

MMarsh

Marsh Corporate Cyber Panel Application (MCCP)

1. Insurance requirements (See Appendix I for a description of available coverages):

Please specify which of the following coverage modules you wish to be included within any quotations as part of the MCCP:

|  |  |  |
| --- | --- | --- |
| Cover Item | Yes | No |
| Privacy & Network Liability |  |  |
| PCI Assessments, Fines and Penalties |  |  |
| Privacy Breach Crisis Costs/Expenses |  |  |
| Network Business Interruption |  |  |
| Contingent Network Business Interruption |  |  |
| Digital Asset Replacement |  |  |
| Cyber Extortion |  |  |
| Media Liability (claims made basis only) |  |  |
| Cyber Crime, i.e. Social Engineering  (may be sub limited and not offered by all participants) |  |  |

Please specify all limit options for which you would like to receive quotations:

|  |  |
| --- | --- |
| $1,000,000 |  |
| $2,000,000 |  |
| $5,000,000 |  |
| $10,000,000 |  |
| $20,000,000 |  |
| Other please specify:Click here to enter text. |  |

Please specify the desired retention level:

|  |  |
| --- | --- |
| $25,000 |  |
| $50,000 |  |
| $100,000 |  |
| $250,000 |  |
| $500,000 |  |
| $1,000,000 |  |
| Other please specify:Click here to enter text. |  |

1. Applicant Profile:

|  |  |  |  |
| --- | --- | --- | --- |
| Name: | Click here to enter text. | | |
| Address: | Click here to enter text. | | |
| Website URLs: | Click here to enter text. | Telephone: | Click here to enter text. |
| Business Description: | Click here to enter text. | | |

1. Gross revenue:

|  | Previous Financial Year | Current Financial Year (est) |
| --- | --- | --- |
| Canada | $ Click here to enter text. | $Click here to enter text. |
| USA | $ Click here to enter text. | $ Click here to enter text. |
| EU | $ Click here to enter text. | $ Click here to enter text. |
| Rest of world | $ Click here to enter text. | $ Click here to enter text. |
| **Total** | **$**Click here to enter text. | $Click here to enter text. |

1. Corporate changes

If the answer is yes to either a merger or acquisition, please detail what cyber due diligence has, or will be performed, as well as, plans to integrate the information security and privacy policies:

|  |  |  |
| --- | --- | --- |
| Have there been any mergers, acquisitions, divestitures in the last 12 months? | YES | NO |
| If yes, please specify  Click here to enter text. |  |  |
| Are there any mergers, acquisitions, divestitures planned in the next 12 months? | YES | NO |
| If yes, please specify  Click here to enter text. |  |  |

1. Use of Computer Systems:
2. What functions are your computer systems generally used for:

|  |  |  |
| --- | --- | --- |
| Item | Yes | No |
| Corporate/Administrative Activities (e.g. Human Resources, Finance, Legal, etc) |  |  |
| Manufacturing/Industrial Activities (e.g. use of operational technology or industrial control systems –SCADA, PLC’s, DCS, etc.) |  |  |
| Online Payment Processing (e.g. acceptance of debit/credit cards,.etc.) |  |  |
| In-store payment collection (e.g. point of sale systems, etc) |  |  |
| Collection, storage or processing of sensitive customer information (e.g. customer facing websites, etc.) |  |  |
| Other: |  |  |

If computer systems are used for any functions not listed above please explain:

|  |
| --- |
| Click here to enter text. |

1. Confidential Data and Privacy:

Please provide a breakdown of the approximate total number of stored and transmitted/processed records in accordance with the following categories. The numbers provided should represent the number of unique individuals you store a certain type of data on. **(Why is this question important? - See Appendix II)**

We understand that certain data sets and/or individual records are likely to fall within more than one of these categories. Please include all categories that apply.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Type | Maintained by Proposer | Maintained by a Third Party on the Proposer’s Behalf | Estimated Number of Unique Individuals for which you have stored information on | |
| External Parties (Customers, vendors, etc.) | | | | |
| Health related |  |  | 0 – 100K  100K – 250K  250K – 500K | 500K – 1M  1M – 5M  Over 5M |
| Payment card data credit/debit |  |  | 0 – 100K  100K – 250K  250K – 500K | 500K – 1M  1M – 5M  Over 5M |
| Financial account information (other than credit card data) |  |  | 0 – 100K  100K – 250K  250K – 500K | 500K – 1M  1M – 5M  Over 5M |
| Government issued ID such as passport number, social insurance numbers, health cards, driver’s licence etc. |  |  | 0 – 100K  100K – 250K  250K – 500K | 500K – 1M  1M – 5M  Over 5M |
| Sensitive personal information (other than as specified above), such as ethnic origin, trade union membership, religious beliefs, political opinions, sex life, genetic data or criminal convictions |  |  | 0 – 100K  100K – 250K  250K – 500K | 500K – 1M  1M – 5M  Over 5M |
| Other |  |  | N/A | N/A |
| Internal Parties (Employees) | | | | |
| Employee records including previous employees where this data is retained |  |  | 0 – 100K  100K – 250K  250K – 500K | 500K – 1M  1M – 5M  Over 5M |

