Tokio Marine HCC
Torre Diagonal Mar, Josep Pla 2, Planta 10
08019 Barcelona, Spain
Tel: +34 93 530 7300 Fax: +34 93 530 7301

Proposal Form

CYBER SECURITY INSURANCE

This is a proposal form for an events/claims-discovered Policy. The Policy is subject to terms & conditions and coverage is limited to losses and claims first discovered during the period of insurance or any discovery period, if applicable.

Please note, completion and signing of this document does not bind either party to enter into a contract of insurance. However, when filling out this proposal form, do provide accurate, complete and honest information. Failure to do so may affect the right to cover should a Policy be issued.

Unless otherwise specified,

- the term "Company" refers to the Proposer and all its subsidiaries. If the information for any subsidiary differs from that provided by the Proposer, please provide this on a separate signed sheet.
- the term "Employee" refers to any natural person who is under any express or constructive contract of employment (whether full time, part-time or temporary) with the Company.

Should the space left for answering be insufficient, please use a separate signed sheet.

Information & Activities

1. Please provide the following details:

Company name (including any trading names):	
Corporate headquarters:	
Five biggest locations (by revenue):	
Number of employees:	
Date of establishment:	
Website address:	

2. Please write a brief description of your Company activity in the space provided below:

3. Consolidated Financial Overview:

	Last Completed Financial Year	Currency:
Gross Annual Revenue:		
Annual Net Income before taxes:		
Revenue arising from online activities:		

4. Please estimate the percentage split of your turnover by regions:

Work carried out for:	Last Year
Domestic clients:	%
European clients:	%
US/Canadian clients:	%
Asian-Pacific clients:	%
Other clients:	%

Cyber Footprint

5. What is the estimated total number of records, including employees and customers, that your Company holds:

6. Type of Record:

	(yes)	If yes, please provide estimated no. of records:	(no)
Personally Identifiable Information (PII)*	☐		☐
Other Personal Information (Religion, Gender…)	☐		☐
Protected Health Information (PHI)**	☐		☐
Debit/Credit Card Numbers	☐		☐
Financial Information	☐		☐
Social Security Numbers	☐		☐
Drivers Licence Numbers	☐		☐
Other type of information	☐		☐

*Information that can be used to uniquely identify, contact or locate a single person, or can be used with other sources to uniquely identify a single individual.
**Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

	(yes)	(no)
7. Do you process or store any type of records on behalf of third parties?	☐	☐

If yes, please explain:

	(yes)	(no)
8. Do you allow your staff to use personal devices for work-related purposes?	☐	☐
If yes, have you set up a Bring Your Own Device (BYOD) policy?	☐	☐

Risk-related Declarations

This section is broken down into the following three subsections:

- PEOPLE (Governance, Compliance, Human Resources...)
- PROCESSES (Policies & Procedures…)
- TECHNOLOGY (Budget, Information Technology…)

These are the three pillars upon which we can assess Security and Cyber Resilience within your organisation.

PEOPLE

9. Please answer regarding Human Resources at your Company:

	(yes)	(no)
a) Do you have a Chief Privacy Officer (CPO), Data Protection Officer (DPO) or Chief Compliance Officer who is assigned responsibility for your global obligations under relevant Data Protection and Privacy legislations?	☐	☐
b) Do you have an information security team (IST)?	☐	☐
If yes, is the IST managed from a central location and has local relays in each region where your Company operates?	☐	☐

		(yes)	(no)
c)	Does your organisation offer Privacy Awareness Training / other cyber-related trainings?	☐	☐
d)	Does your hiring process for employees require, when permitted by law, a full background check including Criminal, Educational, and Credit?	☐	☐

10. Please answer regarding Vendor & Third Party Management at your Company:

		(yes)	(no)
a)	Do you outsource any portion of your information security and/or data processing?	☐	☐

If **yes**, please provide us with the name(s) of the provider(s) and the service(s) being provided.

