LLOYD'S Underwriters

TOKIO MARINE HCC

Cyber Extension Questionnaire

1. **Name:**

2. **Please estimate the total number of Personally Identifiable Information * records, including employees and customers, that your company holds:**

* Personally Identifiable Information relates to records/data 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.

3. **Please estimate what proportion of the total number of Personally Identifiable Information records which you hold that include a High Sensitivity element (e.g. banking or saving account number, debit card number, credit card number, health information, passport number).** %

4. **How fast are you likely to incur a loss of profit as a result of an IT network compromise and a total system downtime?**

Level 1:	Level 2:	Level 3:	Level 4:	Level 5:
48hours+ ☐	24 – 48 hours ☐	12-24 hours ☐	1-12 hours ☐	Immediately ☐

5. **In the event of your IT network being subjected to a non-scheduled closure and total downtime, please estimate your maximum daily loss of profit (net profit before tax):** $

6. **Do you have a disaster recovery plan which protects you against any sudden or unexpected failure of your IT network and security breach/data compromise?** ☐ Yes ☐ No

If **NO**, please advise how you would deal with such an event in a time critical manner:

If **YES**, please advise:

a. Is the backup system managed by a third party? ☐ Yes ☐ No

b. How regularly is it tested?

c. When was it last tested?

d. How long did it take to switch to this back up system?

7. Can you confirm that:

a.	You adhere to and comply with the following data security law where relevant: the federal Personal Information Protection and Electronic Documents Act (PIPEDA) and similar provincial Acts and regulation, and in the United States, "non-public personal information" as defined in the Gramm-Leach Bliley Act of 1999, or as amended; Payment Card Industry (PCI) Data Security Standards.	☐ Yes	☐ No
b.	If the data held is medically related, you comply with the 'protected health' information as defined in the provincial legislation in Canada, or, in the United States, the Health Insurance Portability and Accountability Act of 1996, as amended.	☐ Yes	☐ No
c.	You ensure that all Personally Identifiable Information records are backed up daily and held at a secondary location.	☐ Yes	☐ No
d.	all computer equipment & mobile devices including laptops & tablets have appropriate firewalls, anti-virus, anti-spyware, security, password protection and are regularly updated/patched	☐ Yes	☐ No
e.	You use encryption tools to ensure the integrity and confidentiality of all Personally Identifiable Information records including those on removable media.	☐ Yes	☐ No
f.	You have never experienced an event that did or may have given rise to a claim or circumstance under a cyber and data security policy, including but not limited to hacking incident, virus or malicious code attack, cyber extortion attempt, breach of secure data, wrongful disclosure of personal data or interference with rights of privacy?	☐ Yes	☐ No

If **NO**, to any of the above, please provide an explanation below.

Declaration

On behalf of the Applicant/s, I/we declare that, after full enquiry, the contents of this application are true and that I/we have not misstated, omitted or suppressed any material fact or information. If there is any material alteration to the facts and information which I/we have provided or any new material matter arises before the completion of the contract of insurance, I/we undertake to inform the Insurer.

Signature of Principal / Director / Partner:

Date: