

Important Notice: This form must be completed accurately, in full and in English. All material information likely to influence the acceptance and assessment of the risk must be disclosed. If you are not certain if the information is material or not, provide it otherwise it may affect your policy at a later date. PLEASE NOTE THAT THIS FORM IS NOT AN ACCEPTANCE OR CONFIRMATION OF COVER. 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.

FULL APPLICANT DETAILS

1. Name of Insured	
2. Physical address	
3. Primary contact number	
4. Primary contact email address	
5. Registration number	
6. Indicate the primary nature of the Business	
7. Products and services offered	
8. Subsidiary names (if applicable)	
9. Company website address	
Type of Business (Tick all applicable)	
Manufacturing	
Finance, Banking and Insurance	
Professional, Business and Consumer Services	
Energy	
Retail and Wholesale	
Education	
Healthcare	
Government	
Transportation	
Media and Telekom	

GENERAL UNDERWRITING INFORMATION

Revenue			
Annual Turnover / Gross Revenue			
Gross e-business Revenue (as a percentage of Gross Revenue)			
Select which is applicable to your business			
Business Size	Turnover (annual revenues)	Number of Employees	Tick Applicable
S - Small	Up to USD 1,000,000	Up to 10	
M - Medium	Up to USD 10,000,000	Up to 50	

L – Large	Up to USD 50,000,000	Up to 500	
E – Extra	USD 50,000,001 and above	501 and above	
Geographical split of gross revenue by region			
Europe	Last year	%	Current year %
North America (including Mexico)	Last year	%	Current year %
Central and South America	Last year	%	Current year %
Africa (including Maghreb Countries)	Last year	%	Current year %
Middle East	Last year	%	Current year %
Asia and Oceania	Last year	%	Current year %
Russia and CIS	Last year	%	Current year %
1. Number of employees			
Permanent		Contractors	
		Temporary	
2. Have you been involved in any merges / acquisitions within the past 3 years		Yes	No
3. Do you have any planned merges / acquisitions planned within the next 12 months			

CLAIMS AND INSURANCE HISTORY

1. Have you ever had a cyber insurance policy cancelled or been declined insurance cover in the last 5 years	Yes	No
If YES please provide details		
2. Have you suffered from any of the following within the past 5 years		
a. Systems intrusion, tampering, malicious code attack, loss of data, extortion attempt, data theft or similar	Yes	No
b. Unauthorised transmission or disclosure of sensitive information for which you are responsible	Yes	No
c. Allegations of invasion of privacy, that sensitive information has been compromised or content infringements	Yes	No
d. Unscheduled network outage or interruption	Yes	No
3. Has your organisation changed cyber insurers in the past 5 years	Yes	No
If YES please indicate why		
4. Has your organisation had any cyber related incidents in the past 5 years (whether they resulted in a financial loss or claim or not)	Yes	No
If YES please provide details		
5. If YES to any of the above, were any of these claims declined/rejected by your insurer	Yes	No
If YES please provide details and reasons for declinature		

6. Are you or any of the partners, director 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 cyber claim against the organisation or against a cyber insurance policy	Yes		No	
---	-----	--	----	--

CHAPTER 1 – CYBER RISK ASSESSMENT

CYBER SECURITY POLICIES AND STANDARDS

1. Do you have a dedicated individual responsible for Information Security	Yes		No	
2. Have you implemented information security policies/procedures and communicated these to employees	Yes		No	
3. Are your security policies reviewed on at least an annual basis	Yes		No	
4. Do you comply with privacy and data protection legislation applicable to all jurisdictions and industry standards in which you operate	Yes		No	
5. Do security policies and standards apply across all subsidiaries, joint ventures, and the like	Yes		No	
6. Do you have a data classification policy including security requirements for sensitive data	Yes		No	
7. Please specify any security certificates you hold (for example PCI DSS)				
8. Do you enforce a "strong password policy" across all accounts, including minimum password length restriction, use of special characters and account lockout as a result of failed authentication attempts	Yes		No	
9. Is your company or any of its subsidiaries subject to specific notification requirements in territory	Yes		No	
If YES please provide details				