If possible, and with reasonable approximation, please state the total number of personal (confidential) information records you believe are stored, maintained, or transmitted / processed by you (noting that this number may be lower than the aggregate of all items stated above as a single record may fall within multiple categories). **(Why is this question important? - See Appendix II)**

|  |  |  |  |
| --- | --- | --- | --- |
| Data Type | Maintained by Proposer | Maintained by a Third Party on the Proposer’s Behalf | Estimated Number of Unique Individuals for which you have stored information on |
| Any type of personally identifiable information |  |  | Click here to enter text. |

Is the applicant in possession of **third party** Intellectual Property or Trade Secrets? YES/NO

Does a senior executive have formal enterprise-wide responsibility for Privacy? /NO

Please list the relevant position(s) that has corporate-wide responsibility for Privacy and ensuring compliance with privacy legislation?

|  |
| --- |
| Click here to enter text. |

Do you have a corporate-wide privacy policy? YES/NO Please provide a copy (or at least an outline of the plan – ToC, overview, etc).

Is it customary or within normal operating procedure to share confidential data with third-party organizations? YES/NO

If yes, is this clearly stated in the privacy policy applicable to these data subjects: YES/NO

Do you sell personal information or have you agreed to share personal information any third parties? (please specify which – sell or share):

|  |  |
| --- | --- |
| Nature of personal data | Sold or shared |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

*If there is insufficient space, then please list in a separate document and attach to this application.*

Are all third-party organizations with which you share personal data, required to indemnify you under contract for their unauthorized disclosure or loss of such personal data? YES/NO

If no then please specify what contractual remedies exist:

|  |
| --- |
| Click here to enter text. |

1. Third-Party Dependencies: (Why is this important? - See Appendix II)

Please provide an approximation of the total number of vendors that provide **information technology functions** and provide a list of the vendors that provide your **CRITICAL information technology functions** (this may include, but is not limited to, data centre services, application hosting, data storage, network management, managed security, offsite backup and storage, payment processing).

For Cloud Service providers, please indicate the type of service, e.g. SaaS, IaaS, PaaS. and if you will be in a public, private or hybrid environment.

|  |  |
| --- | --- |
| Service | Item description | Name of vendor |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

*If there is insufficient space, then please list in a separate document and attach to this application.*

Please provide details of **business process (BPO) functions** that have been outsourced to a third-party (this may include HR/payroll, order processing, contact centre services, finance and accounting).

|  |  |
| --- | --- |
| Service | Item description | Name of vendor |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. |

*If there is insufficient space, then please list in a separate document and attach to this application.*

Do you verify that outsource providers and organizations with which you share personal information are able to meet the same or better security standards for your organization? YES/NO

Please state the method of verification:

|  |
| --- |
| Click here to enter text. |

As a business practice, do you generally require indemnification from your service providers in the event they suffer a breach involving confidential information you have entrusted to them? YES/NO

Service providers and insurance requirements:

Do you require your service providers to provide you with evidence of cyber insurance? YES/NO

Do you require your service providers to provide you with evidence of technology professional liability/errors and omissions insurance? YES/NO

1. Network Security:
2. Does a senior executive have formal enterprise-wide responsibility for Information Security? YES/NO

Please list the relevant position(s) that has corporate-wide responsibility for Information Security?

|  |
| --- |
| Click here to enter text. |

1. Number of staff dedicated to IT/IS? Click here to enter text.
2. Do you have a corporate-wide information security policy? YES/NO
3. Is the security policy monitored, and if so, is the Board or any Risk Committee reporting to the board, appraised of any critical cyber risks deemed material to the organization?
4. Do you track and monitor access to sensitive information on your network? YES/NO
5. Do you use anti-virus software that is updated/patched in accordance with the vendor’s recommendations?

|  |  |  |  |
| --- | --- | --- | --- |
| Automatic | Weekly | Monthly | Other Click here to enter text. |

1. Have you installed and do you maintain a firewall configuration to protect data? YES/NO
2. Have you installed and do you maintain an intrusion detection system? YES/NO
3. Log Management:

Are established log policies and procedures in place? YES/NO

How often are the logs reviewed? (e.g. daily, weekly, monthly, ad hoc etc.)

