Tokio Marine HCC
Fitzwilliam House, 10 St. Mary Axe
London EC3A 8BF, United Kingdom
Tel: +44 (0)20 7648 1300

POLICY DOCUMENT
Cyber Security Insurance

Tokio Marine HCC is a trading name of **HCC International Insurance Company plc**, which is a member of the Tokio Marine HCC Group of Companies. HCC International Insurance Company plc is authorised by the UK Prudential Regulation Authority (PRA) and regulated by the UK Financial Conduct Authority (FCA) and Prudential Regulation Authority. Registered in England and Wales No. 01575839 with registered office at 1 Aldgate, London EC3N 1RE, UK.

PLEASE NOTE:

The cover provided by this Policy is afforded solely with respect to Cyber Events and Claims first Discovered during the Policy Period or any applicable Extended Trigger Period and Reported pursuant to the provisions of 7.1 Notice.

Terms in **bold** onwards in this Policy have the meaning provided under 4 – Definitions.

The **Policyholder** is requested to read this Policy and Schedule carefully and to review the coverage with an insurance agent or broker to ensure that the contents and the terms and conditions of cover are fully understood.

If the Policy or Schedule is incorrect, please return it immediately for alteration to HCC International Insurance Company Plc, Fitzwilliam House, 10 St. Mary's Axe, London, EC3A 8BF, United Kingdom.

SAMPLE

Schedule

ITEM 1	POLICY NO.	
ITEM 2	POLICYHOLDER / PRINCIPAL ADDRESS	Email:
ITEM 3	POLICY PERIOD	(a) Inception Date: (b) Expiration Date: both days inclusive at .
ITEM 4	LIMIT OF LIABILITY, SUB-LIMITS AND EXTRA LIMITS:	(a) Aggregate Limit of Liability: GBP for all **Cyber Events**, all **Losses** combined. (b) Optional Extensions and Sub-limits:

Extension	Covered	Sub-Limit
Contingent BI Loss	Yes / No	GBP in respect of **Cloud Providers** only
Accidental Event BI Loss	Yes / No	GBP /n.a.
Betterment Costs	Yes / No	GBP /n.a.
Network Usage Fraud and Cryptojacking	Yes / No	GBP /n.a.
Goodwill Gestures	Yes / No	GBP per **Data Breach** victim, however GBP for all victims
PCI Penalties and Additional Costs	Yes / No	GBP /n.a.
Diverted Funds	Yes / No	GBP /n.a
Bricking Costs	Yes / No	GBP /n.a

All Sub-limits are aggregate for the whole Policy Period and Extended Trigger Period and are part of and not in addition to the Aggregate Limit of Liability stated above.

(c) Extra limits or no erosion of the Aggregate Limit of Liability:

Extension	Covered	Extra Limit
Preventive Consulting Services	Yes / No	GBP in the aggregate for the whole **Policy Period**

ITEM 5 RETENTION:

GBP per **Single Event**, not applying to:

(a) **Emergency Response Costs**

(b) **BI Loss**

(c) **Monitoring Costs**

(d) Preventive Consulting Services (Extension 3.6)

ITEM 6 BI LOSS INDEMNITY PERIOD:

(a) Start:

(i) **Insured's Systems Disruption**: 10 hours from **Reporting**

(ii) **Contingent BI Loss**: [ ] hours from **Reporting**

(b) End: 120 days from start as defined in (a) above

ITEM 7 INCIDENT COORDINATOR:

Crawford & Company

Hotline:

Email:

ITEM 8 TERRITORY

Worldwide (to the extent permitted by law)

ITEM 9 APPLICABLE LAW:

ITEM 10 EXCLUSIVE JURISDICTION:

ITEM 11 PREMIUM:

GBP plus applicable tax

ITEM 12 INSURER:

HCCI International Insurance Company Plc

ITEM 13 UNDERSIZED SECURITY REMEDIATION TIMEFRAMES:

CVSS Score	Time Limit
7-10	15 days from first availability of patch, fix, or mitigation technique.
4-6	30 days from first availability of patch, fix, or mitigation technique.
1-3	90 days from first availability of patch, fix, or mitigation technique.

IMPORTANT NOTICES:

The **Policyholder** hereby confirms that it has received the following information in written form before the conclusion of this Policy:

Information in respect of the Insurer

The risk is insured by:

HCC INTERNATIONAL INSURANCE COMPANY PLC

Authorised by the UK Prudential Regulation Authority (PRA) and regulated by the PRA and the UK Financial Conduct Authority (FCA)

Registered in England and Wales No. 01575839

Registered Address: 1 Aldgate, London, EC3N 1RE, United Kingdom

SAMPLE

Data Protection and Privacy Policy

Tokio Marine HCC respects your right to privacy. In our Privacy Policy (available at https://www.tmhcc.com/en/legal/privacy-policy) we explain who we are, how we collect, share and use personal information about you, and how you can exercise your privacy rights. If you have any questions or concerns about our use of your personal information, then please contact DPO@tmhcc.com.

We may collect your personal information such as name, email address, postal address, telephone number, gender and date of birth. We may also collect your sensitive personal information such as data relating to your physical or mental health or condition. We need the personal or sensitive personal information to enter into and perform a contract with you. We retain personal information and sensitive personal information we collect from you where we have an ongoing legitimate business need to do so.

We may disclose your personal or sensitive personal information to:

- our **group companies**;
- **third party services providers and partners** who provide data processing services to us or who otherwise process personal information for purposes that are described in our Privacy Policy or notified to you when we collect your personal information;
- any **competent law enforcement body, regulatory, government agency, court or other third party** where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your interests or those of any other person;
- a **potential buyer** (and its agents and advisers) in connection with any proposed purchase, merger or acquisition of any part of our business, provided that we inform the buyer it must use your personal information only for the purposes disclosed in our Privacy Policy; or
- any **other person with your consent** to the disclosure.

Your personal and sensitive personal information may be transferred to, and processed in, countries other than the country in which you are resident. These countries may have data protection laws that are different to the laws of your country. We transfer data within the Tokio Marine group of companies by virtue of our Intra Group Data Transfer Agreement, which includes the EU Standard Contractual Clauses.

We use appropriate technical and organisational measures to protect the personal information that we collect and process about you. The measures we use are designed to provide a level of security appropriate to the risk of processing your personal information.

You are entitled to know what data is held on you and to make what is referred to as a **Data Subject Access Request ('DSAR')**. You are also entitled to request that your data be **corrected** in order that we hold accurate records. In certain circumstances, you have other data protection rights such as that of **requesting deletion, objecting to processing, restricting processing** and in some cases **requesting portability**. Further information on your rights is included in our Privacy Policy.

You can **opt-out of marketing communications** we send you at any time. You can exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing e-mails we send you. Similarly, if we have collected and processed your personal or sensitive personal information with your consent, then you can **withdraw your consent** at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent. You have the **right to complain to a data protection authority** about our collection and use of your personal information.

SAMPLE

Complaints Procedure

Tokio Marine HCC is dedicated to providing a high-quality service at all times to the **Insurer**'s clients. Should the **Named Company** or the **Insureds** not be satisfied, or for any questions or concerns about the Policy or any **Claim**'s handling, please contact us as follows:

The Head of International Compliance,

HCC INTERNATIONAL INSURANCE COMPANY PLC

1 Aldgate, London,

EC3N 1RE - United Kingdom

Should we be unable to resolve any difficulty directly with you to your satisfaction, you may be entitled to refer the dispute to the United Kingdom Financial Ombudsman Service who will review your case and who may be contacted at:

Financial Ombudsman Service

South Quay Plaza

183 Marsh Wall

London E14 9SR - United Kingdom

Email: complaint.info@financial-ombudsman.org.uk

Telephone: +44 (0)845 080 1800

SAMPLE

Contents

SAMPLE

TOKIO MARINE HCC

CYBER SECURITY INSURANCE

1. What to Do in Case of an Incident

If you are faced with or suspect a **Cyber Event**, please contact the **Incident Coordinator** immediately by calling the Hotline mentioned in ITEM 7 of the Schedule. It is essential to contact the **Incident Coordinator** as soon as practicably possible in order to reduce any potential or actual **Loss**.

