CHUTTER
UNDERWRITING SERVICES

Cyber & Privacy Liability
Application — Social Engineering / eCrime included

INSTRUCTIONS
For organisations seeking Cyber & Privacy Liability coverage. Technology companies or IT service providers should use the Technology E&O + Cyber application instead. Completion of this application does not bind coverage.

SECTION A — APPLICANT DETAILS

LEGAL NAME OF APPLICANT

OPERATING / TRADE NAME (IF DIFFERENT)

BUSINESS ADDRESS

CITY

PROVINCE / STATE

POSTAL / ZIP

PRIMARY CONTACT NAME

TITLE

PHONE

EMAIL

WEBSITE

YEAR ESTABLISHED

FINANCIAL YEAR END (MM/DD)

TOTAL EMPLOYEES (#)

INDUSTRY SECTOR (CHECK PRIMARY)

- ☐ Legal / law firm
- ☐ Healthcare / medical
- ☐ Retail / e-commerce
- ☐ Hospitality / food service
- ☐ Education
- ☐ Non-profit
- ☐ Accounting / finance
- ☐ Insurance
- ☐ Real estate
- ☐ Manufacturing / industrial
- ☐ Government / public sector
- ☐ Other (describe below)

IF 'OTHER' — DESCRIBE INDUSTRY / SECTOR

DESIGNATED BREACH RESPONSE CONTACT EMAIL

SECTION B — OPERATIONS & REVENUE

DESCRIPTION OF OPERATIONS

Describe the applicant's primary business activities, products or services, and the nature of client relationships.

SECTION B — OPERATIONS & REVENUE (continued)

REVENUE

	LAST COMPLETE FY	CURRENT FY ESTIMATE	NEXT FY ESTIMATE
Canada / domestic revenue ($)			
USA revenue ($)			
Other territory revenue ($)			
Total gross revenue ($)			
Profit / (Loss) ($)			

OTHER TERRITORY — DESCRIBE COUNTRY / REGION

EMPLOYEES — REMOTE / WFH

BUSINESS CHANGES (PAST 12 MONTHS OR ANTICIPATED NEXT 12 MONTHS)

Any significant change in the nature or size of the applicant's business? ☐ Yes ☐ No

Any merger, acquisition, consolidation, or divestment completed or contemplated? ☐ Yes ☐ No

Any significant change in IT systems, infrastructure, or cloud adoption? ☐ Yes ☐ No

IF YES TO ANY — PROVIDE FULL DETAILS

SECTION C — DATA & SYSTEMS PROFILE

Select the applicable record count range for each type of personal data held, processed, or accessible.

TYPE OF PERSONAL DATA HELD / PROCESSED	<10K	10K–100K	100K–500K	500K–1M	>1M
Social insurance / government ID numbers	☐	☐	☐	☐	☐
Consumer financial / banking information	☐	☐	☐	☐	☐
Payment card data (credit / debit)	☐	☐	☐	☐	☐
Protected health information (PHI / medical records)	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐
Employee / HR records	☐	☐	☐	☐	☐
Children's personal information (under 13)	☐	☐	☐	☐	☐
Other sensitive personal information	☐	☐	☐	☐	☐

DESCRIBE ANY OTHER SENSITIVE OR CONFIDENTIAL DATA HELD / PROCESSED

SECTION C — DATA & SYSTEMS (continued)

Systems & infrastructure — does the applicant:

Operate its own on-premises servers or data centre infrastructure?	☐ Yes	☐ No
Use cloud-based systems or services (e.g. Microsoft 365, Google Workspace, AWS, Azure)?	☐ Yes	☐ No
Provide hosting, data storage, or processing services to third parties?	☐ Yes	☐ No
Use any point-of-sale (POS) systems or payment terminals?	☐ Yes	☐ No
Operate any operational technology (OT), industrial control systems (ICS), or SCADA systems?	☐ Yes	☐ No

IF YES TO ANY — PROVIDE BRIEF DETAILS, SPECIFYING WHICH ITEM(S) APPLY

DATA BACKUP PROCEDURES

Include: frequency, storage method (online / offline / air-gapped), encryption, and how often backups are tested for recoverability.

SECTION D — CYBER SECURITY CONTROLS

CONFIRM ALL — tick to confirm YES to each statement. Indicate any NO answers in the field provided.

