Cyber Insurance
Proposal Form

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 _____ Post code _____
3. Primary contact Phone number _____ Email address _____
4. Registration number _____ VAT number _____
5. Closest match to your primary nature of business Choose an item
   If Other, please specify _____
6. Products and services offered

_____

_____

7. Subsidiary names (if applicable)

_____

_____

8. If applicable, please provide additional information on the level of integration and shared infrastructure with subsidiaries

_____

_____

9. Have you been involved in any mergers/acquisitions within the past 3 years Choose an item
10. Do you have any planned mergers/acquisitions within the next 12 months Yes ☐ No ☐
11. Revenue

Annual revenue	Last year	R	Current year	R
Gross e-business revenue	Last year	R	Current year	R
Information Technology budget	Last year	R	Current year	R
Information/Cyber security budget	Last year	R	Current year	R

12. Geographical split of gross revenue by region

South Africa	Last year	%	Current year	%
Africa (excl. SA)	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. Public facing URL addresses (websites and services such as file transfer facilities)

_____

_____

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

15. Your approximate number of external IP addresses — Choose an item

16. Your approximate number of servers (including virtual machines) — Choose an item

17. Approximate number of laptops utilised — Choose an item

18. Approximate number of employees receiving company emails to privately owned devices — Choose an item

SECURITY POLICIES AND STANDARDS

1. How is your information/cyber security structured

   Choose an item

2. Do you have a dedicated individual responsible for Information Security

   Choose an item

3. Do the individual(s) responsible for information security regularly report to executive management — Yes ☐ No ☐

4. Have you implemented information security policies/procedures and communicated these to employees — Yes ☐ No ☐

5. Are your security policies reviewed on at least an annual basis — Yes ☐ No ☐

6. Do you comply with privacy and data protection legislation applicable to all jurisdictions and industry standards in which you operate — Yes ☐ No ☐

7. Do you have a data classification policy including security requirements for sensitive data — Yes ☐ No ☐

8. On correspondence relating to invoicing and receiving of monies, do you have warnings around business email compromise (BEC) fraud and changing of bank account details — N/A ☐ Yes ☐ No ☐

9. Please specify any security certifications you hold (for example PCI DSS)

10. Do you enforce a "strong password policy" across all accounts, including:

- Minimum password length restriction — Choose an item
- 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 — Yes ☐ No ☐
- Account lockout as a result of failed authentication attempts — Choose an item
- How long are accounts locked out for due to failed authentication attempts — Choose an item
- Setting different, random passwords for local administrator accounts across all domain attached computers (Local Administrator Password Solution) — Yes ☐ No ☐
- Multi factor authentication for:
  - – Administrator and privileged level access — N/A ☐ Yes ☐ No ☐
  - – Critical applications and sensitive data access — N/A ☐ Yes ☐ No ☐
  - – Software as a service (SaaS) email solutions e.g. Microsoft Office365 — N/A ☐ Yes ☐ No ☐
  - – Sensitive cloud based applications and systems — N/A ☐ Yes ☐ No ☐
  - – Employee remote access — N/A ☐ Yes ☐ No ☐
  - – Third party remote access — N/A ☐ Yes ☐ No ☐
  - – How have you implemented the additional factor for multi factor authentication: — Choose an item

  If Other, please provide additional information on how you have implemented the additional factor:

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

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

11. For what period of time do you retain audit logs for hardware devices (including firewalls as implemented in your environment) and software (including Active Directory as implemented in your environment) Choose an item

12. How regularly do you analyse audit logs/reports/alerts to identify anomalies or unusual activities Choose an item

PATCH AND VULNERABILITY MANAGEMENT

1. Have you implemented a patch and vulnerability management policy *(If yes, please attach a copy)* Yes ☐ No ☐

2. How frequently are your IT environments subjected to penetration testing Choose an item
   - Were any serious concerns raised at your last test and have these been addressed Choose an item

3. How frequently are your IT environments subjected to third party security assessments, including vulnerability scanning Choose an item
   - Were any serious concerns raised at your last test and have these been addressed Choose an item
   - If all serious concerns have not been addressed, please provide details of outstanding items with remediation actions to be taken and associated timelines

4. Did the scope of the testing performed include both your internal and external IT environment Yes ☐ No ☐

5. Do you perform penetration testing and/or secure code reviews on all new systems/software prior to deployment Yes ☐ No ☐

6. How long after release do you implement security related patches and updates on computers, servers and network appliances (routers, firewalls, etc.):
   - Critical patches and updates (Common Vulnerability Scoring System (CVSS) severity 9.0-10.0) Choose an item
   - Over the past 3 months, how successful have you been in implementing critical patches within this target time frame? Choose an item
   - High patches and updates (CVSS severity 7.0-8.9) Choose an item
   - Medium patches and updates (CVSS) severity 5.0-6.9) Choose an item