CYBER SECURITY REVIEWS AND ASSESSMENTS

1. Do you conduct security reviews or assessments of IT Environments	Yes		No	
2. Are assessments internal / external or both				
3. How frequently are your IT environments subjected to third party security assessments, including vulnerability scanning and penetration testing. Please indicate annually / bi-annually / quarterly / never				
4. Were any serious concerns raised at your last test and have these been addressed	Yes		No	
5. Did the scope of the testing performed include both your internal and external IT environment	Yes		No	
Please attach the latest test reports				

CHAPTER 2- CYBER INCIDENT RESPONSE

CYBER SECURITY IMPLEMENTATION

1. Please indicate which of the following you have implemented (please tick all that apply)	
• Antivirus/malware which is updated in accordance with vendor recommendations	
• Firewalls at all breakout points to external networks	
• Firewalls to segment and protect sensitive data and resources within the network	

• Web application firewalls			
• Intrusion detection or prevention systems			
• Security information and event management solutions			
• Cyber threat intelligence function			
• Data loss prevention tools			
• Access control and remote wipe for mobile devices			
• Access control and remote wipe for BYOD (Bring Your Own Device) devices			
2. Do you manage access permissions, including application of the principles of least privilege and separation of duties	Yes		No
3. Do you actively monitor access to critical servers, data and applications	Yes		No
4. Do you secure all computers, servers and applications according to your technical security configuration standards	Yes		No
5. Have you implemented a formal change control process including risk assessments, testing, approval and roll back	Yes		No
6. Have you implemented a whitelist to prevent unauthorised and/or malicious programs from executing	Yes		No
7. Do you allow for remote access to your network	Yes		No
If YES is remote access exclusively over secured channels (for example Virtual Private Network (VPN) with multi-factor authentication	Yes		No
8. How long after release do you implement security related patches and updates on computers and servers and network appliances (routers, firewalls etc.) Please indicate immediately / monthly / bi-annually / annually / longer			
9. Have you implemented physical controls to restrict and track access to your server room and other sensitive / critical processing facilities	Yes		No
10. Are you making use of any unsupported, or outdated software or operating systems	Yes		No

THIRD PARTY SERVICE PROVIDERS

Does your company make use of Third Party Service Providers for any of the following:

Function	Outsourced		Third party providers name
Cloud data processing/storage	Yes	No	
Data centre/hosting	Yes	No	
Data processing (marketing/payroll)	Yes	No	
Managed cyber 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 third party service providers (tick applicable)							
Administrator		User		Guest		Restricted	
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

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							
2. What is your estimated number of payment card transactions processed per year							
3. Are your point of sale (POS) terminals designed to be tamper-proof						Yes	No
4. Do you segregate your payment network from your normal network				N/A	Yes	No	
5. Are POS terminals standalone or integrated with your systems							
6. How frequently are your POS devices scanned for malware or skimming devices							

PERSONNEL CYBER SECURITY

1. Do you restrict user access based on job function and review access on at least an annual basis				Yes		No	
2. How long after termination of employment do you typically revoke user access privileges (days / weeks / months)							
3. Have you conducted any security/data/privacy training/awareness courses for employees within the last 12 months				Yes		No	
4. Number of employees with system administration privileges							
Permanent		Contractors		Temporary			

CHAPTER 3 – CYBER DIRECT COSTS

1. Approximate number of external IP addresses on your network							
2. Approximate number of servers (including virtual machines) on your network							
3. Number of locations where servers are located							
4. Approximate number of laptops utilised							
5. Approximate number of employees receiving company emails to privately owned devices							
6. How many (if any) BYOD (Bring Your Own Devices) are on your network							
7. Do you make use of professional IT Services for network solutions / IT Management						Yes	No
8. Is your backup process automated						Yes	No

9. How frequently do you generate backups (daily / weekly / monthly)	
10. If backups are generated, where do you store them	
11. How frequently do you perform restoration testing of backups (monthly / biannually / annually)	