- Multi-factor authentication (MFA) is enabled for all remote access to the network, including all Remote Desktop Protocol (RDP) connections.
- Multi-factor authentication (MFA) is enabled for all email accounts.
- MFA is enforced for all privileged / administrator accounts, both local and remote.
- Critical security patches and updates are applied promptly; no end-of-life or unsupported software is in use.
- All endpoints (desktops, laptops, servers) are protected with anti-virus, anti-malware, or endpoint detection software.
- Remote access to the network is only permitted via a VPN or equivalent secure connection.
- Incoming emails are scanned for malicious attachments and links.
- A firewall is in place at the network perimeter.
- User access rights are restricted to the minimum necessary for each role (principle of least privilege).
- Security awareness training is provided to all employees at least annually.

☐ Confirmed — all statements above apply to this organisation.

IF ANY STATEMENT ABOVE DOES NOT APPLY — EXPLAIN HERE

SECTION D — CYBER SECURITY CONTROLS (continued)

Additional security controls — does the applicant have:

A network intrusion detection system providing alerts on unauthorized access?	☐ Yes	☐ No
Centralized log collection and monitoring for network activity?	☐ Yes	☐ No
Regular vulnerability scanning or penetration testing?	☐ Yes	☐ No
Privileged access management (PAM) for administrator / privileged accounts?	☐ Yes	☐ No
Email filtering and anti-phishing controls beyond standard spam filtering?	☐ Yes	☐ No
Immutable or air-gapped backups not accessible from the primary network?	☐ Yes	☐ No

IF YES TO ANY — DESCRIBE FREQUENCY AND SCOPE OF TESTING / CONTROLS IN PLACE

Data storage — is the following data encrypted?

Data stored on laptops and portable devices — encrypted at rest	☐ Yes	☐ No
Data stored in cloud environments — encrypted at rest and in transit	☐ Yes	☐ No
Backup media (tapes, drives) — encrypted	☐ Yes	☐ No
Payment card data — encrypted at point of capture and through transmission	☐ Yes	☐ No

IF ANY STORED DATA IS NOT ENCRYPTED — DESCRIBE WHICH AND WHY

SECTION E — PRIVACY & PAYMENT CARDS

Has the applicant designated a Chief Privacy Officer or equivalent privacy role?	☐ Yes	☐ No
Has the applicant designated a Chief Information Security Officer or equivalent?	☐ Yes	☐ No

IF NO TO EITHER — DESCRIBE WHO IS RESPONSIBLE FOR PRIVACY AND INFORMATION SECURITY

Does the applicant share personal or confidential data with any third-party vendors, processors, or partners?	☐ Yes	☐ No

IF YES — DESCRIBE NATURE OF SHARING AND CONTRACTUAL PROTECTIONS IN PLACE

SECTION E — PRIVACY & PAYMENT CARDS (continued)

Payment cards — does the applicant:

Accept payment cards for goods or services? ☐ Yes ☐ No

Store, process, or transmit payment card data? ☐ Yes ☐ No

Comply with applicable PCI-DSS standards? ☐ Yes ☐ No

Encrypt payment card data at point of capture and through transmission to the processor? ☐ Yes ☐ No

IF NOT PCI COMPLIANT OR CARD DATA IS NOT ENCRYPTED — DESCRIBE CURRENT STATUS

SECTION F — eCRIME & SOCIAL ENGINEERING CONTROLS

CONFIRM ALL — tick to confirm YES to each statement. Indicate any NO answers in the field provided.

- All employees responsible for disbursing or transmitting funds receive annual anti-fraud training (covering social engineering, phishing, and business email compromise).
- Before processing any fund transfer request, instructions are verified via a method independent of the original channel of communication (e.g. phone call to a known number).
- All fund transfer requests above a defined threshold require review and approval by a supervisor or next-level approver.
- Any vendor or supplier request to change banking or account details is independently verified with a known contact before any changes are made.
- The organisation does not act solely on email instructions to transfer funds without independent verification.

☐ Confirmed — all statements above apply to this organisation.