Click here to enter text.

1. Does your organization utilize an internal or external Security Operations Centre (“SOC”) that is responsible for event monitoring and detection, threat monitoring, vulnerability management, incident response, and reporting and tracking? INTERNAL/ EXTERNAL(Outsourced to a Third Party)/NO
2. Do you have a defined process implemented to regularly patch your systems and applications, based on criticality?   
   YES/NO

Please describe your patch management process

|  |
| --- |
| Click here to enter text. |

1. Is all sensitive and confidential information encrypted when:

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Yes | No | Partial (please explain) |
| stored on your databases and servers |  |  | Click here to enter text. |
| on back-up tapes/cassettes/disks |  |  | Click here to enter text. |
| on internal or external email transmissions |  |  | Click here to enter text. |
| when in transit from the network |  |  | Click here to enter text. |
| on wireless networks |  |  | Click here to enter text. |
| in file transfers |  |  | Click here to enter text. |
| stored on personal mobile devices |  |  | Click here to enter text. |
| stored on portable media |  |  | Click here to enter text. |

1. Please identify any security or compensating controls used in addition to or as an alternative to encryption for the transmission or storage of sensitive and confidential information.

An example would be wiping of mobile devices when reported lost or stolen.

|  |
| --- |
| Click here to enter text. |

1. How often do you (or a 3rd party vendor) perform penetration testing on your network? (e.g. monthly, quarterly, annually, etc.)

Click here to enter text.

1. How often do you (or a 3rd party vendor) run vulnerability tests on your network? (e.g. monthly, quarterly, annually, etc.)

Click here to enter text.

1. Does the Board of Directors receive either a written report or presentation on your information security status at least annually? YES/NO
2. Continuity & Backup:

Does the organization have (in the context of network interruptions, and/or privacy breaches)

an Incident Response Plan YES/NO

a Business Continuity Plan YES/NO

Please include an outline or overview (please attach to the application).

Have these plans been tested in the last 12 months? YES/NO

If not, when was the last time these plans were tested and how often do you test them?

|  |
| --- |
| Click here to enter text. |

Is critical/sensitive data backed up on a daily basis? YES/NO

Please describe where data is backed up to and any exceptions that apply to routine daily back-up.

|  |
| --- |
| Click here to enter text. |

Back-up tapes:

Is sensitive information stored on back-up tapes/cassettes/disks, etc. encrypted as a standard practice?  
YES/NO

If you maintain your own back-up tapes/cassettes/disks, etc., are these stored in a physically secured location? YES/NO

Do you have formalized data destruction procedures in place for data and documents no longer needed by your organization? YES/NO

1. Network Business Interruption loss:

Please describe the revenue pattern over a typical 12 month period

|  |
| --- |
| Click here to enter text. |

Please describe the financial impact on your revenue that would arise from the unavailability of your computer network (Corporate/Administrative Systems, Operational Technology, etc.):

For the following durations of downtime: 24 hours and 72 hours

|  |
| --- |
| Click here to enter text. |

Please advise the projected recovery time objectives (in hours) it would take you to restore operations after a cyber-event, e.g. Ddos or network breach

|  |
| --- |
| Click here to enter text. |

What percentage of your revenue is derived from customer-facing websites?

|  |
| --- |
| Click here to enter text. |

1. Regulatory & Legal:

To the best of your knowledge, are you compliant with applicable statutory or regulatory standards concerning personal data stored or processed by you? YES/NO if No, please explain below.

Click here to enter text.

Where applicable, please confirm your compliance with:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Yes | No | Not applicable | Date of last assessment |
| Payment Card Industry Data Security Standards (PCI DSS)  Indicate applicable level:  1 2 3 4  Approximate amount of transactions over the last 12 months  Click here to enter text. |  |  |  | Click here to enter text. |
| PIPEDA, and/or other similar provincial  and/or foreign privacy legislation |  |  |  | Click here to enter text. |

If the scope of PCI compliance does not include all applicable business areas, then please state the business areas that your compliance status does apply to and which business areas remain non-compliant. Please also describe the status and estimated completion date of any PCI compliance plan for non-compliant business areas

|  |
| --- |
| Click here to enter text. |

Has any third-party audit of your privacy practices been undertaken in the last two years? YES/NO