Provider(s):	Service(s):

b)	Do all third party contracts include the following security provisions?		
	A service level agreement that specifies security requirements and responsibilities	☐	☐
	Provisions for compliance with applicable regulations (SOX, HIPAA, PCI…)	☐	☐
	A right to audit clause	☐	☐
	Procedures for escalating security-related events	☐	☐

If any of the above responses are **no**, please explain:

c)	Do you require providers to indemnify you in case of any data breach?	☐	☐
d)	Do you require providers to have their own data protection liability insurance coverage?	☐	☐

11. Please answer regarding Audit & Compliance at your Company:

		(yes)	(no)
a)	Do you have a programme in place to periodically test IT security controls? (This can include internal audits, external audits or security consulting engagements)	☐	☐

If **yes**, do these controls include:

	Outside security specialists performing penetration testing?	☐	☐
	Automated vulnerability scanners?	☐	☐
	Secure configuration checkers?	☐	☐
	Performance tools?	☐	☐
	Source code comparison tools?	☐	☐
	Security policies and controls subject to independent reviews and audits?	☐	☐
b)	Are critical and high risk vulnerabilities remediated within one month?	☐	☐
c)	Do you comply with privacy and data protection legislation applicable to all jurisdictions and industry standards in which you operate? (e.g. Australian Privacy Principles, HIPAA privacy Rules, GDPR…)	☐	☐
d)	Is your Company subject to Payment Card Industry (PCI) Security Standards?	☐	☐
	If **yes**, what level of requirement? ☐ 1 / ☐ 2 / ☐ 3 / ☐ 4		
e)	When acquiring a new company is specific IT Due Diligence undertaken?	☐	☐
	If **yes**, is the IT system of the acquired company screened prior to acquisition?	☐	☐

PROCESSES

12. Please answer regarding Risk Mapping and Information Security at your Company:

		(yes)	(no)
a)	Have you implemented a Data & System Classification policy with specific rules that apply to each classification level?	☐	☐
b)	Have you performed an inventory of critical business information in the last 24 months?	☐	☐

13. Please answer regarding the Information Security Policy at your Company:

		(yes)	(no)
a)	Do you have a formal Information Security Policy implemented corporate-wide and applicable to all business units?	☐	☐
	If **yes**, do you:		
	Make the Policy permanently available for employees, contractors and concerned parties?	☐	☐
	Test the security required by the security policy at least once, annually?	☐	☐
	Regularly identify, assess new threats and adjust the security policy accordingly?	☐	☐
	Include Internet Usage, Acceptable Use and Email Use in the Policy?	☐	☐
	Include use and storage of information on laptops in the Policy?	☐	☐
	Share the Policy with contractors and external consultants?	☐	☐
	If **yes**, when was the last time the Policy was reviewed and / or updated?		

14. Please answer regarding the Password Policy, Logs review & Patch Management at your Company:

		(yes)	(no)
a)	Do you enforce a password management policy?	☐	☐

		< 90 days	< 180 days	Annually	Other
	If **yes**, how often are passwords required to be changed?	☐	☐	☐	

		(yes)	(no)
	And, if **yes**, is password complexity defined and made mandatory?	☐	☐
b)	Does your Company enforce a patch management process?	☐	☐
c)	Once security patches are identified, do you prioritize based on a severity & likelihood analysis?	☐	☐
d)	Are vulnerabilities and exploits monitored on a daily basis by a Security Operations Centre (SOC) or are you subscribed to a Managed Security Service Provider (MSSP)?	☐	☐

15. Please answer regarding Physical Security at your Company:

		(yes)	(no)
a)	Has a security perimeter been identified and documented (including computer rooms, media storage rooms, Data Centres, etc.)?	☐	☐
b)	Which of the following security controls have been implemented within your organisation? (please mark if applicable):		
	Biometric Access Controls to access Company Data Centre(s)	☐	
	ID badges for employee, visitor and vendor access	☐	
	Surveillance cameras and guards monitoring premises	☐	
	Data Centre access logs monitored periodically	☐	
	Smart cards used for physical security	☐	
	Physical security management centralised for all locations	☐	
	Computer, media storage and telecom room access secured and restricted to authorised personnel	☐	
	Cables and network ports protected from unauthorised access	☐	

16. Please answer regarding Disposal at your Company:

		(yes)	(no)
a)	Do you shred all written or printed personally identifiable or other confidential information when it is discarded?	☐	☐
b)	Is disposal of computer systems and media storage devices (hard drives, tapes, CDs, etc.) handled in a secure way (e.g. de-magnetisation, multiple wipes, deletion beyond reconstitution)?	☐	☐

17. Please answer regarding Computer & Network Management at your Company:

		(yes)	(no)
a)	Is separation of duties enforced in all critical process steps for all sensitive operations?	☐	☐
b)	Do you have a virus protection program in place that is installed and enabled on servers, workstations and laptops?	☐	☐
c)	To verify the security of your network perimeter, do you conduct comprehensive penetration tests?	☐	☐
	If **yes**:		
	Is physical penetration tested?	☐	☐
	Are the tests performed by external service providers in some instances?	☐	☐
	If **yes**, how many times a year are penetration tests conducted?		
d)	Are critical applications residing within internal networks (and behind the firewall) monitored 24/7 for security violations?	☐	☐
e)	Do critical systems receive full security testing before deployment?	☐	☐

18. Please answer regarding Change Management at your Company:

		(yes)	(no)
a)	When a new IT system is developed or purchased, are security considerations taken into account?	☐	☐
b)	Are staging, test and development systems kept separate from production systems?	☐	☐
	If **yes**, does that include:		
	Use of sandboxes?	☐	☐
	No sharing of databases and configuration files?	☐	☐
	No sharing of accounts?	☐	☐
	No access to production for developers?	☐	☐

TECHNOLOGY

19. What is your annual aggregate IT Budget?

Prior Year	Current Year

20. Please answer regarding IT Devices at your Company:

a)	How many Data Centres do you have?	
b)	Where are they located?	
c)	How many individual IT devices (e.g. server, desktops, laptops, mobile devices) do you deploy?	

21. Please answer regarding the Network at your Company:

		(yes)	(no)
a)	Are firewalls used to prevent unauthorised access on all connections from internal networks and systems to external networks such as vendor's systems or the internet?	☐	☐
b)	Are remote users authenticated before being allowed to connect to internal networks and systems?	☐	☐
	If **yes**, what tools have been set up? (VPN types and VPN protocols, etc.)		
c)	Is there encryption for:		
	Data at rest?	☐	☐
	Data in transit?	☐	☐
	Network (network level encryption)?	☐	☐
	Endpoint devices (Laptops, tablets and removable media)?	☐	☐
d)	Do you use anti-virus, anti-spyware or an equivalent malware protection?	☐	☐
	If **yes**, are virus signature files downloaded and updated automatically?	☐	☐
e)	Do you use Honeypots or similar techniques to detect and deflect attempts of unauthorised use of Company Information Systems?	☐	☐
f)	Are your networks and systems segregated as opposed to all residing on a flat network?	☐	☐

Cyber Incident Readiness

		(yes)	(no)
22.	Are designated employees trained to obtain and handle forensic evidence, involve law enforcement and handle press relations in response to a suspected intrusion?	☐	☐
23.	Do you have an Incident Management Programme in place that includes cyber-related incidents?	☐	☐
	If **yes**, is it:		
	Formally documented?	☐	☐
	Tested annually to ensure its effectiveness?	☐	☐
	Performed by trained personnel?	☐	☐
24.	Do you have a Business Continuity Plan (BCP) in place that includes cyber-related incidents?	☐	☐
	If **yes**, is it:		
	Managed by a dedicated group?	☐	☐
	Formally documented?	☐	☐
	Tested annually to ensure its effectiveness?	☐	☐
	Performed by trained personnel?	☐	☐
	If **yes**, does it include the use of:		
	Redundant systems and multiple Data Centres?	☐	☐
	A defined "hot site"?	☐	☐

25. How frequently do you back up electronic data?

26. Where do you store back-up electronic data?

	(yes)	(no)
27. Do you store back-up electronic data with a third party service provider?	☐	☐
28. Do you regularly ensure that data backups can be restored as quickly as possible with minimal impact?	☐	☐
29. Please indicate the acceptable time for business interruption to last until a financial loss with a significant impact on your business materializes:		

Historical Information

	(yes)	(no)
30. Are you aware of any personal or corporate data breach, cyber event (including but not limited to DDoS attacks, IT network disruption or suspension, malicious code transmission, hack) occurring at and/or spread from your IT systems or outsourced IT systems and for which a third party (including but not limited to clients, customers, data subjects or employees) might hold you responsible?	☐	☐

If **yes**, please explain:

31. During the past three years:

a) Have you experienced an interruption or suspension of your computer systems for any reason (not including downtime for planned maintenance) which exceeded 4 hours?	☐	☐
b) Has any customer or other person or entity alleged that their personal data has been compromised by you or any service provider processing, handling or collecting personal data on your behalf?	☐	☐
c) Have you ever notified any person that their information was or may have been compromised?	☐	☐
d) Has your organisation been subject to investigation by a data protection authority?	☐	☐

If **yes**, please explain:

32. Have you ever sustained an intentional breach of IT security, network damage, system corruption or loss of data?	☐	☐

If **yes**, please explain:

Data Protection:

All personal data provided to the Insurer in relation to the insurance applied for will be included in a data file controlled by HCC International Insurance Company plc and processed for the sole purpose of fulfilling the insurance contract. The Proposer expressly agrees for the data to be transferred to (i) appropriate third parties (e.g. other insurers, reinsurers, insurance or reinsurance brokers, regulatory authorities) for the purpose of co-insurance, reinsurance, portfolio assignment or management or the adoption of anti-fraud measures, as well as to (ii) other companies of the Tokio Marine group located in countries outside the European Union, with the exclusive purpose of data processing for HCC International Insurance Company plc. The Proposer and any entity or person for which insurance is applied for may at any time exercise their right to access, rectify, cancel or object to its data being processed, by notifying HCC International Insurance Company plc, 1 Aldgate, London, EC3N 1RE, United Kingdom, pursuant to the provisions of the Data Protection Act 1998.

The Proposer declares that any personal data it may provide to the Insurer related to the Proposer or any data subject has been lawfully collected and transferred with the consent of the data subject.

Signature:

Please duly sign and send this Proposal Form to: Tokio Marine HCC, Torre Diagonal Mar, Josep Pla 2, Planta 10, 08019 Barcelona, Spain. Or via email to: cyber@tmhcc.com

Name:
Position:
Date:

Signature:

Declaration

I/we confirm that the information given in this Proposal Form, whether in my/our own hand or not, is correct.

I/we declare that I/we have made a fair presentation of the risk by disclosing all material matters and circumstances which would influence a prudent insurer's assessment of the risk which we know or ought to know including my/our senior management or anybody responsible for arranging my/our insurance, having conducted a reasonable search of the information available to me/us (including information held by third parties) in order to reveal those facts and circumstances. Failing that, I/we have given the Insurer sufficient information to put a prudent insurer on notice that it needs to make further enquiries in order to reveal material matters or circumstances, whether or not those matters and circumstances were the subject of a specific question in this Proposal Form. If there are any material matters or circumstances not specifically covered by a question in this Proposal Form, I/we have listed these on a separate sheet of paper which is signed and dated and attached.

It is understood that the signing of this Proposal Form does not bind the Proposer(s) to complete or the Insurer to accept the insurance applied for.

I/we the Proposer(s) accept these conditions as the proposed Insured or agent of the proposed Insured and that any subsequent Contract of Insurance may become null and void if any of the foregoing conditions are breached.

I/we the Proposer(s) accept these conditions as the Proposed Insured or agent of the Proposed Insured.

I/we the Proposer(s) also agree that in the event any information contained in any completed Proposal Form and/or supplied to support this Proposal Form or other application for the insurance applied for changes or becomes incorrect such as to constitute a material alteration to the risk prior to the inception date of the insurance, we will advise the Insurer in writing immediately on becoming aware of such changes. In such circumstances, the Insurer will be entitled to re-assess the proposal for insurance, including but not limited to withdrawing any prior agreement to provide cover.

The person signing this Proposal Form is duly authorised to do so on behalf of the Proposer(s).