**PROPOSAL FORM**

**Cyber Insurance Policy**

1. The questions comprised in this Proposal form are designed to provide a comprehensive view of the maturity and set-up of the IT and data security within your company
2. The answers to the Proposal form are key to the risk assessment and underwriting process in order to provide Cyber Insurance to you, based on the information we obtained from your side.

We can only conduct a risk assessment and provide Cyber Insurance if the answers to the Proposal form are accurate, comprehensive and understandable. Consequently, inaccurate or misleading answers within the Proposal form could lead to avoidance of coverage under the Cyber Insurance contract or delays in the quoting process. Therefore a responsible IT security person should answer and sign the Proposal form, or at least support the person who is answering, by counter-signing the Proposal form

1. The Proposal form is not exhaustive, which means that, after evaluating your answers, we might have additional questions. In this case, we would request further information to complete our risk assessment and underwriting process with regard to the Cyber Insurance contract
2. The duty of disclosure continues after the despatch of the completed proposal form, to the time and date when the insurance contract is entered into and throughout the contract of insurance. Accordingly, any further or additional information or documentation which may affect anything already disclosed should be notified to insurers as soon as possible
3. If there is insufficient space in this proposal form to provide answers or information, please use additional sheets
4. Completing and signing this risk proposal form does not bind SHA to enter into a contract of insurance
5. Please attach the following information to the Proposal form, as is applicable:
	1. IT Governance Policy (which sets out the principles and standards for the governance of information technology within the company)
	2. Latest Payment Card Industry Data Security Standard certificate
	3. Service Level Agreements with third party service providers
	4. Expiry policy and wording in order for us to revert with a comparable quotation. Premium information may be redacted
6. By completing and signing this proposal form, the proposer accepts and acknowledges that it has read and fully understood its contents and their possible effect in relation to the contract of insurance that may be entered into consequently

|  |
| --- |
| MAIN CONTACT PERSON REGARDING THIS RISK ASSESSMENT |
| 1. Name and surname
 |  |
| 1. Position
 |  |
| 1. Phone number
 |  |
| 1. Email address
 |  |
| COMPANY OVERVIEW |
| 1. Company name
 |  |
| 1. Company registration number
 |  |
| 1. VAT number
 |  |
| 1. Principal address
 |  |
| 1. Postal address
 |  |
| 1. Phone number
 |  |
| 1. Website
 |  |
| 1. Date of incorporation
 |  |
| Any subsequent re-registration / name changes |  |
| 1. Type of organisation
 |
| [ ] Sole Proprietor [ ] State Owned Company [SOC] [ ] Private Company [Pty Ltd] [ ] Public Company [Ltd][ ] Non-Profit Company [NPC] [ ] Personal Liability Company [Inc] |
| 1. Are any of the company’s subsidiaries to be included (shared limit)?

If YES, please provide the following details | Yes[ ]  No[ ]  |
|

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | % Owned | Date created / acquired | Country of incoropration | Activities, if different from parent |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

 |
| 1. Please provide additional information on the level of integration and shared infrastructure with subsidiaries
 |
|

|  |
| --- |
|  |

 |
| *For the rest of the proposal form, questions must be answered in such a way as to disclose information pertaining to subsidiaries also**Insurers will not be held liable for the proposer’s failure to comply with local insurance regulations in territories outside of South Africa in which they operate. Accordingly, claims payment will be done in local territories only if non-admitted coverage is permissible.* |
| BUSINESS ACTIVITIES |
| 1. Tick box that best describes activities
 |
|

