The Liability Company.

LIABILITY MATTERS

Crime & Civil Liability Proposal Form

This proposal form relates to both sections of the policy. Section 1 (Crime) responds to losses discovered by you during the Period of Insurance; Section 2 (Civil Liability) responds to claims first made against you during the Period of Insurance. Please refer to the Policy Wording for the applicable discovery and notification requirements.

- This proposal form must be completed and signed by a duly authorised representative of the proposer.
- Please answer ALL questions. If a question does not apply to your organisation, write “N/A”. If insufficient space is provided, please use additional sheets on your company letterhead.
- Completing and signing this proposal form does not bind the insurer to issue a policy.
- By signing this proposal form you confirm that you have read and understood its contents and that all information provided is true and correct to the best of your knowledge and belief.

Disclosure

You must disclose to the Insurer all facts, matters or circumstances which are material to or which may influence the Insurer in the consideration of this risk. This duty of disclosure continues throughout the currency of any policy issued.

If you do not understand any part of this document, please contact your broker before you sign it. You will be bound by the answers which are given, and by the information provided by you in the proposal form. It is in your interest to make sure that all information is properly understood. If you are in any doubt, discuss the issue with your broker or disclose the information to the Insurers.

Attachments

Before you return this form, have you included the following (please indicate yes or no):

Latest audited Annual Financial Statements and/or Interim Reports	◯ Yes ◯ No
Auditor's Management Letter (latest) and Management's written response	◯ Yes ◯ No
Organisational chart	◯ Yes ◯ No
Copy of standard client contract or letter of engagement (if applicable)	◯ Yes ◯ No

Please attach details where there is not enough space to answer any question in the space provided on this proposal form.

The Liability Company (Pty) Ltd
35 Oxford Office Park, 3 Bauhinia Street
Highveld Techno Park, Centurion
PO Box 17541, Lyttleton, Pretoria, 0140
Authorised FSP 50828

Our Risk Carriers
Underwritten by Old Mutual Insure Limited (FSP 12), a licensed financial services provider and non-life insurer.

Contact Us
T +27 (12) 667 2441
E info@theliabilitycompany.com
W www.theliabilitycompany.com

OLDMUTUAL INSURE

1. Client Information

Full legal name of the Insured
Please attach a list of subsidiaries if cover is required for them.

Trading name (if different)

Principal / registered address

Postal address (if different)

Company registration number

VAT registration number

Financial Services Provider (FSP) number, if applicable

Website address

Financial year end (month)

Total annual revenue (R)

Total assets (R)

Main contact for this proposal

Contact's position / title

Contact's telephone number

Contact's email address

1.1 Nature of Business — please describe your principal business activities and the approximate percentage of total revenue derived from each:

Activity Description	% of Revenue

Has the Proposer provided any new services to its clients in the last 12 months? ◯ Yes ◯ No

If yes, please provide details:

Does the Proposer intend on offering any new services in the next 12 months? ◯ Yes ◯ No

If yes, please provide details:

2. Legal Constitution

Please tick the applicable entity type:

- ☐ a. Sole Proprietor
- ☐ b. Private Company (Pty) Ltd
- ☐ c. Personal Liability Company (Inc.)
- ☐ d. Public Company (Ltd)
- ☐ e. State Owned Company (SOC)
- ☐ f. Non-Profit Company (NPC)
- ☐ g. Other

Date of incorporation / registration

Name and designation of the authorised signatory

3. Subsidiaries and Associated Companies

Are subsidiaries or associated companies to be included within the scope of this policy (shared limit)? ◯ Yes ◯ No

3. Subsidiaries and Associated Companies (continued)

If yes, please list all subsidiaries and associated companies to be included:

Name of Entity	% Owned	Country of Incorporation	Date Established / Acquired	Principal Activities

Is the Proposer itself a subsidiary of another company? ◯ Yes ◯ No

If yes, please name the ultimate holding company:

Has the Proposer been acquired by another entity, or merged with or acquired any other business during the last 12 months? ◯ Yes ◯ No

If yes, please provide details:

Is the Proposer party to any joint venture or partnership agreement? ◯ Yes ◯ No

If yes, please provide details:

4. Staff Complement

4.1 Please provide a breakdown of your staff by function:

Employee Category	Number of Staff	No. of Locations
Directors / Officers		
Finance / Accounting / Treasury		
Operations / Administration		
IT / Technology		
Sales / Client-Facing		
Procurement / Supply Chain		
Warehouse / Stock Control		
Other (please specify)		
TOTAL		

4.2 Employee Controls:

Are criminal history, credit and employment history checks conducted on ALL new employees prior to appointment? ◯ Yes ◯ No

Are all employees required to take a minimum of two consecutive weeks' leave per calendar year? ◯ Yes ◯ No

Do you have established and enforced procedures for terminating employee access to systems and premises upon resignation or dismissal? ◯ Yes ◯ No

Are all employees subject to a written code of conduct / ethics policy? ◯ Yes ◯ No

Are employees required to sign a confidentiality / non-disclosure agreement? ◯ Yes ◯ No

Are managers or supervisors required to rotate between different roles or functions periodically? ◯ Yes ◯ No

Are dual controls maintained over the handling of negotiable instruments, access codes and test keys? ◯ Yes ◯ No

4. Staff Complement (continued)

Have any employees been dismissed for dishonesty, fraud or financial misconduct in the past 3 years? ◯ Yes ◯ No

If yes, please provide details:

5. Financial Controls — Cash & Electronic Funds Transfers

Approximate annual value of all EFT / fund transfers processed (R)

Maximum single payment authorised without dual approval (R)

5.1 Payment Authorisation Controls:

Is dual authorisation required for ALL electronic payments, regardless of value? ◯ Yes ◯ No

Are payment limits assigned to individual users based on seniority / role? ◯ Yes ◯ No

Are all new payees / beneficiaries independently verified before first payment? ◯ Yes ◯ No

Are changes to existing beneficiary bank account details subject to a callback or out-of-band verification procedure? ◯ Yes ◯ No

Are all supporting documents (invoices, purchase orders, etc.) validated and matched to payment instructions before authorisation? ◯ Yes ◯ No

Are bank statements reconciled to the accounting system on a monthly basis, independently of the person responsible for processing payments? ◯ Yes ◯ No

Are petty cash holdings subject to regular independent count and reconciliation? ◯ Yes ◯ No

Is there an established procedure for reporting and investigating unusual or unscheduled payments? ◯ Yes ◯ No

5.2 Salary & Payroll Controls:

Is the payroll independently reviewed each month prior to payment to verify accuracy and active-employee status? ◯ Yes ◯ No

Are changes to payroll standing data (bank account numbers, salary levels) authorised by HR and independently verified? ◯ Yes ◯ No

Is the payroll function outsourced? If yes, is there an audit protocol included in the outsourcing agreement? ◯ Yes ◯ No

If yes, please provide details:

5.3 Cash Handling:

Maximum cash held on premises at any one time (R)

Is cash collected by an accredited cash-in-transit / security company? ◯ Yes ◯ No

Are cash registers or tills independently counted and reconciled daily? ◯ Yes ◯ No

Do any employees handle cash above R50,000 on a single occasion? ◯ Yes ◯ No

If yes, please provide details:

5A. Banking & Payment Fraud Exposure

Does the organisation use multi-factor authentication (MFA) for all online banking platforms? ◯ Yes ◯ No

Are employees trained to identify and resist Business Email Compromise (BEC) and invoice fraud attempts? ◯ Yes ◯ No

5A. Banking & Payment Fraud Exposure (continued)

Is there a written procedure requiring independent verbal confirmation of payment instruction changes received by email? ◯ Yes ◯ No

Are employees trained to detect deepfake voice / video impersonation of management or clients? ◯ Yes ◯ No

Is there a process for employees to report suspected fraud or social engineering attempts without fear of reprisal? ◯ Yes ◯ No

Have employees received formal training on social engineering / phishing awareness in the last 12 months? ◯ Yes ◯ No

Has the organisation experienced any Business Email Compromise, invoice fraud or social engineering incident in the last 3 years? ◯ Yes ◯ No