Once contacted through the Hotline, the **Incident Coordinator** will recommend and coordinate any necessary immediate and further response to contain or avoid any **Cyber Event** and minimise **Loss** and will also guide you through the next steps of substantiating incidents and **Losses**.

Please find a complete description of the Reporting process and duties and the **Incident Coordinator**'s intervention in 7- Reporting and Handling of Incidents and Claims.

2. What is Covered (Standard Coverage)

The **Insurer** shall pay to or on behalf of the **Insured** the following **Losses** (per type of **Cyber Event**) resulting directly and exclusively from a **Cyber Event**, provided that such **Cyber Event** is first **Discovered** during the **Policy Period** and **Reported** as provided under 7.1 Notice, and subject to any Sub-limit stated in ITEM 4 of the Schedule.

CYBER EVENTS	INSURED LOSSES - First Party directly paid or incurred by the Insured	INSURED LOSSES - Liability arising from a Claim or Investigation targeting the Insured
Data Breach	• Emergency Response Costs • Event Management Costs • Notification Costs • Monitoring Costs • Recovery Costs	• Damages • Regulatory Fines and Penalties • Defence Costs • Investigation Costs
Cyber Attack	• Emergency Response Costs • Event Management Costs • Recovery Costs	• Damages • Defence Costs • Investigation Costs
Human Error	• Emergency Response Costs • Event Management Costs • Recovery Costs	• Damages • Defence Costs • Investigation Costs
Insured's Systems Disruption	• BI Loss	• N/A
Electronic Media Claim	• Emergency Response Costs • Event Management Costs	• Damages • Defence Costs
E-threat	• E-threat Response Costs	• Damages • Defence Costs

SAMPLE

3. What Else is Covered (Extensions)

Please note:

- Any **Cyber Event** added by Extension is only covered to the extent it is first **Discovered** and **Reported** as provided under 7.1 Notice (save for the application of Extension 3.2 Extended Trigger Period);
- Any **Loss** added by Extension is covered only to the extent it results directly and exclusively from the **Cyber Event** referred to or added by the same Extension;
- Some extended covers below are subject to a sub-limit. Please refer to ITEM 4 of the Schedule.

Automatic Extensions

Cover hereunder is automatically extended as follows:

3.1 NEW SUBSIDIARIES

Any **Subsidiary** first created or acquired by the **Policyholder** during the **Policy Period** shall be included automatically as an **Insured Entity** from the effective date of its acquisition or creation provided that:

(a) the total number of clients of such **Subsidiary** does not exceed 25% of the number of clients of the **Policyholder**, and

(b) The total revenue of such **Subsidiary** does not exceed 25% of the total revenue of the **Policyholder**, and

(c) it does not derive more than 25% of its overall revenue from operations and activities in the United States of America, its territories and possessions, and

(d) its business activities are included within the business activities of one or more **Insured Entities** existing at the date of its acquisition or creation.

Any other newly acquired or created **Subsidiary** shall only be included as an **Insured Entity** if specifically endorsed hereto in writing and any additional premium and/or amendment of cover terms requested by the **Insurer** has been agreed within ninety (90) days from the effective date of its creation or acquisition.

3.2 EXTENDED TRIGGER PERIOD

If any cover under this Policy is neither renewed nor replaced upon expiry, and to the extent it has not been cancelled for non-payment of premium, the time limit for **Discovery** and **Reporting** is extended up to ninety (90) days from the Expiry Date of the **Policy Period** (Extended Trigger Period), but solely in respect of **Cyber Events** actually occurring, or alleged or suggested in a **Claim** or **Investigation**, during the **Policy Period**. An Extended Trigger Period shall not be afforded in case of a **Change in Control**.

For the purposes of this Extension only, the **Reporting** timeframe under 7.1(a)(ii) is extended up to the expiry of the Extended Trigger Period, with a thirty (30) days' extra notice period where it has not been practically possible to Report within the Extended Trigger Period

3.3 MITIGATION COSTS

Loss is extended to include any **Mitigation Costs** arising from **Circumstances** first **Discovered** during the **Policy Period**.

Optional Extensions

Cover under the following Extensions is afforded solely to the extent marked as Covered in ITEM 4 of the Schedule.

3.4 CONTINGENT BI LOSS

(a) **Cyber Events** are extended to include **Outsourced Systems Disruptions**, and

(b) **Loss** is extended to include **BI Loss** arising directly and exclusively from an **Outsourced Systems Disruption,** subject however to the sub-limit stated in ITEM 4(b) of the Schedule to the extent that such **Outsourced Systems Disruption** was caused or contributed to by a negligent act, error or omission of a **Cloud Provider** or any of its employees or service providers.

SAMPLE

3.5 ACCIDENTAL EVENT BI LOSS

(a) **Insured's Systems Disruption** is extended to include the unavoidable interruption, unavailability or disruption, in whole or in part, of the **Insured's Systems** as the sole and direct result of an **Accidental Event**, and

(b) **Loss** is extended to include **BI Loss** arising directly and exclusively from an **Insured's Systems Disruption** as defined in (a) above.

3.6 PREVENTIVE CONSULTING SERVICES

At the **Policyholder**'s election, any **Insured** may benefit from a selection of services from the Cyber Menu included in Appendix 1 for the purpose of assessing the **Insured**'s exposure and possible ways to enhance resilience to **Cyber Events**.

The costs of such services are covered up to the amount stated in ITEM 4(c) of the Schedule, which is separate from and in addition to the Aggregate Limit of Liability stated in ITEM 4(a) of the Schedule (see 5.2.(c) Extra Limit for Preventive Consulting Services). The **Insured** shall however be free to extend services beyond what the Extra Limit allows at its own costs.

3.7 BETTERMENT COSTS

Loss is extended to include any legally insurable **Betterment Costs** arising from a covered **Cyber Attack**.

3.8 NETWORK USAGE FRAUD AND CRYPTOJACKING

The **Insurer** shall indemnify the **Insured Entity** for any portion of extra charges that:

(a) any information technology, internet or telephony provider of the **Insured Entity** has refused to write off at the **Insured Entity**'s verifiable request, and sustained as a direct result of the unauthorised use of the **Insured's Systems**, or any telephone systems operated and administered by the **Insured Entity** for its business, and

(b) any power utility of the **Insured Entity** has refused to write off at the **Insured Entity**'s verifiable request and sustained as a direct result of the unauthorised use of the **Insured's Systems** to mine cryptocurrencies.

For the purposes of this Extension, such extra charges shall be considered **Loss** hereunder.

3.9 GOODWILL GESTURES

The **Insurer** shall indemnify the **Insured Entity** for any **Goodwill Gestures**, which shall be considered **Loss** hereunder for the purposes of this Extension.

3.10 PCI NON-COMPLIANCE PENALTIES AND ADDITIONAL COSTS

Loss is extended to include the following costs, expenses and losses sustained by the **Insured Entity** resulting directly and exclusively from a **PCI Non-compliance**:

(a) **PCI Penalties**;

(b) **Investigation Costs** including, for the purpose of this extension, the **cost** of any investigation or audit carried out by or on behalf of credit or debit card scheme members or card issuers that the **Insured Entity** is legally liable to pay;

(c) **Emergency Response Costs** and **Event Management Costs** including, for the purpose of this extension, the reasonable and necessary IT and legal expenses paid by the **Insured Entity** to co-operate with an investigation or audit as mentioned under (a) above, but excluding the remuneration of any employee of the **Insured Entity**, the cost of their time and any other costs or overheads of the **Insured Entity**:

(d) **Damages** including for the purpose of this extension, any costs, expenses, liabilities or losses incurred by a card scheme member for the management of the **PCI Non-compliance** that the **Insured Entity** is legally liable to reimburse to such card scheme member under a merchant services agreement.