|  |
| --- |
| Business and professional services (excluding IT) |[ ]
| Defence and military  |[ ]
| Education |[ ]
| Entertainment & Media |[ ]
| Financial Institutions | Bank |[ ]
|  | Insurance company |[ ]
|  | Investment management |[ ]
|  | Credit card processing |[ ]
|  | Other |[ ]
| Food & Agriculture |[ ]
| Healthcare | Private Hospital / clinic |[ ]
|  | Public hospital / clinic |[ ]
|  | Doctor, dentist, etc. |[ ]
| Information Technology | Hardware |[ ]
|  | Software |[ ]
|  | Services Provider (ASP; ISP; Cloud; IT; managed services) |[ ]
| Manufacturing |[ ]
| NGOs, Non-Profit |[ ]
| Pharmaceuticals |[ ]
| State owned companies |[ ]
| Real Estate, Property & Construction |[ ]
| Retail | Primarily online  |[ ]
|  | Primarily traditional |[ ]
| Telecommunications |[ ]
| Tourism & Hospitality |[ ]
| Transportation/ Aviation/ Aerospace |[ ]
| Telecommunications |[ ]
| Other (Specify) |[ ]

 |
| Describe in detail |
|

|  |
| --- |
|  |

 |
| 1. Please list , on a separate page, all websites (domain-names deployed to be addressable from the internet) that should be covered by this insurance
 |
|

|  |
| --- |
|  |

 |
| 1. Do you intend on offering any new services in the next 12 months?

If YES, please provide details | Yes[ ]  No[ ]  |
|

|  |
| --- |
|  |

 |
| 1. Annual revenue (ZAR)
 |
|

|  |  |  |
| --- | --- | --- |
|  | Current Year | Prior Year |
|  | **Traditional** | **e-Commerce** | **Traditional** | **e-Commerce** |
| South Africa |  |  |  |  |
| Rest of Africa |  |  |  |  |
| Europe |  |  |  |  |
| North America |  |  |  |  |
| Other: |  |  |  |  |  |

 |
| 1. Total Assets
 |

|  |  |
| --- | --- |
| South Africa |  |
| Rest of Africa |  |
| Europe |  |
| North America |  |
| Other: |  |  |

 |
| 1. IT Budget
 | Current Year | Prior Year |
| Annual aggregate IT-budget |  |  |
| Percentage of IT security budget therefrom |  |  |
| HUMAN RESOURCES SECURITY  |
| 1. Number of employees in the following categories:
 |

|  |  |
| --- | --- |
| South Africa |  |
| Rest of Africa |  |
| Europe |  |
| North America |  |
| Other: |  |  |

 |
| 1. Do you conduct criminal history, employment history and credit checks on all employees as part of the recruitment process?
 | Yes[ ]  No[ ]  |
| 1. Do you provide at least annual security/data/privacy training or awareness programs to increase your user’s (employees and contractors) security awareness and to prepare users to be more resilient and vigilant against phishing campaigns and other targeted data threats?
 | Yes[ ]  No[ ]  |
| INSURANCE HISTORY AND REQUIREMENTS |
| 1. Details of current Cyber insurance

|  |  |
| --- | --- |
| Limit of Indemnity |  |
| Retention and Waiting Period |  |
| Retroactive cover |  |
| Expiry date  |  |

Please attach expiry policy and wording in order for us to revert with a comparable quotation. Premium information may be redacted |
| 1. Coverage Requirements (Always subject to policy terms, conditions, and exclusions)
 |
|

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Option 1 | Option 1 | Option 3 | Option 4  |
| Aggregate Limit of Indemnity |  |  |  |  |
| Each and Every Claim Excess |  |  |  |  |
| Waiting period(Business Interruption) | [ ]  12 hours | [ ]  24 hours | [ ]  36 hours  |

 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Cover Sections (subject to the terms, conditions and exclusions of the SHA Cyber Insurance Policy wording)