If yes, please provide details:

Does the organisation subscribe to any anti-fraud or threat-intelligence service? ◯ Yes ◯ No

5B. Client Money / Trust Money

Does the organisation hold or handle money or assets belonging to clients or third parties? ◯ Yes ◯ No

If yes — approximate total value of third-party funds under administration / custody (R)

Are third-party funds held in separate, dedicated trust accounts distinct from the organisation's own operating accounts? ◯ Yes ◯ No

Are trust accounts reconciled to client records monthly (or more frequently)? ◯ Yes ◯ No

Is access to trust accounts restricted to authorised signatories under dual control? ◯ Yes ◯ No

Has any trust account ever been subject to a regulatory enquiry, shortfall or complaint? ◯ Yes ◯ No

If yes, please provide details:

6. Procurement Controls

Is there a formal, documented procurement policy in place? ◯ Yes ◯ No

Are all procurement decisions above a defined threshold subject to a competitive tender or quotation process? ◯ Yes ◯ No

Are tender evaluations and contract awards made by a panel or committee (rather than a single individual)? ◯ Yes ◯ No

Are all procurement staff required to declare conflicts of interest (including relationships with suppliers) in writing? ◯ Yes ◯ No

Are all supplier / vendor contracts in writing and reviewed by legal counsel before signature? ◯ Yes ◯ No

Are post-tender negotiations conducted in writing? ◯ Yes ◯ No

Are all approved suppliers / vendors maintained on a formal vendor register? ◯ Yes ◯ No

Has any employee been disciplined or dismissed for procurement-related misconduct in the last 5 years? ◯ Yes ◯ No

If yes, please provide details:

7. Physical Security

Are all office premises protected by an active alarm system linked to an armed response provider? ◯ Yes ◯ No

7. Physical Security (continued)

Is access to the office premises restricted by electronic access control (key card, biometric or similar)? ◯ Yes ◯ No

Are all areas where cash, negotiable instruments or sensitive records are held secured by locked cabinets, safes or vaults? ◯ Yes ◯ No

Is CCTV installed at all entry / exit points and critical internal areas? ◯ Yes ◯ No

Are CCTV recordings retained for at least 90 days? ◯ Yes ◯ No

Have the premises suffered any break-in, theft or attempted theft in the last 3 years? ◯ Yes ◯ No

If yes, please provide details:

Name and registration number of armed response / security company

8. Information Technology

Is access to all computer systems controlled by individual user accounts with role-based access rights? ◯ Yes ◯ No

Are passwords required to be changed at least every 90 days, and is this enforced by system controls? ◯ Yes ◯ No

Is multi-factor authentication (MFA) enforced for all remote access to company systems? ◯ Yes ◯ No

Are source documents and records secured to prevent unauthorised modification prior to entry into the computer system? ◯ Yes ◯ No

Is access to the data processing / server environment restricted to authorised IT personnel only? ◯ Yes ◯ No

Is the IT environment protected by up-to-date anti-virus, anti-malware and firewall solutions? ◯ Yes ◯ No

Are all software and operating systems maintained on current, supported versions with security patches applied promptly? ◯ Yes ◯ No

Are full system backups performed regularly and stored off-site or in a separate, isolated environment? ◯ Yes ◯ No

Are programming / development staff prevented from accessing live production systems? ◯ Yes ◯ No

Does the organisation have a formally documented IT security policy? ◯ Yes ◯ No

Does the organisation hold any recognised information security certification (e.g. ISO 27001)? ◯ Yes ◯ No

Name of your primary IT security / managed services provider

8A. Cyber-Enabled Crime Controls

Does the organisation have a designated Data Security Officer or equivalent? ◯ Yes ◯ No

Is there a written incident response plan for cyber security breaches? ◯ Yes ◯ No

Are intrusion attempts and unauthorised access events monitored and logged on a continuous basis? ◯ Yes ◯ No

Does the organisation conduct regular phishing simulation exercises or penetration testing? ◯ Yes ◯ No

Are employees required to complete formal cyber security awareness training at least annually? ◯ Yes ◯ No

Is web filtering or email gateway filtering deployed to block malicious links and attachments? ◯ Yes ◯ No

8A. Cyber-Enabled Crime Controls (continued)

Has the organisation suffered any cyber security incident, data breach or ransomware attack in the last 3 years? ◯ Yes ◯ No

If yes, please provide details:

9. Internal Audits

Does the organisation have an internal audit function? ◯ Yes ◯ No

If yes — how often are full internal audits conducted?