3.11 DIVERTED FUNDS

Loss is extended to include the amount of funds transferred from the **Insured Entity**'s bank accounts to a **Third Party** not entitled to receive such funds as a direct result of:

(a) a **Cyber Attack**, or

SAMPLE

(b) the **Insured Entity** or any of its employees, directors or officers, having relied in the ordinary course of business on electronic data or instructions fraudulently impaired, input, modified, prepared or initiated using a **Cyber Attack**, except to the extent:

(i) such transfer was intended as or for a loan, extension of credit or similar transaction,

(ii) the data or instructions relied upon purported to represent physical documents, or

(iii) at the time of the transfer of funds, the person authorising or proceeding with it did not strictly follow applicable written procedures for funds transfer, or no such written procedures were in place or their application was not monitored at the **Insured Entity**.

This extension does not include any lost funds, the transfer of which was permitted, contributed or facilitated in any way by phishing or by any instructions made over the telephone or otherwise made by voice.

3.12 BRICKING COSTS

Loss is extended to include **Bricking Costs** arising from a **Cyber Attack**, **Data Breach** or **Human Error**.

4. Definitions

Terms in **bold print** as used in this Policy shall have the following meaning:

4.1 Accidental Event	The power outage, over or under voltage, electrostatic build-up, static electricity or circuit overheating of any power supply device or system owned and operated only by the **Insured Entity**
4.2 Betterment Costs	The fees, costs and expenses (including the fees for the advice of **Third Party** information technology professionals) incurred by the **Insured Entity** with the **Insurer**'s prior written consent (not to be unreasonably withheld or delayed) for the correction, upgrade, replacement, re-sizing or re-design of any part or contents of the **Insured's Systems** hit by a covered **Cyber Attack**, strictly necessary to durably remediate any vulnerability on that part of the **Insured's System** and prevent the repetition of any **Security Breach.**
4.3 BI Loss	Losses suffered and costs incurred by the **Insured Entity** during the indemnity period stated in ITEM 6 of the Schedule directly and exclusively as a result of an **Insured's Systems Disruption** or an **Outsourced Systems Disruption** (if covered); such losses and costs to be calculated and substantiated in accordance with 7.3 BI Loss Valuation.
4.4 Bricking Costs	The repurchasing costs incurred by the **Insured Entity** (with the **Insurer**'s prior written consent not to be unreasonably withheld or delayed) of any part or contents (including data) of that part of the **Insured's Systems** impaired, lost or destroyed as a direct result of a **Cyber Attack**, **Data Breach** or **Human Error**, where it is technically impossible to restore it or where it is more time efficient and cost-effective than recovering it or restoring it.
4.5 Change in Control	Any of the following in respect of the **Policyholder**: (a) the merger with or consolidation into any other entity, or (b) any person or company other than an **Insured Entity** acting alone or in concert:

SAMPLE

(i) acquiring ownership or control or assuming control pursuant to a written agreement with other shareholders of more than 50% of the voting rights in the **Policyholder** and/or more than 50% of the outstanding shares representing the present right to vote for the election of the board of directors of the **Policyholder** and/or assuming the right to appoint or remove the majority of the board of directors of the **Policyholder**; or

(ii) acquiring ownership of all or the majority of the assets of the **Policyholder**; or

(c) the appointment of a receiver, administrator, or liquidator, or the equivalent in any jurisdiction.

4.6 Circumstance

Any fact, matter or circumstance which would cause a reasonable person to believe that a **Cyber Event** may have occurred or will occur. **Circumstances** shall not include any **Cyber Event** which has been **Discovered**. All **Circumstances** resulting from one same originating cause will be deemed to be one single **Circumstance** and to have first been **Discovered** at the time of the earliest **Discovery**.

4.7 Claim

(a) Any written request or demand made to the **Insured** by or on behalf of a **Third Party** seeking monetary or non-monetary relief, or

(b) Any criminal proceedings against the **Insured**, or

(c) Any regulatory proceedings commenced against the **Insured** by a competent regulatory body with specific authority in respect of data protection laws and regulations,

arising directly and exclusively of a **Cyber Event** for which the **Insured** is alleged to be responsible.

4.8 Cloud Provider

A **Service Provider** providing hosted computer application services to the **Insured Entity** or processing, maintaining, hosting or storing the **Insured Entity**'s electronic data and disclosed to and agreed by the **Insurer**.

4.9 Cyber Attack

The fraudulent, malicious or dishonest:

(a) causing or use of a **Security Breach**, or

(b) disruption or overload of the **Insured's Systems**

by a **Third Party** for any purpose.

Cyber Attack shall not include any **Human Error**.

4.10 Cyber Event

(a) Any of the events listed under 2 – What Is Covered, whether actual or alleged or suggested in a **Claim** or **Investigation**, and

(b) Any event added as **Cyber Event** under 3 – Extensions.

All **Cyber Events** resulting from one same originating cause will be deemed to be one single **Cyber Event** and to have first been **Discovered** at the time of the earliest **Discovery**.

4.11 Damages

The amount of final: judgments, arbitral awards or settlement agreements (to the extent entered into with the **Insurer**'s prior written consent), that the **Insured** is legally obliged to pay as a result of a **Claim**.

Damages shall not include:

(a) any fines or penalties (except **PCI penalties** if covered hereunder),

(b) any taxes,

(c) any non-compensatory damages,

(d) the loss, offset or return of any remuneration or profit of the **Insured** or the cost of re-performing any services of the **Insured**,

(e) the costs of carrying out any non-monetary relief, or

(f) any sums payable by reason of the payment by the **Insured** of any amounts in breach of relevant terrorism laws.

4.12 Data Breach

Any of the following if actually or allegedly caused, permitted or made possible by an **Insured Entity** or any other entity holding or processing **Protected Data** on behalf of the **Insured Entity**:

(a) The inadvertent loss, destruction or alteration of, or

(b) The unauthorised disclosure or dissemination of or access to,

Protected Data lawfully collected and held by or on behalf on the **Insured Entity**, including due to the negligent loss of documents, hardware or any other media containing access or security information.

4.13 Defence Costs

The reasonable and necessary professional costs incurred by the **Insured** with the **Insurer**'s prior written consent (which shall not be unreasonably withheld or delayed) to defend, investigate and settle any **Claim**, including the reasonable premiums (but not the collateral) for any appeal bond, attachment bond or similar bond for any civil proceeding.

Defence Costs shall not include any overheads costs or the salary of any employee, director or officer of the **Insured** or any person or entity for whose acts the **Insured** is alleged to be legally liable.

4.14 Discovery / Discovered

The time when a **Responsible Person**, not implicated in any deliberate **Cyber Event**, first becomes aware of:

(a) a **Cyber Event**,

(b) a **Claim** or **Investigation** alleging or anticipating a **Cyber Event**,

whichever awareness occurs first, or

(c) a **Circumstance**,

regardless of whether the knowledge of such **Responsible Person** is sufficient at such time to prove that such **Cyber Event** or **Circumstance** is covered under this Policy and to which extent.

4.15 Electronic Media Claim

Any **Claim** made against the **Insured Entity** by a **Third Party** arising directly and exclusively from:

(a) libel, slander or any other reputational damage, or

(b) breach of any intellectual property right, right of publicity or privacy right,

alleged to have resulted from the content of, or deep-linking or framing within, a public social media or webpage or e-mailing designed and/or sent for the business of the **Insured Entity**.

Electronic Media Claims shall not include any **Claim** based upon, arising from or attributable to any actual or alleged act of discrimination on any grounds.

4.16 Emergency Response Costs

All fees and costs of the **Legal Response Team**, the **IT Response Team** and the **PR Response Team** for services provided to the **Insured Entity**, as recommended and coordinated by the **Incident Coordinator**, within 72 hours from **Reporting** of a **Cyber Event** or **Circumstance**, to:

(a) substantiate the existence, cause and extent of a **Cyber Event**; and

(b) contain the immediate spreading or consequences of such **Cyber Event**.

4.17 E-threat

A verifiable threat made specifically to the **Insured Entity** by any means (including ransomware) to cause or pursue a **Cyber Attack** or a **Data Breach** unless certain conditions (including payments) are met.