1. Employees:

Does the proposer distribute information security policies to its employees and are they required to sign off acknowledging the same at least annually? YES/NO

Do you provide awareness training for employees in data privacy and security including legal liability and social engineering issues at least annually? YES/NO

What is the frequency of training?

|  |
| --- |
| Click here to enter text. |

Is write access to USB drives disabled for employees? YES/NO

Do you have a procedure for the revocation of user accounts and the recovery of inventoried information assets following an employee’s departure from your organization? YES/NO

Does the organization’s hiring policy including background screening/investigations in relation to: criminal convictions, educational background (including designations for IS personnel), credit check’s and work history?

YES/NO

If some but not all of the above forms part of the hiring process, please advise what component(s) is/are not included.

Click here to enter text.

1. Media content (if Media Liability coverage is not being requested, please confirm N/A below):

N/A

Do you have written clearance procedures in place regarding use, licensing, and consent agreements for third-party content used by you on your website or in your promotional materials? YES/NO

Does your website feature opt in/opt out procedures when collecting individual users’ information? YES/NO

Do you or have you ever used flash cookies on your website to track visitors? YES/NO

Do you have written guidelines for your use of social media and its use by your employees? YES/NO

Has legal counsel verified that your domain names(s) and meta tags do not infringe on any third-party’s copyright or trademark? YES/NO

Do you solicit/promote your business via unsolicited email blasts? YES/NO

Do you host any user-generated content or social media networks? YES/NO

Do you have a formalised take-down procedure for comments or content placed on your website or on social media websites by third parties? YES/NO

Please provide details regarding any publishing or broadcasting you perform beyond advertising your own business (e.g. publishing of a trade journal):

|  |
| --- |
| Click here to enter text. |

1. MATERIAL INFORMATION and LOSS INFORMATION

It is your duty to disclose all material facts to insurers. A material fact is one which may influence an insurer’s judgement in its consideration of your proposal. If your proposal is a renewal, it is likely that any change in facts previously advised to insurers will be material and such changes should therefore be notified. If you are in any doubt as to whether a fact is material, please discuss with your Marsh broker.

**Failure to disclose and/or material misrepresentations** could prejudice your rights to recover in the event of a claim or enable insurers to void the policy.

Please provide details of any other information which may be material to insurers consideration of your application for insurance via an addendum.

**Lastly, please provide details of any cyber/privacy losses within the last 2 years, and a description of remediation efforts/lessons learned.**

|  |
| --- |
| Click here to enter text. |

1. DECLARATION / WARRANTY (not required if a renewal)

**Please note**: if this is your first time applying for such coverage, insurers will likely require a warranty upon the procurement of a policy.

As each insurer is particular about their own warranty language, one will be provided (if required) prior to binding coverage.

|  |
| --- |
| Signature (must be signed by an individual authorized by the Company): |

Job title:Click here to enter text.

Date: Click here to enter text.

1. Supplementary Information

Please include the ToC of the documents listed below. .

|  |  |
| --- | --- |
| Document | ToC Included |
| Privacy Policy | YES/NO |
| Privacy Breach Incident Response Plan | YES/NO |
| Disaster Recovery Plan | YES/NO |
| Business Continuity Plan | YES/NO |

Appendix I:

Available Coverage Components

*Note: The proceeding descriptions of coverage are general in nature and are designed to assist you in better understanding of the typical insuring agreements available under a stand alone cyber policy.*

*All insurance coverage is subject to the terms, conditions, and exclusions in the applicable individual policies.*

*Marsh cannot provide assurance that insurance can be obtained for any particular client or risk.*