7. How long after release do you apply patches for components of self developed applications e.g. software development kits Choose an item

SENSITIVE AND PRIVATE INFORMATION

1. To determine your potential data exposure, please provide the **APPROXIMATE NUMBER** of **EMPLOYEE** and **CLIENT** unique data records that you have collected/stored/processed for each of the following data types:

   Bank records or financial account details Choose an item

   Medical records or health information Choose an item

   Payment card details Choose an item
   - 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) Choose an item

   Biometric data (e.g. fingerprints for access control) Choose an item

   Third party corporate confidential data Choose an item

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

3. Are all Internet-accessible systems (e.g. web servers) segregated from your trusted network (e.g. within a demilitarized zone (DMZ) or hosted at a 3rd party provider) N/A ☐ Yes ☐ No ☐

4. Have you implemented data retention and secure destruction policies for physical and electronic data and assets Yes ☐ No ☐

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

5. Have you disabled employee write access to USB devices — Yes ☐ No ☐

6. 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

   _____

   _____

7. Have you implemented a policy on the use, protection and lifetime of cryptographic keys — N/A ☐ Yes ☐ No ☐

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 _____
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 your 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
    - Were any serious concerns raised at your last test and have these been addressed

    Choose an item

SECURITY IMPLEMENTATION

1. Do you operate a local network or operate solely on cloud services — Choose an item

If you are operating purely on cloud services, please proceed to question 11

2. Please indicate which of the following you have implemented (please select all that apply):
   - Next generation firewalls at all breakout points to external networks — Yes ☐

     If Yes, please specify the firewall technology you have implemented _____
   - Segmentation to protect sensitive data and resources within the network — Yes ☐
   - Identity and Access Management (IAM) or Identity as a Service (IDaaS) — Yes ☐
   - Privileged Identity and Access Management (PIM/PAM) — Yes ☐
   - Security Incident and Event Management (SIEM) — Yes ☐
   - Security Orchestration, Automation and Response (SOAR) — Yes ☐
   - Proactive monitoring of events on sensitive/critical servers and applications e.g. Security Operations Center (SOC) — Yes ☐

     What % of sensitive / critical servers are monitored on a proactive basis: — Choose an item

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

If Yes, please provide additional information on the monitoring performed including technologies being used

- Cyber threat intelligence (CTI) function — Yes ☐
- Data loss prevention (DLP) tools — Yes ☐
- Route all outbound web requests through a web proxy — Yes ☐
- Web/Internet content filtering — Yes ☐

3. Do you have a comprehensive Configuration Management Database (CMDB): Yes ☐ No ☐
   - If Yes, What % of your environment is covered by your CMDB: Choose an item
4. Do you have a process to discover and identify hardware assets on your network Yes ☐ No ☐
   - If Yes, how frequently do you run this: Choose an item
5. Do you apply a strict configuration management approach and develop secure images that are used to build all newly deployed computers, servers and applications Yes ☐ No ☐
6. Do you block FTP, SSH, RDP, Telnet, SNMP, SMB and SMTP on externally exposed systems Yes ☐ No ☐
7. Have you implemented controls to restrict unauthorised access to sensitive data via your wireless network N/A ☐ Yes ☐ No ☐
8. Do you provide remote access to your network (please select all that apply):
   - No remote access is allowed — Yes ☐
   - Zero trust network access (ZTNA) is utilised — Yes ☐
   - All remote connections are via Virtual Private Network (VPN) — Yes ☐
   - All remote connections require MFA — Yes ☐
   - Accounts including installation and administration are protected from brute force password attacks — Yes ☐
   - A pre-login security assessment of the device is performed before granting access — Yes ☐
   - Remote desktop protocol (RDP) is blocked for connections from external to the network — Yes ☐
9. Have you implemented physical controls such as reception or access control mechanisms to restrict access to your offices, server room and other sensitive processing facilities Yes ☐ No ☐
10. Are you making use of any unsupported software or operating systems Yes ☐ No ☐

    If Yes, please provide additional information including: which software or operating system, 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

11. Please indicate which of the following you have implemented (please select all that apply):
    - Cloud access security broker (CASB) — Yes ☐
    - Endpoint protection (e.g. Anti-virus) which is updated per vendor recommendations — Yes ☐

      If Yes, please specify the endpoint protection you have implemented
      - Please indicate the % of your environment that is covered by your endpoint protection solution:
        - – Laptops and workstations: Choose an item
        - – Mobile devices, excluding laptops: Choose an item
        - – Servers: Choose an item
    - Anti-tamper features enabled — Yes ☐ No ☐
    - Web application firewalls (WAF) — Yes ☐ No ☐
    - Mobile Device Management (MDM) including access control and remote device wipe — Yes ☐ No ☐
    - Application white-listing to only allow for execution of authorised applications — Yes ☐ No ☐

