iTOO™

In association with Hollard.

CYBER INSURANCE iTOO GO

Name of Insured _____

Physical address _____ Postal code _____

Email address _____ Contact number _____

Nature of operations Choose an item

If Other, please specify _____

Annual turnover/gross revenue R _____ VAT number _____

Policy inception date _____ Policy period _____ Retroactive date _____

Brokerage name _____ Limit of indemnity R Choose an item

You, the undersigned confirm that the Insured:

1. is not a financial institution; call center/telemarketer; payment card aggregator/processor; data processor/outsourcer; healthcare center/provider (turnover > R25 million); internet service/hosting/cloud storage provider; payroll processor; technology service provider (turnover > R25 million); telecommunications provider; gaming/gambling provider; government entity, state owned enterprise — YES ○ NO ○
2. is domiciled in South Africa and does not have operations outside South Africa to be covered under this policy — YES ○ NO ○
3. stores/processes less than 100 000 payment cards per year — YES ○ NO ○
4. is not aware of any circumstances within the past 3 years that would have, may give or has given rise to a claim under the coverage provided by this insurance policy — YES ○ NO ○
5. has implemented the following security controls: — YES ○ NO ○
   - 5.1 firewalls, anti-virus/anti-malware
   - 5.2 processes to apply security related patches/updates within 3 months of release
   - 5.3 password controls including: length of at least 8 characters; use of passwords not reasonably deemed easily guessable and account lockout as a result of at most 20 failed authentication attempts
   - 5.4 default installation/administration account passwords changed from the default password and where possible accounts are disabled, deleted or renamed
   - 5.5 administrative/remote access interfaces such as remote desktop protocol (RDP) are accessible exclusively over secured channels, e.g. virtual private network (VPN)
   - 5.6 physical access to server rooms/sensitive processing facilities is restricted
   - 5.7 **Sensitive System** activity logs are stored for at least 6 months
   - 5.8 backup and recovery procedures for **Sensitive Systems** and **Sensitive Data** including: weekly backup generation, monitoring for successful backup generation and testing the ability to restore from backups at least every 6 months.

Note: Should you have answered No to any of the above questions, please complete the standard ITOO Cyber Insurance Proposal Form. Upon receipt underwriters will review the application and revert.

Annual Turnover	Limit of Indemnity (per claim and in the annual aggregate)					
	*Deductible	R1 000 000	R2 500 000	R5 000 000	R10 000 000	**R25 000 000
R0-R10 000 000	15 000.00	5 045.00	7 970.00	11 465.00	17 655.00	44 135.00
R10 000 001-R25 000 000	25 000.00	6 805.00	10 755.00	15 480.00	22 275.00	44 740.00
R25 000 001-R50 000 000	25 000.00	8 505.00	13 445.00	19 335.00	27 825.00	55 890.00
R50 000 001-R75 000 000	50 000.00	9 790.00	15 460.00	22 245.00	32 005.00	64 290.00
R75 000 001-R100 000 000	50 000.00	10 745.00	16 975.00	24 415.00	35 140.00	70 585.00
R100 000 001-R250 000 000	100 000.00	15 045.00	23 760.00	34 185.00	49 195.00	98 825.00

Annual premiums reflected *** Each and every claim** ****Cyber extortion sub limited to R15 000 000.00**

Terms and Conditions:

- The applicable policy wording is the ITOO SME Cyber Insurance Policy wording, including:
  - A: Cyber Liability
  - B: Crisis Management and Notification Expenses
  - C: Data Recovery and Business Interruption
  - D: Cyber Extortion
  - E: Digital Media Liability
- Business interruption deductible is 12 hours and is sub limited to 50% of the annual limit of indemnity
- Premiums include 15% VAT and 20% Commission
- Quotation valid for 30 days from the date of declaration
- Unless otherwise requested, policy will run for 12 months from the date of inception
- Retroactive date as per inception date unless prior uninterrupted cyber insurance cover has been held
- Risk dependent ITOO reserves the right to review and adjust the above premiums

Declaration

This application does not bind the Proposer to buy or the insurer to issue the insurance, but it is agreed that this form shall be the basis of the contract should a policy be issued. The Proposer declares that the statements set forth in this application are true. The Proposer further declares that if the information supplied on this application changes between the date of this application and the time when the policy is issued, the Proposer will immediately notify the insurer of such changes and the insurer may withdraw or modify the proposed terms of insurance.