|  |  |
| --- | --- |
| **THIRD PARTY COVERAGE OPTIONS:** | |
| NETWORK SECURITY LIABILITY | Liability to a third party as a result of:   * The theft, alteration, destruction, loss or unauthorized release of electronic data on your company’s computer system * Your network’s unwilling participation in a denial-of-service attack * Transmission of malicious code to a third-party’s computer system * The unauthorized access to or unauthorized use of your company’s computer system * The denial of an authorized user’s access to your company’s computer system |
| PRIVACY LIABILITY | Liability to a third party as a result of:   * Loss, theft or unauthorized disclosure of personally identifiable information * Loss , theft or unauthorized disclosure of third-party corporate information including third party trade secrets * A violation of any privacy regulation * Defence against regulatory actions * Amounts payable in connection with PCI-DSS Assessments *(Note: PCI-DSS Assessments coverage is optional and is generally only available for applicants that are PCI compliant)* |
| MULTIMEDIA LIABILITY | Liability arising from online content, arising from:   * Infringement of intellectual property rights * Invasion of privacy * Defamation * Negligent publication or misrepresentation |
| **FIRST PART COVERAGE OPTIONS:** | |
| CRISIS MANAGEMENT | Expenses to respond to a personal data breach event, including:   * Costs for a data breach coach * Computer forensic investigation costs * Notification costs including call center costs * Credit monitoring and identity theft protection costs * Public relations and crisis management costs |
| CYBER EXTORTION | A genuine threat to the computer network or data that leads to payment of:   * Expert fees to conduct an investigation to determine the cause of the threat and to negotiate with the hacker * Monies paid to a third party to terminate or end the threat (i.e. ransom) |
| NETWORK BUSINESS INTERRUPTION AND EXTRA EXPENSE | The interruption or suspension of computer systems that results in:   * Your loss of income * Extra expense incurred to mitigate an income loss   Resulting from:   * A network security breach or network failure. |
| DIGITAL ASSET PROTECTION | The corruption or destruction of electronic data or software that results in the following costs being incurred:   * Costs to determine whether electronic data or software can or cannot be restored, recollected or recreated * Costs to restore, recreate or recollect data or software programs |

Appendix II:

Additional Information on Application Questions - Why is this question important?

1. Confidential Data - Question F.1.:

Providing a reasonable approximation of the amount and type of confidential information the applicant is responsible for allows the applicant and insurer to get a better understanding of the overall exposure and enables both parties to better quantify the privacy exposure. In some cases we at Marsh can use our proprietary model to help applicants assess certain financial consequences associated with a privacy breach.

In this particular question we are asking for the estimated number of unique individuals for which you have stored information on *by data type*. For example, Person A may use the same credit card on four (4) separate occasions and Person B may use two (2) different credit cards on two (2) separate occasions to purchase products on your website. In this particular scenario we would consider you to have stored payment card information on two (2) unique individuals. As another example, let’s say that you collected at least two forms of government identification to confirm the identity of an individual for employment. In this particular scenario we would consider you to have stored government issued identification on one (1) unique individual.

1. Confidential Data - Question E.2.:

Similar to the response above, providing a reasonable approximation of the amount of confidential information the applicant is responsible for allows the applicant and insurer to get a better understanding of the overall exposure and enables both parties to better quantify the privacy exposure. In some cases we at Marsh can use our proprietary model to help applicants assess certain financial consequences associated with a privacy breach.

In this particular question we are asking for the estimated number of unique individuals for which you have stored information on *regardless of the data type*. For example, Person A may use the same credit card on four (4) separate occasions and Person B may use two (2) different credit cards on two (2) separate occasions to purchase products on your website. In addition, Person B may also be an employee and may have provided you with two forms of government identification to confirm their identity for employment. In this particular scenario we would consider you to have stored information on one (1) unique individual.

Continued on next page….

1. Third Party Dependencies – All Questions in Section G:

Many organizations outsource various business and information technology functions. While outsourcing generally increases productivity it can also increase the network security and privacy exposures of an organization.

With regard to network security, insurers are interested in understanding what third party vendors applicants are relying on and how interconnected they are with both their third party vendors and their clients. While outsourcing generally increases productivity it can also lead to an increase on the reliance of others for critical business functions and an increase in the applicant’s network attack surface. Insurers need to know how an interruption at any one of the applicant’s third party vendors might impact the applicant’s business and also how the same interruption might impact other insureds within their security and privacy insurance portfolios. (e.g. if a major cloud service provider had an outage and 50% of the insureds in a particular insurer’s portfolio were using this same cloud service provider how could this impact the insurer and their ability to respond and pay claims?). *In order to keep track of the dependence on third parties, insurers are increasingly requesting that applicant’s provide a detailed list of all business and information technology vendors and some will not provide coverage for security and privacy breaches that arise from a vendor that is not listed. As a result, please provide a complete list of all critical business and information technology vendors and, when possible, provide a list of all critical and non-critical business and information technology vendors.*

Witih regard to privacy, insurers are interested in understanding what third party organizations applicants are sharing confidential information with. Most security and privacy policies provide coverage for confidential information an insured is responsible for even if that information has been provided to a third party by the insured. As a result, it is important for applicants to be aware of the types of sensitive information that they share and with whom they share it with.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document is intended solely for the entity identified as the recipient herein (“you”). This document may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.

Copyright © 2017 Marsh Canada Limited. All rights reserved.