4.18 E-threat Response Costs

The following amounts incurred or paid by the **Insured Entity** for the investigation, resolution or mitigation of the consequences of an **E-threat**, to the extent previously recommended and approved by the **Incident Coordinator**:

(a) the reasonable and necessary fees and expenses of the **Legal Response Team**, **IT Response Team**, **PR Response Team** and any extortion specialist,

(b) any legally insurable payment to the **E-threat** perpetrator, and

(c) any payments to an informant for information not otherwise available.

4.19 Event Management Costs

All of the following costs incurred by the **Insured Entity** after the **Reporting** of an actual **Cyber Event**:

(a) **Forensic Costs**, which means the reasonable and necessary fees, costs and expenses of the **IT Response Team** in:

(i) substantiating the existence, cause and origin of the **Cyber Event** (including, where applicable, the perpetrator), to the extent the incurring **Emergency Response Costs** has not allowed for the ascertainment of the foregoing,

(ii) assessing to what extent the **Cyber Event** has compromised or caused the loss or impairment of **Protected Data** or the **Insured's Systems**, and

(iii) containing any actual or anticipated compromise or loss of, or damage to, **Protected Data** or the **Insured's Systems** caused by the **Cyber Event**, including by giving advice on the preservation or restoration of any exposed electronic data, the removal of malwares from the **Insured's Systems** and the resolution of a denial of service attack,

but excluding any **Betterment Costs** or **Bricking Costs** (if covered hereunder).

(b) **Legal Costs**, which means the reasonable and necessary fees, costs and expenses of the **Legal Response Team** in:

(i) providing preliminary advice to the **Insured Entity** on the possible legal consequences of the **Cyber Event**, and how to address or mitigate such consequences, including, in respect of a **Data Breach**, the necessity to notify victims or regulators or to offer monitoring services; and

(ii) preparing any required notifications to victims of a **Data Breach** or to any competent regulatory authorities in respect

of the **Cyber Event,** but excluding any **Defence Costs** or **Investigation Costs**.

(c) **PR Costs**, which means the reasonable and necessary fees, costs and expenses of the **PR Response Team**, incurred by the **Insured Entity** upon recommendation of and with the prior written consent of the **Incident Coordinator**, to devise a public relation campaign for the sole purpose of limiting the reputational consequences for the **Insured Entity** of a **Cyber Event** that is being, or at risk of being, publicised in any media, and to advise the **Insured Entity** throughout such campaign.

4.20 Financial Infrastructure

Any financial transaction or payment process platform including any securities exchanges, central counterparty clearing houses, and central securities depositories.

4.21 Goodwill Gesture

The reasonable amount of any goodwill or commercial gestures including coupons, discounts or payments, consented by the **Insured Entity** to any victim of a **Data Breach** that the **Insured** has notified to such victim, to mitigate the adverse reputational impact of the same for the **Insured Entity** and effectively redeemed or cashed within twelve (12) months of receipt of such gesture by the victim.

Goodwill Gestures shall not include any **Notification Costs** or **Monitoring Costs**.

4.22 Human Error

A **Security Breach** inadvertently caused or contributed by negligent acts or errors in the active maintenance, operation, programming or update of the **Insured's Systems** by or on behalf of the **Insured Entity**.

4.23 Incident Coordinator

Crawford Co as stated in ITEM 7 of the Schedule.

4.24 Insured

(a) Any **Insured Entity**, and

(b) Any **Responsible Person**, solely in respect of **Claims** or **Investigations** directed towards them in their capacity as such and solely for "Liability" Insured **Losses** as listed under 2 – What is Covered.

4.25 Insured Entity

The **Policyholder** or any of its **Subsidiaries**:

(a) existing on or before the inception of the **Policy Period**, or

(b) included as a **Subsidiary** during the **Policy Period** pursuant to 3.1 New Subsidiaries.

4.26 Insured's Systems

Any computer systems (including hardware and software and electronic data relating to systems configuration or parameters) operated and administered by the **Insured Entity** for its business, excluding any telephone systems.

4.27 Insured's Systems Disruption

The unavoidable interruption, unavailability or disruption, in whole or in part, of the **Insured's Systems** or any electronic data contained therein as the sole and direct result of:

(a) a **Cyber Attack**,

(b) **Human Error**, or

(c) a systems shutdown ordered by a competent civil authority or recommended by the **IT Response Team** in response to a **Cyber Attack.**

4.28 Insurer

HCC International Insurance Company Plc, as named in ITEM 12 of the Schedule, having its registered office at 1 Aldgate, London EC3N 1RE – United Kingdom.

4.29 Investigation

Any official hearing of, or official request for information made specifically to, the **Insured**, by any competent regulatory body in respect of any actual or potential **Cyber Event** before any **Claim** is made in connection thereto.

Investigations shall not include any routine or sector-wide inquiry or investigation.

4.30 Investigation Costs

The reasonable and necessary fees and costs of the **Legal Response Team** incurred by the **Insured** with the **Insurer**'s prior written consent (which shall not be unreasonably withheld or delayed) for its representation at or response to an **Investigation**.

4.31 IT Response Team

(a) Any of the persons or entities named as such in Appendix 2, or

(b) any other independent information technologies experts instructed by the **Insured Entity** with the **Insurer**'s prior written consent.

4.32 Legal Response Team

(a) Any of the persons or entities named as such in Appendix 2, or

(b) any other independent law firm instructed by the **Insured Entity** with the **Insurer**'s prior written consent.

4.33 Loss

Any of the heads of covers listed as "Insured Losses" under 2 - What Is Covered?, plus those included as **Loss** by Extension.

4.34 Mitigation Costs

All reasonable:

(a) **Third Party** professional fees, costs and expenses (other than **Emergency Response Costs**, **Defence Costs** or **Investigation Costs**) paid by an **Insured Entity**, and

(b) payments (or part thereof) made by an **Insured Entity** to identified **Third Parties**,

exclusively to avoid or mitigate the consequences of a **Circumstance Reported** in accordance with 7.1.(a) How and When to Report, solely to the extent that:

(i) the **Insured Entity** has obtained the written consent of the **Insurer** prior to incurring such sums, and

(ii) **Mitigation Costs** shall not exceed the amount of covered **Loss** that the **Insured** establishes to the reasonable satisfaction of the

Insurer would, but for the payment of **Mitigation Costs**, result or have resulted from such **Circumstance**.

Mitigation Costs do not include **Goodwill Gestures**.

4.35 Monitoring Costs

The reasonable costs of:

(a) professional credit and identity theft monitoring services, and

(b) the setting up and operation of external call centre services, or the extension of existing call centre services of the **Insured Entity**,

for the benefit of any natural person victim of a **Data Breach** and incurred by the **Insured Entity** for a period of up to twelve (12) months from **Reporting** of such **Data Breach**.

Monitoring Costs shall only be covered hereunder to the extent that the **Legal Response Team** has, prior to the incurring of such costs:

(i) advised that both the notification and monitoring costs services are required or shall mitigate **Loss** in respect of such natural person, and

(ii) included an offer for such services in any notification sent to victims of the **Data Breach**.

4.36 Notification Costs

The reasonable and necessary costs incurred by the **Insured** to notify:

(a) any victim of a **Data Breach**, and

(b) any competent regulatory body in respect of a **Data Breach**,

to comply with applicable laws and regulations, or to mitigate any potential **Loss**, in respect of such **Data Breach**. **Notification Costs** shall be deemed necessary to the extent that notification is expressly requested or advised as necessary by the **Legal Response Team**, the **Incident Coordinator** or a competent regulatory body.

4.37 Outsourced Systems

Any computer systems including hardware, software and electronic data used or contained therein (but excluding any telephone systems) operated and maintained by a **Service Provider** on behalf and for the business of the **Insured Entity**.

4.38 Outsourced Systems Disruption

The unavoidable interruption, unavailability or disruption, in whole or in part, of **Outsourced Systems**, however caused.