IF ANY STATEMENT ABOVE DOES NOT APPLY — EXPLAIN HERE

MINIMUM THRESHOLD FOR TWO-STAGE SIGN-OFF ON PAYMENTS ($)

APPROXIMATE TOTAL ANNUAL OUTGOING WIRE / EFT VOLUME ($)

SECTION G — BUSINESS CONTINUITY & INCIDENT RESPONSE

Does the applicant have the following plans in place, and have they been tested?

Disaster recovery plan (DRP) — covering IT systems and infrastructure ☐ Yes ☐ No

Business continuity plan (BCP) — covering broader business operations ☐ Yes ☐ No

Incident response plan (IRP) — covering data breaches, ransomware, and network intrusions ☐ Yes ☐ No

DRP — DATE LAST TESTED

BCP — DATE LAST TESTED

IRP — DATE LAST TESTED

RECOVERY TIME OBJECTIVE (RTO) — STATED

RECOVERY POINT OBJECTIVE (RPO) — STATED

Has the applicant's incident response plan been reviewed by external legal counsel or a specialist cyber incident response firm? ☐ Yes ☐ No

SECTION H — PRIOR INSURANCE & CLAIMS HISTORY

CURRENT / PRIOR CYBER INSURANCE

☐ No previous cyber insurance ☐ Currently hold cyber insurance

INSURER	EXPIRY DATE	LIMIT ($)	ANNUAL PREMIUM ($)

RETROACTIVE DATE	DEDUCTIBLE / RETENTION ($)

Has coverage ever been declined, cancelled, or non-renewed? ☐ Yes ☐ No

IF YES — PROVIDE FULL DETAILS

In the past 5 years, has the applicant, or any past or present principal, director, officer, or employee:

Experienced a data breach, ransomware attack, or unauthorized access to systems?	☐ Yes ☐ No
Notified individuals or regulators of a privacy breach or data incident?	☐ Yes ☐ No
Been subject to a government investigation or regulatory action regarding data or privacy?	☐ Yes ☐ No
Received a demand, complaint, or claim relating to privacy or data security?	☐ Yes ☐ No
Experienced an attempted or successful social engineering, wire transfer fraud, or phishing fraud — resulting in a loss?	☐ Yes ☐ No
Experienced an unexpected outage of a critical system lasting more than 4 hours?	☐ Yes ☐ No
Experienced any property damage or business interruption loss as a result of a cyber attack?	☐ Yes ☐ No
Experienced a business interruption caused by an outage at a third-party service provider or cloud vendor?	☐ Yes ☐ No
Suffered any loss arising from the dishonesty or malice of any employee or contractor?	☐ Yes ☐ No

SECTION H — CLAIMS HISTORY (continued)

If YES to any — complete the table below for each matter. Attach additional sheets if required.

DATE	DESCRIPTION OF INCIDENT / CLAIM	AMOUNT CLAIMED ($)	STATUS	AMOUNT PAID ($)	REMEDIATION STEPS TAKEN

Is the applicant currently aware of any of the following:

Any known vulnerability, incident, or breach that has not yet been fully remediated? ☐ Yes ☐ No

Any circumstance that might reasonably be expected to give rise to a claim? ☐ Yes ☐ No

Any threatened or actual regulatory investigation relating to data or privacy? ☐ Yes ☐ No

IF YES TO ANY — PROVIDE FULL DETAILS

SECTION I — COVERAGE REQUESTED

CYBER LIABILITY LIMIT REQUESTED

☐ $250,000 ☐ $500,000 ☐ $1,000,000 ☐ $2,000,000 ☐ $3,000,000 ☐ $5,000,000

DESIRED EFFECTIVE DATE

RETROACTIVE / PRIOR ACTS DATE

SECTION J — DECLARATION

IMPORTANT NOTICE

The undersigned declares that the statements and information contained in this application, and any supplementary materials submitted in connection with it, are true, accurate, and complete in all material respects. The applicant understands and agrees that this application shall form the basis of and be incorporated into any policy issued. The applicant acknowledges that the insurer will rely upon the representations made herein when underwriting and issuing coverage. Any material misrepresentation, misstatement, or failure to disclose relevant information may render the policy void from inception or result in the denial of coverage, subject to applicable law.

FULL NAME (PRINT)

TITLE / POSITION

DATE (MM / DD / YYYY)

SIGNATURE OF AUTHORIZED REPRESENTATIVE