|  |
| --- |
| **Data Breach Response (1st party)***(we will pay on the insured’s behalf any reasonable and necessary costs resulting from an actual or suspected data breach)* |[ ]
| **Restoration (1st party)***(we will pay on the insured’s behalf any reasonable and necessary costs to restore their data and software after a data breach, to the closest possible condition in which they were immediately before the data breach)* |[ ]
| **Business Interruption (1st party)***(we will pay the insured for the reduction of net profit during the interrupted period which has been directly caused by a cyber-incident)* |[ ]
| **Cyber Extortion (1st party)***(we will reimburse the insured for any ransom they pay [where legally permissible and subject to our prior written consent] and any reasonable and necessary costs to resolve cyber extortion)* |[ ]
| **Cyber Crime (1st party) [optional]***(we will reimburse the insured for any money illegally taken from them as a direct result of cyber-crime)* |[ ]
| **PCI-DSS (1st party) [optional]***(we will reimburse the insured for any monetary fines and penalties levied against them by a Payment Card Brand due to their breach of PCI-DSS which is directly caused by a cyber-incident)* |[ ]
| **Confidentiality and privacy (3rd party)***(we will reimburse any sums the insured is under a legal liability to pay arising from a third party claim or a claim against them by an employee for a data breach relating to confidential information or personal data of a third party, or for infringement of your respective data protection laws and the insured’s legal defence costs incurred with our consent)* |[ ]
| **Network Security (3rd Party)***(we will reimburse any sums the insured is under a legal liability to pay if a third party claim is made for a data breach, theft of data or a DoS attack on a third party’s computer systems which is directly caused by a malicious act or malware on the insured’s computer systems that the insured failed to prevent as well as the insured’s legal defence costs incurred with our consent)* |[ ]
| **Media (3rd Party) [optional]***(we will reimburse any sums the insured is under a legal liability to pay arising from a third party claim for: defamation, breach of copyright, title, slogan, trademark, trade name, service mark, service name or domain name or breach or interference of privacy rights, resulting from the insured’s online media activities and your legal defence costs incurred with our consent)* |[ ]

 |
| 1. **Loss History**
 |
| * 1. Do you currently hold or have you ever held Cyber Insurance providing same or similar coverage as coverage being sought?
 | Yes[ ]  No[ ]  |
| * 1. Has any insurer ever cancelled or non-renewed a policy that provided the same or similar coverage as coverage being sought?
 | Yes[ ]  No[ ]  |
| * 1. Have you at any time in the past three (3) years had any incidence, unplanned business interruption, claims or suits involving unauthorised access, intrusion, breach, compromise, or misuse of our network, including embezzlement, fraud, theft of proprietary information, breach of personal information, theft or loss of laptops, denial of services, electronic vandalism or sabotage, computer virus or other incident?
 | Yes[ ]  No[ ]  |
| * 1. Have you at any time in the past three (3) years ever received claims or complaints with respect to allegations of defamation, invasion or injury of privacy, theft of information, breach of information security, transmission of malware, participation in denial of service attack, request to notify individuals due to an actual or suspected disclosure of personal information
 | Yes[ ]  No[ ]  |
| * 1. Are you aware of any release, loss or disclosure of personally identifiable information in your care, custody or control, or in the control of anyone holding such information on your behalf in the most recent three (3) years
 | Yes[ ]  No[ ]  |
| * 1. Are you aware of any actual or alleged fact, circumstance, situation, error or omission, or potential issue that might give rise to a loss or claim against you under the cyber insurance policy for which you are applying for, or any similar insurance presently or previously in effect or currently proposed
 | Yes[ ]  No[ ]  |
| If **YES**, please attach full details including description of each incident, claim or suit and the cause, internal costs, costs to third parties, whether affected individuals were notified, time to discover, recovery time and steps taken to mitigate future exposure |

|  |
| --- |
| DATA AND CRYPTOGRAPHY |
| 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:.
 |
|

|  |  |  |
| --- | --- | --- |
| Data Type | Approximate Number of unique data records | Data of US or European citizens (anywhere) OR data in US or Europe located data centres |
|[ ]  Personally Identifiable Information (PII): |  |  |
|[ ]  Personal Health Information (PHI) |  |  |
|[ ]  Payment card Information (PCI) |  |  |
|[ ]  Usernames and passwords |  |  |
|[ ]  Third party corporate confidential data |  |  |
|[ ]  Other (Specify) |  |  |  |