4.39 PCI Non-compliance

Any actual or alleged non-compliance of the **Insured Entity** with the Payment Card Industry Data Security Standards

4.40 PCI Penalties

The amount of any penalties that the **Insured Entity** is legally liable to pay or reimburse to a payment card scheme member as the sole and direct result of a **PCI Non-compliance.**

4.41 Policy Period

The period stated in ITEM 3 of the Schedule.

4.42 Policyholder

The entity named in ITEM 2 of the Schedule.

4.43	**Protected Data**	(a) In respect of any natural person, any information relating to such person that allows identification of her or him directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity, or (b) In respect of any business or professional, any information of any kind not known or readily ascertainable by proper means by others, the holding and secrecy of which brings economic value or competitive advantage to such business or professional.
4.44	**PR Response Team**	(a) Any of the persons or entities named as such in Appendix 2, or (b) any other independent public relation consultants instructed by the **Insured Entity** with the **Insurer**'s prior written consent.
4.45	**Recovery Costs**	The reasonable and necessary fees and costs of the **IT Response Team** in restoring or recollecting any part or contents (including data not relating to systems configuration or parameters) of the **Insured's Systems** impaired, lost or destroyed as a direct result of a **Cyber Attack**, **Data Breach** or **Human Error** to its state immediately before such **Cyber Event**, or to the available technical equivalent. **Recovery Costs** shall not include **Bricking Costs** or **Betterment Costs** (if covered hereunder).
4.46	**Regulatory Fines and Penalties**	Any legally insurable civil or administrative fines or penalties awarded against the **Insured** as a result of a **Claim** by a regulatory body based upon a **Data Breach**.
4.47	**Reporting / Reported**	The reporting of a **Cyber Event** or **Circumstance** in accordance with 7.1 Notice.
4.48	**Responsible Person**	Any member of the board of directors or management board, managing director, Chief Executive Officer, Chief Financial Officer, Chief Operation Officer, Chief Information Security Officer, Chief Technology Officer, Risk Manager, Head of IT, General Counsel, Head of Audit (or holder of any equivalent position) of the **Insured Entity**.
4.49	**Security Breach**	(a) The unauthorised access to, (b) The impairment or destruction of data or programs within, or (c) The input of unauthorised data or codes into, the **Insured's Systems** by any person by any means and for any purpose.
4.50	**Service Provider**	Any independent **Third Party** providing information technology services to the **Insured Entity** in accordance with a written contract with such **Insured Entity**. **Service Provider** does not include any **Third Party** providing **Financial Infrastructure.**
4.51	**Single Event**	One or a series of **Circumstances** and/or **Cyber Events** having the same originating cause or source.

A **Single Event** shall be deemed **Discovered** at the time of the earliest **Discovery** of a **Circumstance** or **Cyber Event** of such series.

4.52 Subsidiary

Any legal entity within which and during such time that the **Policyholder**, either directly or through one or more **Subsidiaries**:

(a) owns more than 50% of the issued and outstanding shares; or

(b) controls more than 50% of the voting rights; or

(c) controls the right to vote for the election or removal of the majority of the board of directors.

For the avoidance of doubt, cover shall be afforded hereunder only in respect of **Cyber Events** at any such entity if it is first **Discovered** during the time the entity qualified as a **Subsidiary** as defined above.

4.53 Third Party

Any person or corporate entity other than an **Insured Entity** or a **Responsible Person**.

5. Extent of Cover (Trigger, Amount, Duration, Consent)

Coverage under this Policy is subject to limitations in terms of:

- when a **Cyber Event** or **Circumstance** is first **Discovered** – see 5.1
- amount of **Loss** covered – see 5.2
- for some **Losses**, duration of cover– see 5.3
- the **Insurer**'s consent for consultants' costs – see 5.4

5.1 POLICY TRIGGER AND ATTACHMENT

(a) This Policy covers only **Cyber Events** and **Circumstances** which are first **Discovered** (whether directly or as indicated, alleged or suggested in a **Claim** or **Investigation**) and **Reported** in the **Policy Period**.

(b) All **Cyber Events, Circumstances**, **Claims** and/or **Investigations** having the same originating cause or source shall be deemed together as a **Single Event**, which shall be deemed first **Discovered** at the time of earlier **Discovery** and shall be applied only one retention amount if covered under this Policy.

5.2 AMOUNT

(a) Total Maximum – Aggregate Limit of Liability

The maximum aggregate liability of the **Insurer** under this Policy in respect of all **Cyber Events**, **Losses** and **Insured** shall be the Aggregate Limit of Liability stated in ITEM 4 of the Schedule.

No provision hereunder or recovery made by the **Insurer** shall have the effect of increasing such aggregate limit, except to the extent of the extra limit under Extension 3.6 Preventive Consulting Services, if purchased.

(b) Sub-Limited Covers

For those **Losses** subject to sub-limits as stated in ITEM 4 (b) of the Schedule, the maximum liability of the **Insurer** shall be the indicated sub-limit, regardless of the number of **Losses** and **Circumstances** and regardless of the numbers of **Insureds** claiming under this Policy. When the sub-limit applicable to a type of **Loss** is exhausted, no further **Loss** of the same type shall be payable hereunder.

Save where otherwise stated in the Schedule, sub-limits are aggregate for the whole **Policy Period** and Extended Trigger Period and are included in and not in addition to the Aggregate Limit of Liability stated in ITEM 4 of the Schedule.

(c) Extra Limit for Preventive Consulting Services

SAMPLE

Notwithstanding the provisions under (a) and (b) above, the costs covered under Extension 3.6 Preventive Consulting Services shall be separate from and in addition to the Aggregate Limit of Liability or any Sub-Limits and shall not erode them, subject to the maximum amount stated as Extra Limit in ITEM 4(c) of the Schedule.

(d) Retentions

For each **Single Event** the **Insurer** shall only pay the amount of **Loss** exceeding the retention stated in ITEM 5 of the Schedule, except in respect of **Emergency Response Costs**, **BI Loss**, **Monitoring Costs** and costs and services under 3.6 Preventive Consulting Services. Payment of the foregoing exempted **Losses** shall not erode any applicable retention.

5.3 DURATION – COVERS LIMITED IN TIME

(a) **BI Loss** is covered only during the Indemnity Period stated in ITEM 6 of the Schedule.

(b) **Monitoring Costs** and **Emergency Response Costs** are covered only up to the period stated in the relevant Definitions.

(c) Subject always to trigger provisions under 2 - What Is Covered and 5.1 Policy Trigger and Attachment, no other **Loss** shall be limited in duration under this Policy, except as otherwise provided by endorsement.

5.4 INSURER CONSENT AND CONSULTANT COSTS

(a) Agreed Consultants

To the extent the **Legal Response Team**, **IT Response Team** or **PR Response Team** retained by the **Insured** in respect of a **Cyber Event** are those named in the Appendix 2:

(i) their instruction for such **Cyber Event** shall not be subject to the **Insurer**'s prior written consent, and

(ii) their fees and costs shall be assumed to be reasonable and necessary.

(b) Free Choice Consultants

If the **Insured** chooses to instruct a **Legal Response Team**, **IT Response Team** or **PR Response Team** that is not named in the Appendix 2:

(i) the instruction and incurring of costs of such consultant shall be subject to the **Insurer**'s prior written consent to be eligible for cover hereunder, however

(ii) in respect of **Emergency Response Costs**, the prior written consent of the Insurer shall not be required but costs must be recommended and monitored by the **Incident Coordinator**.

Please note: Prior written consent herein shall be required for each individual **Cyber Event**, even where a series of **Cyber Events** is considered a **Single Event** because they share the same originating cause or source.

6. What is Not Covered (Exclusions)

The **Insurer** shall not be liable to make any payment hereunder in respect of any portion of any **Cyber Event**, **Circumstance** or **Loss** caused or contributed to by:

6.1 KNOWN MATTERS

any **Single Event** first **Discovered** before the inception of the **Policy Period**.

6.2 DELIBERATE OR RECKLESS CONDUCT

any dishonest, fraudulent, criminal, malicious or reckless act or omission committed by or with the solicitation, inducement, knowledge, condoning or other form of support or conscious tolerance of, any person who was a **Responsible Person** of the **Insured** at the time of such act or omission.

For the purposes of this Exclusion, the conduct of an **Insured** shall not be imputed to any other **Insured**, save for that of the **Responsible Persons** of the **Policyholder**, which shall be imputed to all **Insureds**.

This Exclusion shall not apply to **Defence Costs** unless such wrongdoing is established by final adjudication or written admission of the **Insured**.

SAMPLE

6.3 BETTERMENT

any enhancement or upgrade of the **Insured's Systems** to a level beyond the state existing immediately prior to the **Cyber Event**, except any **Bricking Costs** or **Betterment Costs** if covered hereunder**.**

6.4 UNDERSIZED SECURITY EXCLUSION

any failure to:

(a) update the **Insured's Systems** security within the Time Limit indicated in the "Remediation Timeframes" in ITEM 13 of the Schedule, in respect of any Identified Vulnerability in the **Insured's Systems**.

(b) proceed with at least one weekly full backup and one daily incremental backup of all **Insured's Systems** databases.

For the purposes of this Exclusion 'Identified Vulnerability' means any vulnerability that:

(i) is officially published and documented in the Common Vulnerabilities and Exposures (CVE) system with an associated fix, mitigation technique or official patch available to the **Insured**, and

(ii) is scored using the Common Vulnerability Scoring System (CVSS).

6.5 INFRASTRUCTURE FAILURE

any electrical, mechanical, software telecommunications, satellite or internet failure and/or interruption, including but not limited to surge, current, voltage or energy spike, brownout or blackout, outages to gas, water, telephone, cable or telecommunications, except:

(a) in respect of Extension 3.4 Contingent BI Loss (if applicable), to the extent that such failure originates directly from covered **Outsourced Systems**, or

(b) in respect of Extension 3.5 Accidental Event BI Loss (if applicable), to the extent that such failure originates directly from the power supply owned and operated only by the **Insured**.

6.6 ASSUMED LIABILITY

any liability contractually assumed by the **Insured**, whether directly or by waiver or limitation of rights against third parties, that exceeds the ultimate liability (taking into account recourse actions) that would attach in the absence of such contractual assumption, except to the extent of covered **PCI Penalties**.

6.7 INSOLVENCY

the insolvency, bankruptcy, liquidation, administration or receivership of an **Insured** or any **Service Provider** operating and administering **Outsourced Systems**.

6.8 TOXIC HAZARD

the direct or indirect emission, discharge, release, scattering or presence of any:

(a) solid, liquid or gaseous substance, waste, particle or matter, whether organic, mineral or other, or

(b) odour, noise, vibrations, temperature variation or turbulence, waves or radiations of any kind,

contaminating or otherwise affecting air quality, the atmosphere, water quality, soils or subsoils, fauna, flora, human health or exceeding applicable statutory limits.

6.9 INADEQUATE GOODS OR SERVICES OR UNDUE REMUNERATION

(a) any **Claim** alleging an act, error or omission in the provision of or failure to provide professional services or advice by or on behalf of the Insured, except to the extent such act, error or omission was contributed to by a covered **Data Breach**,

(b) any **Claim** arising out of the misrepresentation of the quality, qualities or performance of goods or services supplied by the **Insured**, or out of the defective performance, failure to provide or supply or unfitness for purpose of such goods or services, including any **Claim** arising out of a product recall, whether based on an actual or suspected defect in the said products or otherwise, or

(c) any **Claim** in respect of the fees, commissions or other compensation of the **Insured** for the actual, alleged or required provision of services or supply of goods by the **Insured**.

SAMPLE

6.10 DATA PROTECTION COMPLIANCE GAPS

any measures actually or allegedly required to ensure compliance with mandatory rules applying to the collection, storage, processing or protection of **Protected Data**, except to the extent covered under **Notification Costs** or **Monitoring Costs**.

6.11 BODILY INJURY AND PHYSICAL DAMAGE

(a) any **Claim** for bodily injury or emotional distress, except to the extent of emotional distress arising from a covered **Data Breach** or alleged in a covered **Electronic Media Claim**, or

(b) any physical damage to or loss of destruction of any property, except to the extent of any covered **Recovery Costs**, **Bricking Costs** or **Betterment Costs**.

6.12 GOVERNMENT OR REGULATOR ACTION

any act, notice or order of any government or regulatory body or agency disrupting the operation of or access to the **Insured's Systems** or **Outsourced Systems**, provided that this Exclusion shall not apply to:

(a) **Cyber Attacks** committed by any such body or agency against the **Insured's Systems**, or

(b) any **Insured's Systems Disruption** as per point (c) of the Definition of that term.

6.13 WAR AND TERRORISM

any actual, threatened or feared:

(a) act of war, invasion, act of foreign enemy, hostile operations between sovereign states, whether fully or partially recognized and whether war has been declared or not, civil war, rebellion, revolution, insurrection, riot or civil commotion, military or usurped power or martial law, or any other

(b) violence or other intended harm to human life or health or to property by an individual or group(s) of individuals, whether acting alone or on behalf of or in connection with any organization(s) or government(s), for political, religious or other ideological reason and for the purposes of intimidating, coercing or harming, in part or in whole, any government, population or segment of economy, except to the extent exclusively carried out through an actual **Cyber Attack**, or

(c) use by or for a sovereign state of any computer systems (including hardware and software and electronic data relating to systems configuration or parameters) to disrupt, deny, degrade, manipulate or destroy information in a computer system of or located in another sovereign state, effectively causing directly or indirectly a detrimental impact in the functioning of a Critical National Infrastructure of any sovereign state (according to such state's definition of Critical National Infrastructure, or its equivalent), regardless of whether this is committed in the course of events described in (a) or (b) above.

A detrimental impact on a Critical National Infrastructure shall be deemed ascertained when such impact has been made public whether in the media, official statements or otherwise.

This exclusion 6.13(c) shall only apply to the extent that the **Insurer** can establish the attribution of such act to a sovereign state on the balance of probabilities within 3 months of **Reporting** of the **Cyber Event**, by relying on attribution made, if any, and/or the opinion of:

(i) the sovereign state victim of such operation or the sovereign state where computer systems have been so impacted; and/or

(ii) any official Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT); and/or

(iii) the European Network and Information Security Agency (ENISA) or the US Cybersecurity and Infrastructure Security Agency (CISA); and/or

(iv) IBM, Microsoft, McAfee or any other company with similar, prominent IT security expertise and international repute; and/or

(v) the **IT Response Team** or, if requested by the **Insured** or the **Insurer**, any independent IT expert appointed jointly by the **Insured** and the **Insurer** (in which case the time necessary for such appointment shall suspend the abovementioned 3 month-period); and/or

SAMPLE

(vi) in case evidence under (i) to (v) is unavailable in that timeline, any other evidence as is available.

6.14 RELATED PARTIES

any **Claim** against an **Insured** brought by or on behalf of:

(a) any other **Insured**,

(b) any shareholder of an **Insured Entity** in their capacity as such,

(c) any entity in respect of which an **Insured** holds more than 25% of the voting rights (if applicable) or a managerial interest, or

(d) any parent company of the **Policyholder** or subsidiary thereof.

6.15 PATENTS

any actual or alleged breach of patent rights.

6.16 SECURITIES CLAIMS

any **Claim** alleging a violation of any laws (statutory or common), rules or regulations regulating securities of an **Insured Entity**, the purchase or sale or offer or solicitation of any offer to purchase or sell securities of an **Insured Entity**, or any registration relating to such securities.

6.17 CHARGEBACKS

any chargeback request made to the **Insured** by, on behalf or at the instigation of a credit, debit or other card provider.

6.18 LOANS AND TRADING

(a) any actual or alleged failure by the **Insured** or any debtor of the **Insured** to pay or reimburse any loan, loan instalment or similar agreement or operation.