CHAPTER 4- CYBER BUSINESS INTERRUPTION

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 (hours / days / weeks / monthly)	
2. Do you have an incident response plan including a team with defined roles and responsibilities, and timelines to restoration?	Yes <input type="checkbox"/> No <input type="checkbox"/>
3. Do you have a documented and approved disaster recovery and business continuity plans	Yes <input type="checkbox"/> No <input type="checkbox"/>
4. How long would it take you to be fully operational following a cyber incident (Hours / days / weeks / monthly)	
5. Are copies of your incident response, business continuity and/or disaster recover 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 <input type="checkbox"/> No <input type="checkbox"/>
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 such as cloud backup services	Yes <input type="checkbox"/> No <input type="checkbox"/>
7. What is the estimated financial impact of a disruption of failure of your IT environment to your business (USD Thousands / Hundreds of Thousands / Millions)	

CHAPTER 5- CYBER DIRECTORS AND OFFICERS

1. Is the company a private or public company	Private <input type="checkbox"/>	Public <input type="checkbox"/>
2. Is the company listed on a stock exchange	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If YES please advise in which country(ies) the company is listed in		
3. Do any management, officers or employees hold any of the following		
a. Outside board positions (i.e. sit on any non-subsidiary company boards)	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4. Are directors and officers made aware of their fiduciary duties in so far as cyber security is concerned to act in the best interests of the company	Yes <input type="checkbox"/>	No <input type="checkbox"/>
5. Are directors and officers actively involved in the management of the company's cyber security including oversight, implementation of cyber security practices and procedures as well as the remediation of any cyber security threats	Yes <input type="checkbox"/>	No <input type="checkbox"/>
6. Are directors and officers aware of their duty to disclose material information relating to cyber security to stakeholders and regulatory bodies	Yes <input type="checkbox"/>	No <input type="checkbox"/>
7. Are there any contractual obligations which can be affected by a cyber related incident such as agreements with customers, partners or service providers which may expose the directors and officers of the company	Yes <input type="checkbox"/>	No <input type="checkbox"/>
8. Are directors and officers trained in the compliance and governance requirements in so far as the cyber environment	Yes <input type="checkbox"/>	No <input type="checkbox"/>

9. Does the company have an employee handbook which is accessible to all employees that addresses cyber risks and exposures	Yes		No	
10. Does the company have policies and procedures in place to ensure compliance with relevant legislation with regards to cyber exposures	Yes		No	

CHAPTER 6 – CYBER THIRD PARTY LIABILITY

1. Does the company have contractual agreements with customers, partners or third parties that address cyber security requirements or data protection obligations	Yes		No	
2. Does the company transfer or share cyber risks with third parties such as shared responsibility or indemnification clauses in contracts and the like	Yes		No	
3. Do you keep any third party stock or equipment at any premises, that can be affected by a cyber event	Yes		No	
If YES please provide details and amounts in US\$ held				

DIGITAL MEDIA LIABILITY

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

SENSITIVE AND PRIVATE INFORMATION

12. Do you collect/store/process any of the following EMPLOYEE and CLIENT data				
a. Bank records or financial account details	approximate no. of records			
b. Medical records or health information	approximate no. of records			
c. Payment card details	approximate no. of records			
• do you store the card numbers	Yes		No	
• do you store the card expiry date	Yes		No	
• do you store the card validation codes (CVC/CVV number)	Yes		No	
d. Personal identity information (names, ID numbers, contact details, addresses)	approximate no. of records			
e. Third Party corporate confidential data	approximate no. of records			
13. Do you make use of or provide any web application functionality to collect sensitive information	Yes		No	
14. Have your internet facing systems been configured so that no sensitive or personal data resides directly on them, but is instead stored behind a firewall on internal databases/systems	Yes		No	

15. Have you configured your network and externally visible applications and services to ensure that access to sensitive data is restricted to properly authorised requests	Yes		No	
16. Have you implemented data retention and secure destruction policies for physical and electronic data and assets	Yes		No	
17. Have you disabled employee write access to USB devices	Yes		No	
18. Do you have public facing URL addresses (websites and services such as file transfer facilities)				
19. Approximate number of external IP addresses on your network				
20. Approximate number of servers (including virtual machines) on your network				
21. Number of locations where servers are located				
22. Approximate number of laptops utilised				
23. Approximate number of employees receiving company emails to privately owned devices				

