separation of duties — Choose an item >>
4. Do you actively monitor access to sensitive/critical servers, data and applications — Yes / No
5. Do you secure all computers, servers and applications according to your technical security configuration standards — Yes / No

    *If **YES**, please provide additional information on the sources consulted to define technical security configuration standards*

6. Have you implemented a formal change control process including risk assessments, testing, approval and roll back — N/A / Yes / No
7. Have you implemented controls to restrict unauthorised access to sensitive data via your wireless network — N/A / Yes / No

8. Have you implemented a whitelist to prevent unauthorised and/or malicious programs from executing — Yes / No

9. Do you allow for remote access to your network — Choose an item >>

   *If **YES**, is remote access exclusively over secured channels (for example Virtual Private Network (VPN) with multi factor authentication)* — Yes / No

   *If **YES**, are controls implemented to protect accounts including installation and administration accounts from brute force password attacks* — Yes / No

   *If **YES**, please provide additional information on the controls implemented to secure remote access including controls to protect against brute force password attacks*

10. How long after release do you implement security related patches and updates on computers, servers and network appliances (routers, firewalls, etc.) — Choose an item >>

11. Have you implemented physical controls such as reception or access control mechanisms to restrict access to your offices — Yes / No

12. Have you implemented physical controls such as biometric access control to restrict and track access to your server room and other sensitive processing facilities — Yes / No

13. Are you making use of any unsupported software or operating systems — Yes / No

    *If **YES**, please provide additional information including: whether these are visible to external networks; the nature of data and/or systems running on these; any controls implemented to mitigate the risk and plans to remediate*

THIRD PARTY SERVICE PROVIDERS

Function	Outsourced	Third party providers name
Cloud data processing/storage	Yes / No	
Data centre/hosting	Yes / No	
Data processing (marketing/payroll)	Yes / No	
Managed security services	Yes / No	
Network implementation/maintenance	Yes / No	
Off-site archiving, backup and/or storage	Yes / No	
Payment processing	Yes / No	
Software implementation/maintenance	Yes / No	
Systems development, customisation and maintenance	Yes / No	
Other (please specify)	Yes / No	

1. What level of access do you grant to third party service providers	Choose an item >>
2. Do agreements with third party service providers require levels of security commensurate with your information security policies	N/A Yes No
3. Do you review that third party service providers are adhering to contractual and/or regulatory requirements regarding data protection	N/A Yes No
4. Do you require indemnification from third party service providers for any liability attributable to them (including data breach and system downtime)	N/A Yes No

INCIDENT RESPONSE, BUSINESS CONTINUTITY AND DISASTER RECOVERY PLANNING

1. Please indicate the time after which a disruption or failure of your IT environment, including network and applications, would have a significant impact on your revenue and operations	Choose an item >>
2. Do you have an incident response plan including a team with defined roles and responsibilities	Yes No
*If **YES**, how frequently do you review, test and/or update the incident response plan*	Choose an item >>
3. Do you keep an incident log of all data security breaches and network failures	Yes No
*If **YES**, are incidents investigated and escalated based on severity*	Yes No
4. Do you have documented and approved disaster recovery and business continuity plans	Yes No
*If **YES**, how long would it take you to be operational following an incident*	Choose an item >>
*If **YES**, what is your anticipated potential data loss*	Choose an item >>
*If **YES**, how frequently do you review, test and update such plans*	Choose an item >>
5. Are copies of your incident response, business continuity and/or disaster recovery plans kept in hard copy or in a separate and secure environment so that they are accessible in the event of a full network outage	Yes No
6. Do you have any third party service providers who you are dependent upon to have incident response, business continuity and/or disaster recovery plans	Yes No
*If **YES**, do you review the adequacy of such plans*	Yes No
7. How frequently do you generate backups	Choose an item >>
If backups are generated, where do you store them	Choose an item >>
8. Do you monitor for the successful generation of backups	Yes No
9. How frequently do you perform restoration testing of backups	Choose an item >>

10. Please provide information on the impact a disruption or failure of your IT environment would have on your operations (please include estimates on impact to revenue and third parties)

11. Please provide information on measures implemented to prevent and/or mitigate the impact of a disruption or failure of your IT environment including network and applications

PERSONNEL SECURITY

1.	Do you conduct background checks on potential employees as part of the recruitment process	Yes		No	
2.	Do you restrict user access based on job function and review access on at least an annual basis	Yes		No	
3.	How long after termination of employment do you typically revoke user access privileges	Choose an item >>			
4.	Have you conducted any security/data/privacy training/awareness courses for employees within the past 12 months	Yes		No	
5.	Does employee awareness training include targeted phishing campaigns and/or assessments to test understanding	Yes		No	

DIGITAL MEDIA LIABILITY

1.	Do you have a formal review process for both online and offline content prior to publishing	Yes		No	
	*If **YES**, are such reviews performed by a qualified legal resource*	Yes		No	
2.	Do you make use of any copyrighted material provided by others	Yes		No	
	*If **YES**, do you obtain written permission to use such material and confirm that use thereof does not infringe upon any intellectual property rights*	Yes		No	
3.	Do you provide any platforms or forums which users can post or upload their own content to	Yes		No	
	*If **YES**, is such content reviewed before publishing*	Yes		No	
	*If **YES**, do you have a process for quickly removing any offending content*	Yes		No	

CLAIMS AND INSURANCE HISTORY

1.	Have you ever had an insurance policy cancelled or been declined insurance cover	Yes		No	
2.	Have you suffered from any of the following within the past 5 years:				
	• Systems intrusion, tampering, malicious code attack, loss of data, extortion attempt, data theft or similar	Yes		No	
	• Unauthorised transmission or disclosure of sensitive information for which you are responsible	Yes		No	

- Allegations of invasion of privacy, that sensitive information has been compromised or content infringement

Yes		No	

- An unscheduled network outage or interruption

Yes		No	

3. 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

Yes		No	

*If **YES**, to any of the above, please provide additional information including remediation action taken*

LIMIT OF INDEMNITY

	Option 1	Option 2	Option 3	Option 4
Quote				
Deductible				

DECLARATION

I/We, the undersigned, declare that the statements set forth in this proposal form together with any other information supplied are true and correct and that I/we have not misstated or suppressed any material facts.

I/We agree that this proposal form together with any other information supplied by me/us shall form the basis upon which the contract of insurance is concluded and shall be incorporated therein.

I/We further undertake that in the event that the information provided changes between the date of this application and inception of cover, I/We will notify ITOO of such changes as soon as reasonably possible.

_____ _____

Name (duly authorised) Designation

_____ D D M M Y Y Y Y

Signature Date