(b) any trading losses or liabilities incurred by the business of any **Insured Entity**, including but not limited to loss of client account and/or custom

7. Reporting and Handling of Incidents and Claims

7.1 NOTICE

The **Insurer** shall only be liable in respect of **Cyber Events**, **Circumstances** or **Claims** and **Investigations** that have been notified in compliance with the following:

(a) How and When to Report

(i) Upon **Discovery** of an actual or suspected **Cyber Event** or **Circumstance**, or of a **Claim** or **Investigation**, the **Insured** shall:

(1) contact the **Incident Coordinator** through the Hotline stated in ITEM 7 of the Schedule, then

(2) other than for **Emergency Response Costs**, substantiate the following in writing using the Email address stated in ITEM 7 of the Schedule:

a. any actual, suspected or potential incident, dates, persons or entities involved or affected including potential claimants or data subjects, and the underlying alleged or suspected wrongdoings,

b. the actual or anticipated consequences, including claims and losses, of the actual or suspected **Cyber Event**, **Claim** or **Investigation**,

c. in respect of **Circumstances** only, the reason to anticipate a **Cyber Event**, and

d. any report issued by the **IT Response Team** under 3.6 Preventive Consulting Services.

(ii) Such full notice shall be given as soon as practicable within the **Policy Period** or, where this has not been reasonably possible, no later than thirty (30) days after the end of the **Policy Period**.

SAMPLE

(b) Notice of Single Events

If a **Circumstance** or **Cyber Event** has been **Reported** pursuant to (a) above, then any subsequent **Circumstance**, **Cyber Event**, **Claim** or **Investigation** which are part of the same **Single Event** as such reported **Circumstance** or **Cyber Event** shall be considered **Reported** during the **Policy Period**, provided that each of them has been individually reported as soon as practicable in accordance with the provisions of 7.1(a) above.

7.2 INCIDENT MANAGEMENT

Upon contact through the Hotline, the **Incident Coordinator** will liaise with the **Insured** and coordinate incident management in respect of any actual or suspected **Cyber Event** to optimise the response, minimise or mitigate **Loss** and facilitate **Loss** settlement.

In particular, the **Incident Coordinator** shall:

(a) recommend or approve the necessary **Emergency Response Costs**,

(b) in respect of **Event Management Costs**:

(i) be entitled to give prior written consent on behalf of the **Insurer** in respect of the appointment of a **Legal Response Team**, **IT Response Team**, or **PR Response Team** other than those named in the Appendix 2;

(ii) recommend or approve the necessary **PR Costs**,

(c) recommend or approve the necessary **E-threat Response Costs**,

(d) coordinate the action of all specialists involved, whether pre-agreed before the inception of this Policy or appointed post-incident with the **Insurer**'s prior written consent;

(e) swiftly refer to the **Insurer** any request for prior written consent in respect of **Monitoring Costs**, **Defence Costs**, settlement agreements to end a **Claim**, **Investigation Costs** and **Betterment Costs** (where applicable), and will communicate the **Insurer**'s answer to the **Insured**, and

(f) guide (but not advise) the **Insured** through the **Reporting** process and provide the **Insured** with a **BI Loss** valuation (at the **Insurer**'s expenses) according to the method stipulated in 7.3 BI Loss Valuation.

Please note – it is agreed and understood that:

(1) the **Incident Coordinator** shall act according to the terms and conditions of the Policy but is not entitled to advise the **Insured** on cover hereunder. Except in respect of the approval of **Emergency Response Costs** or **PR Costs** incurred as part of **Event Management Costs**, the **Insurer** shall not be bound by recommendations made or actions taken by the **Incident Coordinator**,

(2) the **IT Response Team** and **PR Response Team** are always deemed appointed by or on behalf of the **Insured** only, even where the **Incident Coordinator** may facilitate or coordinate instructions to those specialists, while the **Legal Response Team** shall be deemed jointly retained by the **Insurer** and the **Insured**.

7.3 BI LOSS VALUATION

BI Loss shall be calculated following adjustment as the sum of:

- the Loss of Net Profit (see (a) below),
- the Increased Costs of Working (see (b) below) and
- the Additional Increased Costs of Working (see (c) below),

incurred by the **Insured Entity** during the Indemnity Period stated in ITEM 6 of the Schedule directly and exclusively as a result of an **Insured's Systems Disruption** or, if covered, an **Outsourced Systems Disruption** (hereinafter, a "Systems Disruption").

(a) Loss of Net Profit

Loss of Net Profit shall be the reduction in the net profits which the **Insured Entity** would have earned in the absence of a Systems Disruption, calculated:

SAMPLE

(i) by reference to the accounting principles applied by the **Insured Entity** and declared to the **Insurer** at placement, failing which they shall comprise net profits before payment of income taxes, applying commonly accepted accounting principles;

(ii) taking into account:

(1) the **Insured Entity**'s revenues generated and costs incurred during each of the 12 months preceding the Systems Disruption as shown in the **Insured Entity**'s accounts,

(2) any factors, whether specific to the **Insured Entity**'s business or otherwise, which would have reduced the net profits during the Indemnity Period in the absence of the Systems Disruption, and

(3) any contractual reductions suffered or contractual credits given by the **Insured Entity** to reflect reduced service by the **Insured Entity** to relevant **Third Parties**, with the exception of:

a. any contractual penalties that bear no reasonable relationship to the **Third Party**'s actual loss,

b. the cost of meeting any claim by a **Third Party** for damages,

c. any actual or alleged lost business opportunities or reputational damage,

d. the costs of removing errors, weaknesses or vulnerabilities from, or the costs of any enhancement or upgrade of, the **Insured's Systems** or **Outsourced Systems**, or

e. any statutory or regulatory fines or penalties.

(iii) deducting the amount of:

(1) any recoveries from liable parties in respect of the Systems Disruption and its consequences,

(2) any savings which the **Insured Entity** is or should be able to make in fixed or variable costs, including taxes, as a result of or following the Systems Disruption,

(3) any benefit gained by the **Insured Entity** from the wider impact on the business of competitors of systems disruptions of a similar sort, and

(4) any discount to reflect any underinsurance of the **Insured Entity**'s anticipated net profits, as declared at placement.

(b) Increased Costs of Working

Increased Costs of Working are any external costs and expenses incurred by the **Insured Entity** in the realistic and reasonable expectation of thereby reducing any Loss of Net Profit that would otherwise be covered hereunder, of an amount at least equal to such costs and expenses, whether or not that result is actually achieved.

Increased Cost of Working shall not include:

(i) the fees of any forensic IT professionals,

(ii) any **Betterment Costs** or the costs of any enhancement or upgrade of the **Insured's Systems** or **Outsourced Systems**, or

(iii) any professional legal costs.

(c) Additional Increased Costs of Working

Additional Increased Costs of Working are those additional operating expenses, including overtime salaries, taxes, interest and rents, that are necessarily incurred to enable the **Insured Entity** to continue trading following a Systems Disruption with the minimum practicable insured Loss of Net Profit.

Additional increased Cost of Working shall not include bonuses, salaries paid to employees or officers for their regular, contracted hours, the fees of any forensic IT professionals nor any **Betterment Costs** if covered.

SAMPLE

(d) Expert Resolution

If the **Insured** and the **Insurer** do not agree on the valuation of **BI Loss** valuation made by the **Incident Coordinator**, such valuation shall be determined in accordance with the calculation method set out above by an independent loss adjuster mutually agreed by them, acting as an expert and not an arbitrator.

The costs of such expert determination shall be borne equally by the **Insured** and the **Insurer**.

7.4 ALLOCATION

(a) Mutual Agreement

The **Insurer** shall pay only those amounts or portions of **Loss** relating to matters, persons and/or entities covered hereunder. If any **Cyber Event** involves both covered and non-covered matters, matters, persons and/or entities, the **Insured** and the **Insurer** shall use their best efforts to determine a fair and proper allocation of the **Loss** covered hereunder.

(b) Expert Resolution

If an allocation cannot be agreed as per A. above, it shall be determined by a legal counsel mutually agreed by the **Insured** and **Insurer** acting as an expert and not an arbitrator. The expert determination shall be based upon the written submissions of the parties with the support, as necessary, of mutually agreed information technology experts. There shall be no obligation on such counsel to provide reasons unless specifically requested by either party.