Is the internal audit function independent of the finance and operations functions? ◯ Yes ◯ No

Does the internal audit scope include a review of segregation of duties, system access controls and payment controls? ◯ Yes ◯ No

Were any significant control weaknesses identified in the most recent internal audit? ◯ Yes ◯ No

If yes, please describe and confirm remediation status:

9A. Governance and Senior Management Controls

Are all directors and employees required to declare outside business interests and relationships that may create a conflict of interest? ◯ Yes ◯ No

Is there a formal whistleblowing / tip-off hotline or confidential reporting mechanism in place? ◯ Yes ◯ No

Does the Board of Directors or an Audit Committee formally review financial controls and internal audit findings at least annually? ◯ Yes ◯ No

Are management accounts and financial results reviewed by an independent party (audit committee, board or equivalent) at least quarterly? ◯ Yes ◯ No

Does the organisation have a formal fraud response plan, including defined escalation procedures? ◯ Yes ◯ No

Has any director or senior manager been subject to any disciplinary action, regulatory sanction, or criminal investigation in the last 5 years? ◯ Yes ◯ No

If yes, please provide details:

9B. Outsourcing and International Exposure

Does the organisation outsource any financial, IT or operational functions to third-party service providers? ◯ Yes ◯ No

Are contracts with outsourced service providers reviewed by legal counsel and subject to formal service level agreements? ◯ Yes ◯ No

Are outsourced service providers required to carry their own professional indemnity / crime insurance? ◯ Yes ◯ No

Does the organisation have operations, employees or clients in countries outside South Africa? ◯ Yes ◯ No

Does the organisation have any exposure to the United States of America or Canada (operations, clients, employees or assets)? ◯ Yes ◯ No

If yes, please provide details:

9B. Outsourcing and International Exposure (continued)

Please list the key outsourced service providers (name, function)

10. External Audits

Name of external auditor / firm of auditors

Date of last completed external audit

Have all material recommendations from the external auditor's management letter been implemented? ◯ Yes ◯ No

Has the external auditor issued a qualified, adverse or disclaimer of opinion in the last 3 years? ◯ Yes ◯ No

If yes, please provide details:

11. Professional Services & Civil Liability

This section relates specifically to Section 2 (Civil Liability) of the policy. Please answer all questions in respect of the professional services for which coverage is required under this policy.

11.1 Services and Regulatory Status:

Please describe in detail the professional services provided to clients for which Civil Liability cover is required:

FSCA / FSRA licence category and FSP number (if applicable)

Other regulatory licences held (specify regulatory body and licence type)

Is the organisation licensed and compliant with all legislation applicable to its business activities? ◯ Yes ◯ No

Has the organisation received any admonishment, warning, directive or sanction from any regulatory authority in the last 5 years? ◯ Yes ◯ No

If yes, please provide details:

11.2 Client Engagements and Contracts:

Does the organisation use a standard written contract or letter of engagement with all clients? ◯ Yes ◯ No

Are client contracts regularly reviewed by an attorney or in-house legal counsel? ◯ Yes ◯ No

Are all publications, marketing materials and client communications reviewed by legal counsel and/or a compliance officer prior to release? ◯ Yes ◯ No

Does the organisation have any contracts with service providers that limit or waive the organisation's rights of recourse against that service provider? ◯ Yes ◯ No

If yes, please provide details:

Does the organisation have a documented client complaints handling procedure? ◯ Yes ◯ No

How are client complaints recorded, investigated and resolved? (brief description)

11.3 Prior Claims and Circumstances (Civil Liability — Claims Made):

Important: Please disclose ALL known circumstances that could reasonably give rise to a civil liability claim, even if no formal claim has yet been made. Failure to disclose may prejudice cover.