 |
| 1. Have you implemented data retention and secure destruction policies for physical and electronic data and assets?
 | Yes[ ]  No[ ]  |
| 1. Have you implemented encryption for the following:
 |
| * 1. Sensitive data/backups stored outside your environment
 | Yes[ ]  No[ ]  |
| * 1. Sensitive data stored in your environment (data at rest)
 | Yes[ ]  No[ ]  |
| * 1. Data stored on portable devices (laptops, external storage devices, tablets, phones, etc.)
 | Yes☐ No☐ |
| * 1. Sensitive data transmitted outside your environment
 | Yes[ ]  No[ ]  |
| If YES please attach details |  |
| 1. Have you disabled employee write access to USB devices?
 | Yes[ ]  No[ ]  |
| 1. Does your web server encrypt confidential data (HTTPS)?
 | Yes[ ]  No[ ]  |
| 1. Do you consider confidentiality when using operational data for testing to ensure that all sensitive details are protected by removal or modification?
 | Yes[ ]  No[ ]  |
| COMPLIANCE |
| 1. Have you assigned a responsible person for information security (e.g. Chief Information Security Officer "CISO")?
 | Yes[ ]  No[ ]  |
| 1. Have you assigned a responsible person for providing guidance and ensuring awareness of privacy principles (e.g. Data Privacy Officer DPO)?
 | Yes[ ]  No[ ]  |
| 1. Have you implemented a procedure to permanently comply with all privacy relevant legislative statutory, regulatory and contractual requirements (e.g. GDPR, POPIA)??
 | Yes[ ]  No[ ]  |
| 1. Please check all legal frameworks you have to adhere to.
 |
|

|  |
| --- |
|[ ]  Protection of Personal Information Act 4 of 2013 [POPIA] |
|[ ]  General Data Protection Regulation GDPR (2016/679) [GDPR] |
|[ ]  US Federal Privacy Act of 1974 [Privacy Act] |
|[ ]  US Health Insurance Portability and Accountability Act [HIPA] |
|[ ]  US Health Information Technology for Economic and Clinical Health [HITECH] |
|[ ]  Other – please specify  |  |

 |
| 1. Please check all standards for which you have successfully been audited or hold a valid certificate

|  |
| --- |
|[ ]  International Organization for Standardization [ISO 27001:2013] |
|[ ]  National Institute of Standards and Technology [NIST] |
|[ ]  Other – please specify and describe scope of certification |  |

Please attach copies |
| ACCESS CONTROL  |
| 1. Do you restrict employees' and external users' privileges on a business-need to know basis (particularly administrative permissions and access to sensitive data e.g. personal data)?
 | Yes[ ]  No[ ]  |
| 1. Do you review / audit on at least an annual basis?
 | Yes[ ]  No[ ]  |
| 1. Do you have a formal access provisioning process in place for assigning and revoking access rights?
 | Yes[ ]  No[ ]  |
| 1. Do you prohibit “local admin” rights on employee workstations / laptops?
 | Yes[ ]  No[ ]  |
| 1. Do you revoke, at least on a monthly basis, all systems access, accounts and associated rights after termination of users (incl. employees, temporary employees, contractors and vendors)?
 | Yes[ ]  No[ ]  |
| 1. Do you monitor excessive permissions (e.g. segregation of duties rules)?
 | Yes[ ]  No[ ]  |
| 1. Have you implemented a password policy that requires passwords of adequate complexity and rotation (i.e. complexity, length and avoiding re-use)?
 |
| [ ] Mandatory complexity and rotation [ ] Mandatory complexity[ ] Mandatory rotation [ ] No policy |
| 1. Are password parameters consistently applied across the organization?
 | Yes[ ]  No[ ]  |
| 1. Do you change the initial password on all internet-enabled devices? For example most internet routers have the initial password as “12345678”
 | Yes[ ]  No[ ]  |
| SECURITY SOFTWARE AND NETWORK PROTECTION |
| 1. Do you use malware protection for all web-proxies, email-gateways, workstations and laptops?