The costs of such expert determination shall be borne equally by the **Insured** and the **Insurer**.

7.5 SUBROGATION AND RECOVERIES

(a) The **Insurer** shall be subrogated to all of the rights of recovery of the **Insured** to the extent of all **Loss** payments. The **Insured** shall do nothing to prejudice such rights of recovery, shall provide to the **Insurer** all information, assistance and cooperation, and shall do everything necessary to secure any rights, including the execution of any documents necessary to enable the **Insurer** effectively to bring suit in the name of the **Insured** whether such acts become necessary before or after payment by the **Insurer**.

(b) To the fullest extent permitted by law, any recoveries, whether effected by the **Insurer** or the **Insured**, following the payment of **Loss** hereunder and after deducting the actual cost of obtaining such recovery but excluding the own labour or establishment costs of the **Insured**, will be allocated in the following order:

(i) initially, to reimburse the **Insured** for any **Loss** which exceed the amount of **Loss** paid under this Policy (disregarding the amount of any retention applicable),

(ii) subsequently, to reimburse the **Insurer** for any payment made for such **Loss**, and

(iii) finally, to reimburse the **Insured** for such **Loss** sustained by the **Insured** by reason of any applicable retention.

7.6 SETTLEMENT OPPORTUNITIES

If:

(a) the **Insurer**, a claimant or a regulatory body recommends the settlement of a **Claim** or **Investigation** within the Policy's applicable Limit of Liability which is acceptable to both the **Insurer** and the claimant or regulator (a "Settlement Opportunity"), and

(b) the **Insured** consents to such a settlement within (i) thirty (30) days of the date the **Insured** was first made aware of the Settlement Opportunity, or (ii) the time-limit set by the claimant or regulator for acceptance, whichever is shorter,

then the **Insured**'s applicable retention amount shall be retroactively reduced by 10%. If the **Insured** refuses the Settlement Opportunity or consents to it outside the foregoing timeframe, the retention amount shall remain that indicated in the Schedule even if consent is given by the **Insured** to a subsequent settlement.

7.7 FRAUDULENT CLAIMS

If the **Insured** reports any **Cyber Event** or **Circumstance** hereunder knowing it to be, in part or in whole, part false or fraudulent as regards amounts or otherwise, then all deriving **Loss** (including the **Loss** arising from **Cyber Events** or **Circumstances** having the same originating cause) shall be

SAMPLE

excluded from cover and any portion of such **Loss** already paid by the **Insurer** shall be immediately refundable by the **Insured** or **Policyholder**.

8. General Conditions

8.1 CHANGE IN CONTROL | AUTO RUN-OFF

In case of a **Change in Control** during the **Policy Period**,

(a) the **Policyholder** shall give the **Insurer** written notice thereof as soon as practicable, and

(b) cover hereunder will continue until the end of the **Policy Period** but solely with respect to any **Cyber Events** actually or alleged, deemed or suggested to have arisen before the effective date of such **Change in Control**.

8.2 REPRESENTATIONS AND SEVERABILITY

Knowledge of an **Insured** shall not be imputed to nor affect entitlement to cover of any other **Insured**, save for that of **Responsible Persons** of the **Policyholder**, which shall be imputed to all **Insureds**.

8.3 MATERIAL CHANGE IN RISK

The **Insured** shall promptly notify the **Insurer** of any change that increases the risks stipulated in the policy and that results from events within his control or knowledge. On being notified of any material change in the risk, the **Insurer** may cancel the contract, propose, in writing, changes in the terms and conditions or propose an additional premium. Unless the new terms or conditions are accepted and the new premium paid by the **Insured** within thirty days of the proposal, the policy ceases to be in force.

Notwithstanding the above general obligation, the **Insured** shall notify in particular the following events to the **Insurer** as material changes in the risk:

(a) Change in the system update policy (patching)

(b) Change in the back-up policy

(c) Changes to critical systems safety policy

(d) Changes and/or migration of critical systems

8.4 PREMIUM PAYMENT

The **Insurer** may cancel from inception any coverage under this Policy for non-payment of premium within thirty (30) days from the Inception Date stated in ITEM 3(a) of the Schedule, by sending no less than five (5) days' written notice (including by Email) to the **Policyholder** at the registered address stated in ITEM 2 of the Schedule or via the insurance broker.

8.5 NOTICES AND AUTHORITY

The **Policyholder** shall act on behalf of all **Insureds** with respect to the giving and receiving of any notice required under this Policy, the payment of all premiums, the allocation of **Loss**, the request for services under 3.6 Preventive Consulting Services, the declaration of risk and execution of this Policy and any amendments thereto.

8.6 INTERPRETATION

(a) Any reference in this Policy to:

(i) the singular shall include the plural and vice versa; and

(ii) the masculine shall include the feminine and vice versa; and

(iii) a position or title or legal status of an individual shall include the equivalent position in any other relevant jurisdiction.

(b) Policy headings and titles are for reference only and shall have no interpretational value.

8.7 APPLICABLE LAW AND JURISDICTION

This Policy is to be governed by, and its terms are to be construed in accordance with the applicable law stated in ITEM 9 of the Schedule. Any dispute or difference arising under or in respect of this Policy is to be subject to and determined within the exclusive jurisdiction of the laws of the country stated in ITEM 10 of the Schedule.

SAMPLE

8.8 ENTIRE AGREEMENT

By acceptance of this Policy, the **Insured** and the **Insurer** agree that this Policy (including the Proposal and any materials submitted therewith) and any written endorsements attached hereto constitute the sole and entire agreement between the parties with respect to this insurance. Any prior agreement or understanding between the parties is therefore no longer valid.

8.9 ASSIGNMENT

This Policy shall not be assigned without the prior written consent of the **Insurer**, and any other purported assignment shall be null and void.

8.10 OTHER INSURANCE OR INDEMNIFICATION

Unless otherwise required by law, this Policy shall always apply in excess of any other valid and collectible insurance or indemnification available to the **Insured**, except in respect of any **Emergency Response Costs**.

8.11 TERRITORY

To the extent permitted by law, this Policy applies to **Cyber Events** actually or allegedly taking place and to **Claims** made anywhere in the world as indicated in ITEM 8 of the Schedule.

8.12 THIRD PARTIES RIGHTS

Nothing in this Policy is intended to confer any directly enforceable benefit on any third party other than an **Insured**, whether pursuant to the Contracts (Rights of Third Parties) Act 1999 of England and Wales, any equivalent or similar legislation, regulations or rules in any other jurisdiction or otherwise

8.13 TRADE SANCTIONS

This Policy does not apply to the extent any applicable trade or economic sanctions, or other laws or regulations prohibit the **Insurer** from providing insurance, including, but not limited, to the payment of **Loss**.

SAMPLE

APPENDIX 1 – Cyber Menu

SAMPLE

APPENDIX 2 – Incident Coordinator and Expert Panel

SAMPLE

TOKIO MARINE HCC

Why Tokio Marine HCC

Tokio Marine HCC is a leading specialty insurance group conducting business in approximately 180 countries and underwriting more than 100 classes of specialty insurance. Headquartered in Houston, Texas, the company is comprised of highly entrepreneurial teams equipped to underwrite special situations, companies and individuals, acting independently to deliver effective solutions. Our products and capabilities set the standard for the industry, as many of our approximately 3,600* employees are industry-leading experts.

Tokio Marine HCC's major domestic insurance companies have financial strength ratings of "A+ (Strong)" from Standard & Poor's Financial Services LLC, "A++ (Superior)" from A.M. Best Company, Inc., and "AA- (Very Strong)" from Fitch Ratings; its major international insurance companies have financial strength ratings of "A+ (Strong)" from Standard & Poor's Financial Services LLC.**

Tokio Marine HCC is part of Tokio Marine, a premier global company with a market cap of approximately $36 billion.***

* Employees as of 31/12/2021
** At the time of printing
*** Market Cap as of 30/09/2022