11. Professional Services & Civil Liability (continued)

Is the organisation currently involved in any litigation as a defendant, or subject to any regulatory investigation, relevant to the services described in this proposal? ◯ Yes ◯ No

If yes, please provide details:

Are you or any principal aware of any act, error, omission or circumstance that could reasonably give rise to a claim against the organisation for Civil Liability? ◯ Yes ◯ No

If yes, please provide details:

Has any application for Professional Indemnity or Civil Liability insurance by the organisation ever been declined or cancelled? ◯ Yes ◯ No

If yes, please provide details:

11.4 Trust Services (for Optional Extension — Professional Trust Services):

Does the organisation provide trust administration, fiduciary services or act as trustee of any trust or special purpose vehicle? ◯ Yes ◯ No

Do any employees act as trustee in a personal capacity at the organisation's behest? ◯ Yes ◯ No

If yes, please provide details:

Minimum qualifications required for employees acting as trustee

Describe internal monitoring procedures for trust activities

11.5 Document Control (for Optional Extension — Loss of Documents):

Does the organisation maintain a formal document retention and destruction policy? ◯ Yes ◯ No

Are original client documents and title deeds held in a secure, fireproof environment? ◯ Yes ◯ No

Are all documents scanned / digitised and backed up electronically? ◯ Yes ◯ No

11.6 Inter-Company Arrangements (for Optional Extension — Inter-Company Liability):

Does the organisation provide professional services to any subsidiary, holding company or associated entity under a formal, arm's-length written agreement? ◯ Yes ◯ No

If yes, please provide details:

12. Previous / Current Insurance

	Crime Insurance	Civil Liability Insurance
Name of current insurer		
Policy number		
Sum Insured / Limit of Indemnity (R)		
Deductible / Excess (each and every loss / claim) (R)		
Policy expiry date		
Retroactive date		
Annual premium (R)		

Please attach a copy of the current policy wording and schedule. Premium information may be redacted.

13. Claims History

Please provide details of ALL losses, claims and circumstances relevant to this insurance sustained or notified during the past FIVE (5) years, whether insured or not and whether or not a deductible / excess was applied. Attach additional sheets if required.

13.1 Crime Losses (Section 1 — Losses Discovered):

Nature of Loss / Claim	Date Committed / Occurred	Date Discovered / Reported	Amount (R)	Insured / Uninsured	Status / Recovery

13.2 Civil Liability Claims (Section 2 — Claims Made):

Nature of Loss / Claim	Date Committed / Occurred	Date Discovered / Reported	Amount (R)	Insured / Uninsured	Status / Recovery

13.3 For each loss / claim listed above, please describe the corrective measures taken to prevent recurrence and any action taken against the perpetrator:

14. Sum Insured and Deductible

Please indicate the Sum Insured and Deductible (each and every loss) required. You may complete up to three options for quotation purposes. Note: Crime (Section 1) is the Aggregate Sum Insured for all losses discovered during the Period of Insurance; Civil Liability (Section 2) is the Aggregate Sum Insured for all claims made during the Period of Insurance.

Cover	Option 1	Option 2	Option 3
Section 1 — Crime: Sum Insured (R)			
Section 1 — Crime: Deductible each and every loss (R)			
Section 2 — Civil Liability: Sum Insured (R)			
Section 2 — Civil Liability: Deductible each and every loss (R)			
Combined Overall Aggregate Limit (R) — if different			

15. Crime Extensions — Section 1

Tick all extensions required. Extensions are subject to the terms, conditions and exclusions of the policy and to insurer acceptance.

	Extension	Sub-limit / Notes
☐	**Unidentifiable Employees** Cover where the specific employee causing the loss cannot be identified.	
☐	**Extended Cover for Past Employees** Extends cover to dishonest acts of employees for 90 days following cessation of employment.	
☐	**Forged Transfer Instructions** Specific sub-limit for losses arising from forged or fraudulent payment instructions.	

15. Crime Extensions — Section 1 (continued)

	Extension	Sub-limit / Notes
☐	**Reinstatement of Sum Insured** Sum Insured reinstated once in respect of losses wholly unrelated to any previous paid loss.	