If YES, please attach details | Yes[ ]  No[ ]  |
| 1. Do you timely – at least within one month of release – apply updates to critical IT-systems and applications (“Security Patching”)?
 | Yes[ ]  No[ ]  |
| 1. Are all internet access points to you network secured by appropriately configured firewall(s)?
 | Yes[ ]  No[ ]  |
| 1. Is there an appropriately and regularly maintained firewall between wireless access points and the parts of your network on which sensitive data is stored?
 | Yes[ ]  No[ ]  |
| 1. Do you monitor your network and identify security events?

Please attach details describing how you access vulnerabilities in your network | Yes[ ]  No[ ]  |
| 1. Are all internet accessible systems (e.g. web-, email servers) segregated from your trusted network (e.g. within demilitarized zone “DMZ” or at third party provider)?
 | Yes[ ]  No[ ]  |
| 1. Are your information processing facilities (i.e. any system, service or infrastructure or physical location housing same) implemented with redundancy?
 | Yes[ ]  No[ ]  |
| GENERAL SOFTWARE AND INFRASTRUCTURE |
| 1. How many computers/laptops form part of your network?
 |
| [ ]  Less than 5 [ ] 5 – 25 [ ] 25 – 100 [ ] 100 – 500 [ ]  Greater than 500 |
| 1. What operating systems are installed in the computers?
 |
| [ ]  Linux [ ]  Windows 10 [ ]  Window 7[ ]  Older than Windows 7 [ ]  Other (specify) [ ]  MSC OS (specify version) |
|

|  |
| --- |
| Specify: |

 |
| 1. How often are operating system updates and patches installed?
 |
| [ ] Automatic [ ] Manual Weekly [ ] Manual once a month [ ] Manual greater than one month intervals [ ] Not updated |
| 1. Do you allow for BYOD (“bring your own device”)?
 | Yes[ ]  No[ ]  |
| If “YES”, have you implemented Mobile Device Management Control (MDM)? | Yes[ ]  No[ ]  |
| 1. Have you implemented remote device wipe for mobile devices receiving company emails?
 | Yes[ ]  No[ ]  |
| 1. Do you provide remote access to you IT systems / network?
 | Yes[ ]  No[ ]  |
| 1. How do you secure the remote access?
 |
| [ ] ID / Password only [ ] VPN or equivalent [ ] VPN or equivalent with 2 factor authentication [ ] Other (please specify) |
|

|  |
| --- |
| Specify: |

 |
| 1. Do you have bespoke software on your systems? I.e. software that has been created or commissioned for your business?
 |
| [ ] Yes, developed / customized internally [ ] Yes, developed / customized by 3rd party [ ] No  |
| THIRD PARTY SERVICE PROVIDERS |
| 1. What part of your network, computer system or information security functions have been outsourced?
 |
|

|  |  |
| --- | --- |
| Function | Providers name |
| ☐ | None |  |
|[ ]  Application service provider |  |
|[ ]  Data Centre, managed security |  |
|[ ]  Data processing |  |
|[ ]  IT and Network service provider |  |
|[ ]  Management of entire IT system |  |
|[ ]  Offsite backup and storage |  |
|[ ]  Other cloud computing services |  |
|[ ]  Other (please specify  |  |
|  |  |  |

 |
| 1. Do you perform risk assessments prior to conducting business with third party providers?
 | Yes[ ]  No[ ]  |
| 1. Have you validated that the security level of each third party provider is commensurate with your own (i.e. via audit, independent audit)?
 | Yes[ ]  No[ ]  |
| 1. Do you have written and signed contract(s) with the respective service providers including a requirement that third parties protect data that is either accessed of processed by them (i.e. a non-disclosure / confidentiality / hold harmless agreement or waiver of liability due to any failure to safeguard data)?
 | Yes[ ]  No[ ]  |