Name _____ Signature _____ Position _____ Date _____

ANNEXURE A

PHYSICAL DAMAGE

Please complete this section only if you require physical damage cover

Note: For the purposes of this proposal form connected tangible assets refers to: all tangible assets including internet of things devices; smart connected assets and all physical IT assets including servers, networking and endpoint devices, which are connected to your network and operating environment and that belong to or are rented, leased, or hired by you.

1.	Approximate value of connected tangible assets on your network	Original purchase cost	Last year	R	Current year	R
		Current replacement value	Last year	R	Current year	R

Please provide additional information on the nature of connected tangible assets on your network

2. Have you implemented controls such as firewalls to segment and protect connected tangible assets on your production line/facility networks from your general company network and the internet — YES ○ NO ○ N/A ○

Please provide additional information on the controls implemented to protect/restrict access to connected tangible assets on your production line or facility networks

3. Please indicate the estimated time it would take to source replacement or equivalent connected tangible assets (based on the assets to be covered which would be the hardest to replace or source alternatives for) — Choose an item

Please provide additional information on the availability of replacement or equivalent connected tangible assets

4. Please indicate the time after which the failure of your connected tangible assets would have a significant impact on your revenue and operations — Choose an item

CLAIMS AND INSURANCE HISTORY

1. Have you suffered any damage to connected tangible assets as a result of a cyber incident within the past 5 years — YES ○ NO ○
2. Have you suffered any unscheduled outage or interruption of connected tangible assets as a result of a cyber incident within the past 5 years — 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 this insurance policy — YES ○ NO ○

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

LIMIT OF INDEMNITY (max R250 000)

	Option 1	Option 2	Option 3	Option 4
Quote				
Deductible				

ANNEXURE B

E-FINANCIAL LOSS AND PHONE PHREAKING

Please complete this section only if you require e-financial loss cover

1.	Please advise	Total annual value of funds transferred electronically	R
		Maximum value per individual electronic transaction	R
		Average value of client funds held for which you are responsible (includes funds held in trust)	R
2.	Do you load payments via your own applications or via online banking applications		Choose an item
	If via your own applications, please state the name of the applications and whether these are in-house developed		
3.	Have you implemented two factor authentication to gain access to payment applications		YES ○ NO ○
4.	Have you implemented dual authorisation to load a new beneficiary		YES ○ NO ○
5.	Have you implemented segregation of duties between loading, releasing and authorising payments		YES ○ NO ○
6.	Have you implemented dual authorisation to release payments above a specified threshold		Choose an item
7.	Number of employees with access to load, release or authorise payments		Choose an item

PHONE PHREAKING

Please complete this section only if you require phone phreaking cover

1.	Do you make use of an internet connected telephony system (IP telephony)	YES ○ NO ○
	If YES please state the name of your system/service provider	
2.	What is your average monthly IP telephony costs including calls and bandwidth	R
3.	Do you host your IP telephony solution yourself or is this hosted by your service provider	Choose an item
4.	How frequently is your IP telephony environment subjected to third party security assessments, including vulnerability scanning. *Please attach the latest testing report.*	Choose an item
	• Were any serious concerns raised at your last test and have these been addressed	Choose an item
5.	Have all default installation and vendor accounts been secured via changing the account password and where possible disabling, deleting or renaming the accounts	YES ○ NO ○ N/A ○
6.	Have you implemented any active monitoring with automated alerts or thresholds for call charges and/or bandwidth	YES ○ NO ○

CLAIMS AND INSURANCE HISTORY

1.	Have you suffered any e-financial losses as a result of a cyber incident within the past 5 years	YES ○ NO ○
2.	Have you suffered any phone phreaking losses as a result of a cyber incident within the past 5 years	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 this insurance policy	YES ○ NO ○

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

LIMIT OF INDEMNITY (max R250 000)

	Option 1	Option 2	Option 3	Option 4
Quote				
Deductible				