CHAPTER 7- CYBER PROFESSIONAL INDEMNITY

1. Is there a detailed description of the professional services that your organisation offers	Yes		No	
2. Do key personnel involved in professional services have the required qualifications and experience	Yes		No	
3. Do you have a defined standard of care and diligence exercised in providing professional services to clients	Yes		No	
4. Do your standard contracts or service agreements with clients include indemnification clauses	Yes		No	
5. Are there measures in place to prevent errors and omissions in the provision of professional services	Yes		No	
6. Are there established risk management procedures to identify and mitigate potential professional liability risks	Yes		No	
7. Does your organisation adhere to industry standards and best practices in the provision of professional services	Yes		No	
8. Has your organisation experienced contractual disputes related to professional services, and so, have they been resolved	Yes		No	

REQUESTED COVER STRUCTURE

Requested cover start date

D	D	M	M	Y	Y	Y	Y
---	---	---	---	---	---	---	---

Base Policy Limits

Chapter	Limit Details	S - Small	M - Medium	L - Large	E - Extra
1 - Assessment	Method	Desk Top	Desk Top	Site Visit	Site Visit
2 - Incident Response	Up to USD	10,000	25,000	100,000	250,000
3 - Direct Costs	Up to USD	25,000	50,000	250,000	500,000
4 - Business Interruption	Up to USD	25,000	50,000	250,000	1,000,000
5 - Directors & Officers	Up to USD	100,000	150,000	500,000	1,000,000
6 - Third Party Liability	Up to USD	100,000	250,000	1,000,000	5,000,000
7 - Professional Indemnity	Up to USD	50,000	150,000	1,000,000	1,000,000
Annual Aggregate Limit (Chapters 3,4,5,6,7)	Up to USD	150,000	350,000	2,500,000	5,000,000

DESIRED LIMIT OF INDEMNITY

Please tick if an increase in the standard limit of liability is required according to business category:

Insured Category	S - Small	
	Limit	
Standard Limit	150,000	
Increase to	350,000	
	1,000,000	
	2,500,000	
	5,000,000	

Insured Category	M - Medium	
	Limit	
Standard Limit	350,000	
Increase to	1,000,000	
	2,500,000	
	5,000,000	
	7,500,000	

Insured Category	L - Large	
	Limit	
Standard Limit	2,500,000	
Increase to	5,000,000	
	7,500,000	
	10,000,000	
	12,500,000	

Insured Category	E - Extra	
	Limit	
Standard Limit	5,000,000	
Increase to	7,500,000	
	10,000,000	
	12,500,000	
	15,000,000	

DESIRED DEDUCTIBLE STRUCTURE

Please tick if an increase in the standard deductible is required according to business category:

	S - Small	M - Medium	L - Large	E - Extra
Standard Deductible (USD) Each and every event	5,000	10,000	25,000	50,000
Increased deductible to:	7,500	15,000	50,000	100,000
Increased deductible to:	10,000	25,000	75,000	150,000
Increased deductible to:	15,000	40,000	100,000	200,000
Increased deductible to:	25,000	60,000	125,000	250,000

DECLARATION

1. I know this insurance is executed and placed with a foreign Insurer and I have checked the legality of the process. I know that local regulator does not regulate foreign Insurers.
2. I declare my answers are full, correct and made under my own free will with no facts or material details omitted that may affect the risk assessment by the Insurer. It is agreed this application will be the basis for the quote.
3. I know that all questions in this application are considered material information and I do not know any further information that may affect the Insurers decision as to the cover, its scope and terms.
4. I know and agree that document will be issued in English. The fact that a document is in English, which may not be my mother tongue, will not be a basis for any claim by me towards the Insurer and the cover.
5. I know the insurance will become effective only after the Insurer has confirmed cover in writing, and also only after the premium payment has been made. It is y sole duty to read and pay attention to the different conditions of the policy.
6. Neither I nor the business proposed for insurance or any employee of mine or of the business proposed for insurance been convicted of any criminal offense, other than traffic violation in the past 5 years.
7. If the business proposed for insurance legally needs any local license or permit, it is declared and certified that such license is obtained and is valid.

Please note: It is precedent condition to any liability under this policy that the Insured or the Insured's employees will be present or be in the immediate proximity of the Insured premises at all times the premises are being used.

Name (duly authorised)

Designation

Signature

D	D	M	M	Y	Y	Y	Y
---	---	---	---	---	---	---	---

Date