RIDGE CYBER APPLICATION – LARGE RISK

($100m - $425m Revenue)

As used throughout this application, "you" means the person signing the application, as well as the entity(ies) seeking insurance and the applicant's principals, partners, directors, risk managers, or employees that are in a supervisory role. The questions contained in this application pertain to all persons or entities seeking insurance, and not just the signatory.

Please answer all the questions on this form. Before any question is answered please carefully read the declaration at the end of the application form, which you are required to sign. Underwriters will rely on the statements that you make on this form. In this context, ANY INSURANCE COVERAGE THAT MAY BE ISSUED BASED UPON THIS FORM WILL BE VOID IF THE FORM CONTAINS FALSEHOODS, MISREPRESENTATIONS, OR OMISSIONS. PLEASE TAKE CARE IN FILLING OUT THIS FORM.

You may provide any further additional information by means of a separate attachment if necessary.

1. GENERAL INFORMATION

a. Name of Applicant(s):

b. Names of any wholly owned subsidiaries:

c. Address:

d. Date Business Established: e. Website:

f. Please explain your main business operations:

g. If you have been involved in any mergers or acquisitions within the last three years then please provide full details:

2. OPERATIONAL INFORMATION

a. Next Financial Year end: b. Currency: c. # of Employees:

	Last Year:	Current Year:	Next Year (est.):
d. Annual Gross Revenue:			
e. Net Income:			

f. What percentage of gross annual revenue/turnover is accounted for by sales or operations through your website or e-commerce platform? %

g. What is the percentage of annual number of transactions undertaken by payment card? %

h.

Percentage of last year's annual revenue generated from the following jurisdictions:	
1. Canada	%
2. USA	%
3. Other:	%

i. Approximately how many unique individuals do you**, or a third party on your behalf**, store or process the following types of sensitive information on? *Note: These do not need to be exact numbers, just reasonable approximations*

I. Payment Card Information:

II. Healthcare Information:

III. Government Information (S.I.N., driver's licence, passport, etc.):

IV. Financial Information, not including payment card information (Bank account info, etc.):

3. NETWORK INFORMATION

a. Usual daily hours of operation

b. Indicate time after which the inability for staff to access your internal computer network and systems would have a significant impact on your business:

☐ Immediately ☐ After 6 hrs ☐ After 12 hrs ☐ After 24 hrs ☐ After 48 hrs ☐ Never

c. Indicate time after which the inability for customers to access your networks would have a significant impact on your business:

☐ Immediately ☐ After 6 hrs ☐ After 12 hrs ☐ After 24 hrs ☐ After 48 hrs ☐ Never

d. Provide brief details below of the impact on your business if your internal network or applications should fail or be disrupted (include commercial relations, revenues, and brand impact):

4. BUSINESS CONTINUITY

a. Do you have a business continuity plan in force to avoid business interruption due to systems failure? Yes: ☐ No: ☐
If 'No', please provide details in the 'Additional Notes' section of this Application regarding the current process in place for responding to and mitigating a potential interruption of your systems?

b. Briefly describe your recovery/continuity plans to mitigate or avoid business interruption due to network failure, which may include outsourcing, additional employment, system redundancy etc.

c. Has an incident response plan been implemented and tested for a ransomware incident? Yes: ☐ No: ☐

d. How often is this plan tested and updated?

☐ Monthly ☐ Quarterly ☐ Annually ☐ Other

e. How is this plan tested?

☐ Internal Discussion ☐ Internal tabletop exercise ☐ 3rd party tabletop exercise ☐ Other

f. Please describe any other steps that you take to detect and prevent ransomware attacks:

g. Do you maintain regular back-ups (at least weekly), in an encrypted format? Yes: ☐ No: ☐

h. Are your regular back-ups in an encrypted format? Yes: ☐ No: ☐

i. Are your regular back-ups disconnected from and inaccessible through the organization's network? Yes: ☐ No: ☐

j. Do you test the data integrity of your back-ups on at least a quarterly basis? Yes: ☐ No: ☐

If not quarterly, how often?