- Secure client invoicing system Yes ☐ No ☐

  If Yes, please provide additional information on the secure invoicing performed including technologies being used

- Email filtering solutions
  - – Sender policy framework (SPF) Yes ☐ No ☐
  - – Domain Keys Identified Mail (DKIM) Yes ☐ No ☐
  - – DMARC (Domain-based Message Authentication, Reporting and Conformance) Yes ☐ No ☐
- Email security including URL rewriting, malware protection and protection against impersonation attacks Yes ☐ No ☐

  If Yes, please specify the email security technology implemented

ACCESS MANAGEMENT

1. Do you manage access permissions, including application of the principles of least privilege and separation of duties — Choose an item
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 general employees have local administrator rights on their laptops/desktops — Yes ☐ No ☐
4. Do you restrict user access based on job function and review access on at least an annual basis — Yes ☐ No ☐
5. How long after termination of employment do you typically revoke user access privileges? — Choose an item
6. Number of employees with system administration privileges

Permanent		Contractors		Temporary	

7. Are administrator accounts managed via just-in-time access, time bound, and/or require approvals to provide privileged access — Yes ☐ No ☐
8. How frequently are administrator account passwords changed? — Choose an item
9. Do you require that network administrators have separate accounts for 'regular' and 'privileged' access — Yes ☐ No ☐
10. Do you block privileged access accounts from accessing online services (e.g. web browsing, email) — Yes ☐ No ☐
11. Do you keep privileged account credentials in a password safe, requiring users to check out the credential which is then rotated afterwards — Yes ☐ No ☐
12. Do you keep a log of all privileged account use for at least 30 days — Yes ☐ No ☐
13. Do you actively monitor privileged account access — Yes ☐ No ☐
14. Have you disabled or denied interactive logons for system accounts — Yes ☐ No ☐
15. Do you review authorisations for non-privileged access rights at least annually? — Yes ☐ No ☐

CHANGE MANAGEMENT

1. Have you implemented a formal change control process including risk assessments, testing, approval and roll back — N/A ☐ Yes ☐ No ☐
2. Do you segregate your development and testing environments from the production environment — N/A ☐ Yes ☐ No ☐
3. Do you conduct automated security tests or code analysis during system development — N/A ☐ Yes ☐ No ☐
4. For self developed and / or custom applications do you have secure backup of the code base which is protected from your production environment so that the likelihood of one incident impacting live and backup code bases is mitigated — N/A ☐ Yes ☐ No ☐

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

THIRD PARTY SERVICE PROVIDERS

Function	Outsourced		Third party provider's 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 CONTINUITY 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
   - Do you ensure that at any time you have a backup or replicated copy which is protected from your production environment so that the likelihood of one incident impacting live and backup data is mitigated Backup or replicated copies can be protected via being isolated, offline, immutable or via other ransomware protected backup solutions — Yes ☐ No ☐

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

- Please provide additional information on how you protect backup copies from being impacted by for example a widespread ransomware incident

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. Have you conducted any security/data/privacy training/awareness courses for employees within the past 12 months Yes ☐ No ☐
   - If Yes, please specify the names of any employee awareness training solutions being used

3. Does employee awareness training include targeted phishing campaigns and/or assessments to test understanding Yes ☐ No ☐

DIGITAL MEDIA MANAGEMENT

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 ☐

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

OPERATIONAL TECHNOLOGY (OT)

The term Industrial control system (ICS) embraces several types of control systems and associated instrumentation used for industrial process control. Operational Technology (OT) is defined as the collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process. Industrial Security in this context is used to secure Operational Technology.

Please complete this section only if you have ICS and OT.

SECURITY POLICIES AND STANDARDS

1. Do your information security policies/procedures cover your OT environments — Yes ☐ No ☐
2. Have you documented the data flows and communication paths for your OT environments — Yes ☐ No ☐

PATCH AND VULNERABILITY MANAGEMENT

1. How frequently are your OT environments subjected to penetration testing — Choose an item
   - Were any serious concerns raised at your last test and have these been addressed — Choose an item
2. How frequently are your OT environments subjected to vulnerability scanning — Choose an item
   - Were any serious concerns raised at your last test and have these been addressed — Choose an item

SECURITY IMPLEMENTATION

1. Have you implemented endpoint protection (e.g. Anti-virus) which is updated per vendor recommendations on industrial systems — Yes ☐ No ☐
2. Do you apply a strict configuration management approach and develop secure images that are used to build all newly deployed industrial systems — Yes ☐ No ☐
3. Have you segregated your OT environment from the general company network — Yes ☐ No ☐

   If yes, please provide additional information including the technology used to segregate the environments.