|  |
| --- |
| INFORMATION SECURITY INCIDENT MANAGEMENT |
| 1. How do you perform back-ups?
 |
| [ ] Automatic [ ] Manual [ ] No backups done |
| 1. How often do you perform backups?
 |
| [ ] Daily [ ] Weekly [ ] Monthly [ ] No backups done |
| 1. Where do you store your backups?
 |
| [ ] Cloud [ ] External hard drive [ ] Network hard drive [ ] Hard drive on PC |
| 1. Are backups regularly tested to validate the accuracy and integrity of the data to verify the ability to restore data as quickly as possible
 | Yes[ ]  No[ ]  |
| 1. In the event of a computer / system failure, how long would it take you to restore data from the data backups?
 |
| [ ] Less than 6 hours [ ] Between 6 and 12 hours [ ] More than 12 hours [ ] Unknown |
| 1. Do you have an incident response plan for data breaches, network intrusions or IT virus infections?
 | Yes[ ]  No[ ]  |
| 1. Have you conducted a Business Impact Analysis “BIA”?
 | Yes[ ]  No[ ]  |
| 1. Do you have a disaster recovery / business continuity plan in place (“BCM”) that specifically addresses cyber incidents?
 | Yes[ ]  No[ ]  |
| 1. Is this plan reviewed, updated and tested annually?
 | Yes[ ]  No[ ]  |
| 1. Are identified issues eliminated?
 | Yes[ ]  No[ ]  |
| 1. Can you indicate the acceptable time until a financial loss for you materializes with significant impact on your business?
 |
| [ ] Less than 12 hours [ ]  12 to 18 hours [ ] 18 to 24 hours [ ] Greater than 24 hours |
| 1. Can you indicate the acceptable time until a financial loss for your client(s) / customer(s) materialises
 |
| [ ] Less than 12 hours 12 to 18 hours [ ] 18 to 24 hours [ ] Greater than 24 hours |
| PCI-DSS (ONLY COMPLETE IF COVER IS REQUIRED) |
| 1. How do you accept credit card payments?
 |
| [ ] Online payment [ ] Point of Sale payment [ ] None |
| 1. Which merchant level according to PCI definitions to you represent currently? Please attach certification.
 |
| [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] None |
| 1. Do you ensure that card validation codes are not stored in any of your databases, log files or anywhere else within your network?
 | Yes[ ]  No[ ]  |
| 1. Do you mask all but the last four digits of a card number when displaying or printing cardholder data?
 | Yes[ ]  No[ ]  |
| 1. Are you fully compliant with EMV card processing standards?
 | Yes[ ]  No[ ]  |
| 1. Do you scan your point of sale devices daily for malware or skimming devices?
 | Yes[ ]  No[ ]  |
| 1. Is your payment card data encrypted at all times?
 | Yes[ ]  No[ ]  |
| 1. Does a third party process payment card data on your behalf?
 | Yes[ ]  No[ ]  |
| If YES, has the payment processor provided you with evidence that they are PCI certified?Please attach details | Yes[ ]  No[ ]  |
| CYBER CRIME (ONLY COMPLETE IF COVER IS REQUIRED) |
| 1. What value of your own funds do you manage on an annual basis?
 | Yes[ ]  No[ ]  |
| 1. What is the average daily value of own fund transferred electronically?
 | Yes[ ]  No[ ]  |
| 1. What is the maximum daily value of own funds transferred electronically?
 | Yes[ ]  No[ ]  |
| 1. What is the maximum value of any single electronic own funds transfer?
 | Yes[ ]  No[ ]  |
| 1. Are special logon passwords (separate from an individual’s operator’s password) used when logging into a terminal to provide verification of the terminal’s identity
 | Yes[ ]  No[ ]  |
| 1. How are payments loaded?
 |
| [ ] Online banking application [ ] Own application developed in-house[ ] Own application developed by 3rd party (please attached details) |
| 1. How do you gain access to payment applications?
 |
| [ ] Multi factor / two factor authentication [ ] Password[ ] Other (please attach details describing) |
| 1. Do you maintain documents procedure for the electronic transfer of funds?
 | Yes[ ]  No[ ]  |
| If YES, does the procedure clearly define:

|  |  |
| --- | --- |
| All authorized personnel? | Yes[ ]  No[ ]  |
| How many personnel are authorized to load, release and authorize payments? | Yes[ ]  No[ ]  |
| All authorized personnel for correspondence with corporate customers  | Yes[ ]  No[ ]  |
| Call back procedures? | Yes[ ]  No[ ]  |
| Transfer limits? | Yes[ ]  No[ ]  |
| Dual authorization to load or maintain beneficiary details? | Yes[ ]  No[ ]  |
| Dual authorization to release payment above a specified limit? | Yes[ ]  No[ ]  |
| Segregation of duties for loading, releasing and authorization of payments? | Yes[ ]  No[ ]  |
| Validation process for all supporting documents before payment are authorised? |  |

 |

|  |
| --- |
| MULTIMEDIA (ONLY COMPLETE IF COVER IS REQUIRED) |
| 1. What kind of electronic / online activities do you perform?
 |
|

|  |
| --- |
| Electronic own content publishing |[ ]
| Content under license from a 3rd party |[ ]
| Files for down load |[ ]
| Giving advice (medical, legal, etc.) |[ ]
| Straining under written license / consent agreement (e.g. video, music) |[ ]
| Presentation of product / services of theirs (e.g. advertising, buying, selling) |[ ]
| Collection of sensitive information (e.g. PPI, PCI, PHI, other) |[ ]
| Unlicensed 3rd part content (e.g. chat rooms, customer reviews, blogs, message boards) |[ ]
| Adult content, gaming, gambling |[ ]
| Other (Specify) |  |[ ]

 |
| 1. Which web-based services to you use for distribution of such content?
 |
|

|  |
| --- |
| Website (own and/or 3rd party hosted |[ ]
| Social Media (Twitter, Facebook, Snapchat, Instagram, etc.) |[ ]
| Email services (newsletter) |[ ]
| Online advertising |[ ]

 |
| 1. Do you outsource the production of any electronic content

If YES please attach details | Yes[ ]  No[ ]  |
| 1. Do you have processes for screening and – if required – removing libelous or slandering content, unlicensed content or content infringing on third parties’ intellectual property right?
 | Yes[ ]  No[ ]  |
| 1. Do you have a process for reviewing all content before it is posted by or on behalf of the company?
 | Yes[ ]  No[ ]  |
| * 1. If YES, is this review performed by a qualified attorney?
 | Yes[ ]  No[ ]  |
| * 1. If NO, what procedures are in place to avoid posting improper or infringed content? Please attach details.
 |
|

|  |
| --- |
|  |

 |
| 1. Have you, in the last three (3) years, received a complaint or cease and desist demand alleging trademark or copyright infringement, invasion of privacy, or defamation with regard to any content published, displayed or distributed by you or on your behalf?

If YES, please attach details | Yes[ ]  No[ ]  |
| 1. Do you share – either commercially or free – any information about users, subscribers or visitors of your website internally of with third parties?
 | Yes[ ]  No[ ]  |
| 1. Does your website provide a privacy policy (e.g. about collection of data, use of cookies, etc.) and a legal notice about the use of third parties’ rights and links to external websites including a disclaimer and is such content approve by a qualified attorney?
 | Yes[ ]  No[ ]  |
| LOSS MITIGATION SERVICE |
| In the event of a claim falling under the insurance policy you are applying for, do you agree to allow an (external) insurer approved claims handling expert and/or IT specialist to be provided with access to your IT system and network to provide loss mitigation service? | Yes[ ]  No[ ]  |
| DECLARATIONS |
| 1. I/We declare that the above statements are true and complete
2. At the present time, other than as stated above, l/We have no reason to anticipate any claim being brought against me/us that would constitute a claim under the Insurance now being renewed or applied for
3. I/We declare that, in the event of this being a renewal of a policy currently insured via Stalker Hutchison Admiral for and on behalf of Santam Limited, there have been no material alterations to the risk as submitted to underwriters originally, and, if a new application, that all material facts have been disclosed
4. 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
5. Due to SHA’s FSCA Licensing status and, in light of the requirements set out in the Protection of Personal Information Act 2013 (POPIA) we are not, strictly speaking, allowed to contact you directly and would generally communicate with you via your broker. However, there may be instances where we may need to contact you directly in order to advise you of important matters relating to your Policy. Therefore, please indicate below how you would prefer to be contacted in the unlikely event that we should need to contact you directly