Frequency:

k. Have you recently carried out a network security audit? Yes: ☐ No: ☐

If 'Yes', who performed the audit and when was it remediated

Audited by:

l. Was any serious concern raised with any aspect of the network? Yes: ☐ No: ☐

If 'Yes' to (i) above, please confirm that concerns were remediated. Yes: ☐ No: ☐

5. THIRD PARTY SERVICE PROVIDERS

a. Please provide a list of information technology vendors by function that provide information technology services that are critical to your business.

Service	Name of Service Provider
a. Web Hosting	
b. Internet Service	
c. Managed Security Service(s)	
d. Data Back-up Solution Product/Service Provider(s)	
e. Application Service Provider(s)	
f. Data Processor(s)	
g. Cloud Provider(s)	
h. Point of Sale/Payment System	
(Detail of Service)	(Name of Service Provider)
i. Other	

b. Other Non-IT Third Party Dependencies:
Please provide a list of Non-IT Vendors that you have outsourced critical business functions to and/or that you rely on to conduct your business (logistics, billing, etc.).

Name of Non-IT Vendor:	Service Being Provided by Vendor:

c. Do you conduct regular reviews of your third party service providers and partners to ensure that they meet your requirements for protecting sensitive information in their care? Yes: ☐ No: ☐

d. Please provide details of what reviews and vetting procedures are in place for third-party service provider: (formal assessment of the security risks of the service provider; a means to assess the security providers' security posture such as SAS70, CICA Section 5970, BITS or otherwise; etc.)

e. Do you have appropriate indemnification provisions in your favour in contracts with these third-party service providers and partners? Yes: ☐ No: ☐

6. NETWORK SECURITY

a. Do you employ a Chief Privacy Officer or Chief Information Officer who has responsibility for meeting your worldwide obligations under privacy and data protection laws? Yes: ☐ No: ☐

b. Are all employment positions analysed and employees assigned specific rights, privileges and unique user ID and passwords, which are changed periodically? Yes: ☐ No: ☐

c. Do you have user revocation procedures on user accounts and inventoried recovery of all information assets following employment termination? Yes: ☐ No: ☐

d. Do you have next-generation firewalls in force across your network? Yes: ☐ No: ☐

e. Do you use malware protection or endpoint detection and response (EDR) tools? Yes: ☐ No: ☐

f. If yes, which vendor, and product:

Other:

RIDGE CYBER APPLICATION – LARGE RISK
($100m - $425m Revenue)

g. Indicate how many endpoints you have:

I. # of workstations / desktops	
II. # of laptops	
III. # of servers	

h. What percentage of your endpoints is this EDR tool deployed to? |

i. If below 90% deployment, is there a roadmap in place to increase this deployment above 90%? Yes: ☐ No: ☐

I. When is the anticipated completion date? |

j. How is this EDR tool monitored and managed?

☐ Internal IT Team ☐ Outsourced to 3rd Party ☐ Other

k. Do you ensure that all wireless networks have protected access? Yes: ☐ No: ☐

l. Do you enforce multi-factor authentication for all remote network access originating from outside your network by employees and third parties (VPN, remote desktop, web-based email access, etc.)? Yes: ☐ No: ☐

m. Do you enforce multi-factor authentication for all privileged account access (both remote and on premises)? Yes: ☐ No: ☐

n. Do you enforce multi-factor authentication for access to back-ups (both remote and on premises)? Yes: ☐ No: ☐

o. Do you enforce multi-factor authentication for all sensitive / confidential information access (both remote and on premises)? Yes: ☐ No: ☐

p. Do you have access control procedures and hard drive encryption to prevent unauthorized exposure of data on all laptops, PDAs, smartphones, and portable devices? Yes: ☐ No: ☐

q. Do you encrypt all sensitive information that is transmitted within and from your organization? Yes: ☐ No: ☐

r. Is sensitive information stored on segregated servers with separate access controls? Yes: ☐ No: ☐

s. Is all sensitive and confidential information stored on your databases, servers and data files encrypted? Yes: ☐ No: ☐