   _____

   _____
4. Do you manage access permissions, including the application of the principles of least privilege and separation of duties for your OT environments — Choose an item
5. Do you or any supplier (e.g. for remote maintenance access) have local internet breakouts from your OT environment — Yes ☐ No ☐
6. Do you allow for remote access to your OT environments (please select all that apply):
   - No remote access is allowed — Yes ☐
   - Zero trust network access (ZTNA) is utilised — Yes ☐
   - All remote connections are via Virtual Private Network (VPN) — Yes ☐
   - All remote connections require multi factor authentication (MFA) — Yes ☐
   - Access is restricted to selected individuals — Yes ☐
   - Accounts including installation and administration are protected from brute force password attacks? — Yes ☐
   - A pre-login security assessment of the device is performed before granting access? — Yes ☐
   - Remote desktop protocol (RDP) is blocked for connections from external to the network? — Yes ☐
7. Have you implemented application whitelisting on OT systems — Yes ☐
8. Have you implemented technology to monitor OT environment so that it can update the hardware inventory and remove unauthorised devices — Yes ☐
9. Do you use industrial wireless technologies (e.g. Wireless HART, Bluetooth) with enabled access control and encryption features in dedicated networks — Yes ☐ No ☐
10. How long after release do you implement security related patches and updates on OT systems and applications:

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

- Critical patches and updates (Common Vulnerability Scoring System (CVSS) severity 9.0-10.0) — Choose an item
- Over the past 3 months, how successful have you been in implementing critical patches within this target time frame? — Choose an item
- High patches and updates (CVSS severity 7.0-8.9) — Choose an item
- Medium patches and updates (Common Vulnerability Scoring System (CVSS) severity 5.0-6.9) — Choose an item

11. How long after release do you apply patches for components of self developed applications e.g. software development kits — Choose an item

12. Are you making use of any unsupported software or operating systems in your OT environment — Yes ☐ No ☐

- If Yes, please provide additional information including: whether these are visible to external networks; the nature of systems running on these; reasons for not updating; any controls implemented to mitigate the risk and plans to remediate

INCIDENT RESPONSE, BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

1. Do your critical industrial systems have redundant designs or failover capabilities to prevent physical damage or business interruption — Yes ☐ No ☐

2. How frequently do you generate backups of OT systems' including firmware, operating systems, applications, licenses and configuration data sets — Choose an item
   - Do you ensure that at any time you have a backup copy which is not connected to or accessible via your OT or production environment so that the likelihood of one incident impacting live and backup data is mitigated — Yes ☐ No ☐

   Please provide additional information on how you protect backup copies from being impacted by for example, a widespread ransomware incident

3. How frequently do you perform testing of backups of OT to validate the accuracy and integrity of the backup — Choose an item

ADDITIONAL COMMENTS

1. Would you like to share further information or details regarding your ICS and OT security

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

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: — Yes ☐ No ☐

   - 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 nature of the incident, damages incurred and remediation action taken

_____

_____

_____

PRIVACY

In accordance with the applicable laws, we may be required to share your personal information with other insurers, industry bodies, credit agencies and service providers. This includes information about your insurance, claims and premium payments. We do this to provide insurance services, prevent fraud, assess claims and conduct surveys. We will treat your personal information with caution and have put reasonable security measures in place to protect it. By signing this application for insurance, you agree to the processing and sharing of your personal information.

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

Signature _____ Date _____

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**

ANNEXURE A

Theft of Funds (R250 000 or 10% of limit of indemnity subject to maximum limit of R5 000 000)

Please complete this section only if you require theft of funds cover

1. Total annual value of funds transferred electronically R _____
2. Maximum value per individual electronic transaction R _____
3. Average value of client funds held for which you are responsible (includes funds held in trust) R _____
4. 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

5. Have you implemented two factor authentication to gain access to payment applications Yes ☐ No ☐
6. Have you implemented dual authorisation to load a new beneficiary? Yes ☐ No ☐
7. Have you implemented segregation of duties between loading, releasing and authorising payments Yes ☐ No ☐
8. Have you implemented dual authorisation to release payments above a specified threshold Choose an item
9. Number of employees with access to load, release or authorise payments Choose an item

CLAIMS AND INSURANCE HISTORY

1. Have you suffered any theft of funds losses as a result of a cyber incident within the past 5 years Yes ☐ No ☐
2. 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

iTOO Special Risks (Pty) Ltd
Villa Arcadia, 22 Oxford Road, Parktown, Gauteng, 2193 | PO Box 87419, Houghton, 2041 | Tel: 0861 004 866 | Email: info@itoo.co.za | **www.itoo.co.za**