[ ] SMS [ ] E-Mail [ ] Phone [ ] Mobile [ ] Post |
|  | Dedicated individual responsible for Insurance / Risk Management | Dedicated individual responsible for Information Security and Privacy |
| Name |  |  |
| Signature |  |  |
| Date |  |  |

**PROTECTION OF PERSONAL INFORMATION ACT**

We understand that the information provided in this application for insurance and all documentation provided with it may be deemed to be personal information in terms of the Protection of Personal Information Act 2013 (the POPI Act) and we will accordingly take all reasonable steps to ensure that your information is processed / used / stored in accordance with the POPI Act and for the following purposes:

* To verify the information disclosed herein against any other source;
* To communicate with you directly should you request us to and in accordance with relevant regulatory requirements;
* To compile non-personal statistical information to assist in assessing similar risks;
* To assess the risk to be underwritten and, if a Policy of Insurance is issued pursuant to and based upon such information, to use the disclosed information at claims stage to assess any claims that may be made against any such Insurances;
* To transmit your personal information to any affiliate, subsidiary, service provider/consultant/advisor or re-insurer so that we can provide insurance services to you and to enable us to further our legitimate interests including statistical analysis, reinsurance and credit control;
* To combat insurance fraud and properly evaluate risks, we will store your personal information on a shared database created by the South African Insurance Association (SAIA) in order to verify it against available sources and databases on the system.

Personal Information of Minors (Complete if Applicable)

If any information provided herein relates to a Minor (i.e. a child under the age of 18) we require that a competent person (parent/legal guardian) provide consent to the processing of such information for the above purposes and for any purpose that is compatible therewith.

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*full name of competent person*), hereby provide my consent to the processing of any information provided herein relating to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*name of minor whose personal information is disclosed herein*) for the purpose as disclosed above. I further understand that I have the right to withdraw this consent at any time but that this may mean that any insurance issued pursuant to this application may be terminated and/or that any claims issued against such insurance may not be able to be finalised

Further disclosures

Please note that there may be instances where we will be required to transfer your personal information outside South African borders, generally for purposes of furthering the Insurer’s legitimate interests regarding reinsurance or for the processing of any claim that arises outside South African borders. However, before transferring your personal information, we will ensure that the entity to whom the information is being transferred is subject to similar data protection conditions as those imposed by the POPI Act failing which we will advise you accordingly and request your consent to transfer information as required.

Note that the provision of the information required/requested herein is mandatory as it is necessary for us to accurately underwrite the insurances, which you are hereby applying for, and if any information is withheld or is misrepresented the Insurer may be entitled to void any insurances issued pursuant to this application.

Although any insurance issued pursuant to this application will be reviewed annually (where appropriate) it is your responsibility to ensure that the information provided to the Insurer remains accurate and up to date, we therefore encourage you to contact us at any time to advise us of changes to the information provided.

In addition, you may contact us at any time to exercise the following rights that you have in terms of the POPI Act (subject to any regulatory obligations placed on us/Santam Ltd):

* To request that we provide you with access to your personal information held/processed by us;
* To request that we erase or correct the your personal information that we hold (where appropriate/possible);
* To request that we transfer any personal information held by us to you or to any other person/system selected by you in a structured, commonly used and machine-readable format;
* To request that we restrict the processing of your personal information for reasons provided for in the POPI Act.

Should you wish to lodge a complaint regarding our compliance with the POPI Act or in respect of the processing of your personal information, please contact the Santam Client Care department (contact details below):

Email:complaints@santam.co.za

Telephone:0860 102 725

Fax:(021) 915 7434

Alternately, you also have the right to approach the South African Information Regulator (contact details below) should the above process not adequately address your concerns.

Email: complaints.IR@justice.gov.za

Postal address:

 PO Box 31533

 Braamfontein

Johannesburg

 2017

Physical address:

 JD House

27 Stiemens Street

 Braamfontein

 Johannesburg

 2001