If you answer "No" to questions (o), (r), or (s) above, please describe (in the box below) how confidential/sensitive information is protected on your networks, databases, and mobile devices in the absence of encryption, and please provide the details of the access control provisions in-place for confidential/sensitive information (least-privileged access, PAM tools, etc.):

t. Do you conduct employee cybersecurity awareness training on at least an annual basis? Yes: ☐ No: ☐

u. Does this training include phishing simulation exercises? Yes: ☐ No: ☐

v. Do you provide additional training for employees who fail this training? Yes: ☐ No: ☐

w. When you operate Point of Sale devices are they regularly scanned for malware or skimming devices? Yes: ☐ No: ☐

x. Do you have a software / patch management policy in place? Yes: ☐ No: ☐

y. Are critical patches implemented within 14 days? Yes: ☐ No: ☐

z. Is there any unsupported or "End-of-Life" software or hardware in use? Yes: ☐ No: ☐

aa. Are inbound and outbound emails scanned for malicious links, attachments, and content? Yes: ☐ No: ☐

ab. For email security, are the following utilized?

☐ Sender Policy Framework (SPF) ☐ DomainKeys Identified Mail (DKIM) ☐ Domain Messaging Authentication Reporting & Conformance (DMARC)

ac. Are Advanced Threat Protection settings enabled for all email users? Yes: ☐ No: ☐

7. INFORMATION AND DATA MANAGEMENT

a. Does your information asset program include a data classification standard (public, internal use only, confidential, etc.)? Yes: ☐ No: ☐

b. Do you post a privacy policy on your website which has been reviewed by a qualified lawyer? Yes: ☐ No: ☐

c. Does your privacy policy include a legally reviewed statement advising users as to how any information collected will be used, and for what purposes? Yes: ☐ No: ☐

d. Do you have procedures in force for honouring the specific marketing "opt-out" requests of your customers that are consistent with the terms of your published privacy policy? Yes: ☐ No: ☐

e. Do you have procedures in place to monitor the period for which customer data is held and have processes for deleting this information at the end of that period? Yes: ☐ No: ☐

f. Do you have procedures in force for deleting all sensitive data from systems and devices prior to their disposal from the company? Yes: ☐ No: ☐

g. Is all information held in physical form (paper, disks, CD's etc.) disposed of or recycled by confidential and secure methods, which are recognized throughout the organization? Yes: ☐ No: ☐

h. Do you keep an incident log of all system security breaches and network failures? Yes: ☐ No: ☐

i. Please confirm up-to-date compliance with relevant regulatory and industry frameworks:

Personal Information Protection and Electronic Documents Act (PIPEDA)	Yes: ☐	No: ☐	N/A: ☐
Personal Health Information Protection Act (PHIPA)	Yes: ☐	No: ☐	N/A: ☐
Canada's Anti-Spam Legislation (CASL)	Yes: ☐	No: ☐	N/A: ☐
Payment Card Industry (PCI) Data Security Standard	Yes: ☐	No: ☐	N/A: ☐

If 'Yes', what level of PCI compliance ☐ 1 ☐ 2 ☐ 3 ☐ 4

Other (provide details)

8. MEDIA AND INTELLECTUAL PROPERTY PROCEDURES

a. Do you have a process to review all media content and advertising materials prior to release? If 'No', please provide details in the 'Additional Notes' section of this Application on your current process in place for reviewing all media content and advertising material prior to release. Yes: ☐ No: ☐

b. If you use freelance designers or obtain content from third parties do you have legally reviewed contracts in force outlining the rights and responsibilities of each party and ensure that you are held harmless in respect of content provided to you? Yes: ☐ No: ☐ N/A: ☐

c. Do you have customer acceptance/sign off for content? Yes: ☐ No: ☐

d. Do you have appropriate take down procedures in respect of any user generated content? Yes: ☐ No: ☐

If 'Yes', what type of media or marketing content are you providing to others as a professional service?