16. Civil Liability Extensions — Section 2

Tick all optional extensions to Section 2 (Civil Liability) required. Extensions are subject to the terms, conditions and exclusions of the policy and to insurer acceptance.

	Extension	Sub-limit / Notes
☐	**Professional Trust Services** Extends cover to claims for breach of trust or breach of fiduciary duty arising from professional trust services.	
☐	**Stop Payment Order Liability** Extends cover to liability arising from failure to comply with stop payment instructions on cheques, drafts or debit mandates.	
☐	**Loss of Documents** Extends cover to liability arising from the destruction, loss or mislaying of documents in your custody, and costs of replacement.	
☐	**Inter-Company Liability** Extends cover to claims from subsidiary and associated group companies where services are outsourced within the group on arm's-length terms.	
☐	**Compensation for Court Attendance** Pays daily compensation to directors / employees required to attend court as witnesses in connection with a covered claim.	

17. Policy Extensions — Applicable to All Sections

These extensions apply to both Section 1 (Crime) and Section 2 (Civil Liability) if selected. Tick all extensions required.

	Extension	Sub-limit / Notes
☐	**Claims Preparation Costs** Covers reasonable costs incurred in producing and certifying particulars to substantiate the amount of any loss (subject to sub-limit).	
☐	**Audit Expenses** Covers the cost of audits or examinations required by supervisory authorities as a result of a covered loss (subject to sub-limit).	
☐	**Mitigation Costs** Covers reasonable costs incurred after discovery of a covered circumstance to prevent, limit or mitigate the effects of a loss.	
☐	**No Claims Bonus** A discount on renewal premium where no claims, losses or incidents have been reported in the prior period.	
☐	**Extended Reporting Period** Entitles the Insured to an additional 12-month extended discovery / reporting period after policy expiry (subject to an additional premium of 100% of the annual premium).	
☐	**Reinstatement of Sum Insured** Aggregate Sum Insured reinstated once following a paid loss, for wholly unrelated subsequent losses.	
☐	**New Subsidiaries** Automatic cover for newly created or acquired subsidiaries below a defined assets threshold, subject to reporting requirements.	

18. Privacy Notice (POPIA)

In order to provide you with insurance, The Liability Company (Pty) Ltd and Old Mutual Insure Ltd are required to collect and process your personal information as provided in this proposal form. We will share your personal information with other insurers, reinsurers, industry bodies, regulatory authorities, credit agencies and service providers as necessary to underwrite, administer and service this insurance, investigate and assess claims, prevent fraud and comply with our legal obligations.

18. Privacy Notice (POPIA) (continued)

We will treat your personal information with care and have implemented reasonable technical and organisational measures to protect it. Your personal information will be processed in accordance with the Protection of Personal Information Act 4 of 2013 (POPIA). By signing this proposal form you consent to the collection, processing and sharing of your personal information for the purposes described above.

19. Declaration

I/We, the undersigned, declare that:

1. The statements, answers and information provided in this proposal form and all attached documents are true, complete and correct to the best of my/our knowledge and belief.
2. I/We have not withheld or suppressed any material facts or information that might be relevant to the insurer's assessment of this risk.
3. I/We agree that this proposal form, together with any other information provided by me/us, shall form the basis of any contract of insurance concluded between the Proposer and the insurer.
4. I/We undertake to notify the insurer immediately of any material changes to the information provided in this form that occur between the date of this proposal and the inception of cover.
5. I/We confirm that I/we am/are duly authorised by the Proposer to complete and sign this proposal form.

Signed at _____ Dated _____

Full name _____

Position / Designation _____

Signature _____

20. Cooling Off Rights

In terms of the Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS) and the General Code of Conduct for Authorised Financial Services Providers and Representatives, you have the right to cancel this policy within 30 days of receipt of the policy wording, subject to the deduction of a pro-rata premium for any period of cover and any administration fees that may apply.

To exercise this right, please notify The Liability Company in writing at: info@theliabilitycompany.co.za or at the contact details set out in the policy schedule.

21. Additional Notes (if required)