9. CRIME CONTROLS

a. Do at least two members of staff review and authorize any transfer of funds, signing of cheques (above $10,000) or the issuance of instructions for the disbursement of assets, funds or investments? Yes: ☐ No: ☐

b. Do you verify all requests to change customer/vendor/supplier details by confirming via a direct call using the existing contact information previously provided and on file from the entity requesting the change? Yes: ☐ No: ☐

c. If online banking software is used to perform wire transfer functions, is two-factor authentication activated to gain access to the portal? Yes: ☐ No: ☐

10. INCIDENTS, CLAIMS, & CIRCUMSTANCES

During the last five years have you:

a.	Sustained any unscheduled or unintentional network outage or interruption?	Yes: ☐	No: ☐
b.	Suffered a breach of network security that resulted in a system intrusion, tampering, virus or malicious code attack, loss of data, hacking incident, data theft or similar incident or situation?	Yes: ☐	No: ☐
c.	Received notice or become aware of any privacy violations or that any data or personally identifiable information has become compromised?	Yes: ☐	No: ☐
d.	Notified any customers that their information may have been compromised?	Yes: ☐	No: ☐
e.	Been subject to any disciplinary action, regulatory action, or investigation by any governmental, regulatory, or administrative agency?	Yes: ☐	No: ☐
f.	Received any injunction(s), lawsuit(s), fine(s), penalty(ies) or sanction(s)?	Yes: ☐	No: ☐
g.	Suffered any incidents of employee theft, forgery, computer fraud, electronic theft, telecommunications fraud, social engineering or any other related crime related losses or incidents?	Yes: ☐	No: ☐
h.	Become aware of any circumstance or incident that could be reasonably anticipated to give rise to a claim against the type of insurance(s) being requested in this application?	Yes: ☐	No: ☐
i.	Have you or any of the applicant's principals, partners, directors, risk managers, or employees, during the last three years, sustained any loss or had any claim made against them, whether insured or otherwise, involving the type of insurance(s) being requested in this application?	Yes: ☐	No: ☐

If 'Yes' to any of the questions above, please provide the following details for each incident/claim: (Note: You may provide any further additional information by means of a separate attachment if necessary.)

a. a brief description of the incident, including its impact on your business operations
b. initial steps taken to respond to the incident
c. policies and procedures put in place to reduce the likelihood of a similar incident from occurring in the future
d. total cost of responding to and recovering from the incident, including lost income

11. PREVIOUSLY PURCHASED COVERAGE

a. Do you have insurance in place for the type of coverage being requested in this application? Please provide details.

Insurer	Limits	Deductible	Expiry Date	Premium	Retroactive Date

b. Have you ever been refused insurance or had any special terms or conditions imposed by any insurer? Yes: ☐ No: ☐

c. Has any insurance for the type of coverage requested in this application been declined or cancelled? Yes: ☐ No: ☐

If 'Yes' to (b.), or (c.) above, please provide full details

Data Protection

By accepting this insurance you consent to Ridge Canada Cyber Solutions Inc. using the information we may hold about you for the purpose of providing insurance and handling claims, if any, and to process sensitive personal data about you where this is necessary (for example health information or criminal convictions). This may mean we have to give some details to third parties involved in providing insurance cover. These may include insurance carriers, third party claims adjusters, fraud detection and prevention services, reinsurance companies and insurance regulatory authorities.

Where such sensitive personal information relates to anyone other than you, you must obtain the explicit consent of the person to whom the information relates both to the disclosure of such information to us and its use by us as set out above. The information provided will be treated in confidence and in compliance with relevant Data Protection legislation. You have the right to apply for a copy of your information (for which we may charge a small fee) and to have any inaccuracies corrected.

IMPORTANT – Cyber Policy Statement of Fact

By accepting this insurance you confirm that the facts contained in the proposal form are true. These statements, and all information you or anyone on your behalf provided before we agree to insure you, are incorporated into and form the basis of your policy. If anything in these statements is not correct, we will be entitled to treat this insurance as if it had never existed. You should keep this Statement of Fact and a copy of the completed proposal form for your records.

This application must be signed by the applicant. Signing this form does not bind the company to complete the insurance. With reference to risks being applied for in the United States, please note that in certain states, any person who knowingly and with intent to defraud any insurance company or other person submits an application for insurance containing any false information, or conceals the purpose of misleading information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

The undersigned is an authorized principal, partner, director, risk manager, or employee of the applicant and certifies that reasonable inquiry has been made to obtain the answers herein which are true, correct and complete to the best of his/her knowledge and belief. Such reasonable inquiry includes all necessary inquiries to fellow principals, partners, directors, risk managers, or employees to enable you to answer the questions accurately.

Name		Position	
Signature		Date	

ADDITIONAL NOTES