Zurich Security and Privacy Protection

ZURICH

Proposal form

Completing the Proposal form

1. This application must be completed in full including all required attachments.
2. If more space is needed to answer a question, please attach a separate sheet with details.
3. The terms Proposer, whenever used in this proposal form shall mean the Policyholder listed below and all Subsidiary companies of the Policyholder for which coverage is proposed under this proposal.
4. The terms Policyholder and Subsidiaries have the same meaning in this proposal form as in the policy.

Duty of Disclosure

Before you enter into a contract of general insurance with us, you have a duty at common law to disclose to us every matter you know, or could reasonably be expected to know that a prudent insurer would want to take into account in deciding whether to insure you and, if so, on what terms. This applies to all persons to be covered under this contract of insurance.

You have the same duty to disclose those matters to us before you renew, extend, vary or reinstate a contract of general insurance.

Your duty however, does not require disclosure of a matter:

- that diminishes the risk to be insured;
- that is of common knowledge;
- that we know or in the ordinary course of our business we ought to know;
- that we indicate to you that we do not want to know.

Non-disclosure or misrepresentation

If you make a material misrepresentation to us, or if you do not comply with your duty of disclosure, we may treat your policy as if it never existed.

False statement and Fraudulent acts

Your policy is based on the information supplied to us by you or on your behalf. All statements made by you or on your behalf on the proposal and/or questionnaire, in support of this policy, on any claim form or in support of any claim must be true and correct. If you take any action or make any statement in connection with this policy or any claim made under it, which is fraudulent in any way or which is supported by untrue or incorrect information, we are entitled to avoid this policy and all benefits under it will be forfeited.

Privacy Act 2020

Zurich respects your privacy. The following is brought to your attention. However this does not apply to companies.

(a) This Proposal collects personal information about you;

(b) The information is collected by Zurich to evaluate the insurance being sought;

(c) The intended recipient of the information is Zurich;

(d) The information is being collected and held by Zurich;

(e) The collection of this information is required pursuant to the common law duty to disclose all material facts relevant to the insurance sought and is mandatory;

(f) The failure to provide this information may result in your application for insurance being declined, or your insurance being void from the beginning;

(g) You have rights to access, and correct this information subject to the provisions of the Privacy Act 2020.

Data sharing consent

In order to provide a seamless insurance service globally, Zurich may transfer any data Zurich has received from and any data it holds on the policyholder to other units of Zurich Insurance Group Ltd, such as branches, subsidiaries, or affiliates within Zurich Insurance Group Ltd, cooperative partners of Zurich Insurance Group Ltd, coinsurance and reinsurance companies located in the country of the policyholder or abroad.

Zurich as well as such recipients may use, process and store the data, in particular for the purpose of risk evaluation, policy execution, premium setting, premium collection, claims assessment, claims processing, claims payment, statistical evaluation or to otherwise ensure Zurich's global insurance service delivery.

If a broker or agent is acting on behalf of the policyholder, Zurich is authorised to use, process and store data of the policyholder received from such broker or agent, and to forward to such broker or agent data of the policyholder relating to the execution of the policy and the collection of premiums and payment of claims.

Zurich may procure data from government offices and third parties relating to the policyholder to assess a claim in the event of loss or damage.

ZU20968 - V3 12/13 - PCUS-008235-2013 (A)

1 General information details

Policyholder and Subsidiaries

Policyholder name

Mailing address Postcode

Ownership: Public ◯ Private ◯ Year established Number of employees

Website address

Risk manager Email address

Name of all subsidiaries or affiliates (*please insert attachment if too numerous*)

Is applicant controlled, owned, affiliated or associated with any other firm, corporation or company? Yes ◯ No ◯

If 'Yes', please describe

During the past five (5) years

Has the name of the applicant been changed? Yes ◯ No ◯

Has any other business been acquired, merged or consolidated with the applicant? Yes ◯ No ◯

If 'Yes', please describe

Requested Coverage

Requested Coverage(s):		**Requested Limits of Liability:**	**Deductible:**	
1.1	Privacy Breach Costs	$	$	each Privacy Event
1.2	Digital Asset Replacement Expenses	$	$	each Security Event
1.3	Security and Privacy Liability	$	$	each Claim
	Regulatory Proceeding Defence	$	$	each Regulatory Proceeding
1.4	Business income loss and Dependent business income loss	$	The greater of: $ or hours	each security event each Security Event (Waiting Hours Retention)
1.5	Cyber Extortion Threat and Reward payments	$	$	each Cyber Extortion Threat (excluding Reward payments)
	Reward payments	$	NIL	
1.6	Internet Media Liability	$	$	each Claim

Requested Retroactive dates:

Security and Privacy Liability

Internet Media Liability

2 Policyholders profile

	Year	New Zealand Turnover	US Turnover	International (excluding US) T/O	Total Turnover
Projected		$	$	$	$ 0
Current		$	$	$	$ 0

3 Business activities

(a) Does the applicant allow online purchases, bill payment, banking or trading? Yes ◯ No ◯

If 'Yes', what portion of the applicant's revenue is received through the online distribution channel?

◯ None ◯ 0-2% ◯ 3-10%

◯ 11-25% ◯ 26-100%

(b) What types of personal information does the applicant collect, process, and store (please check all that apply)?

◯ Business and Customer Information ◯ Healthcare Information ◯ Tax File Numbers

◯ Credit Card Information ◯ Financial Account Information ◯ Intellectual Property/Trade Secrets

(c) Does the applicant transfer sensitive information with personal identifiers across international borders? Yes ◯ No ◯

(d) Does the applicant outsource any of its primary business functions to a third party? If so, please indicate:

◯ Human Resources ◯ Customer Service ◯ Marketing

◯ Business Development ◯ Information Technology ◯ Internal Audit

◯ Other

(e) Does the applicant share personal information with business partners, vendors, or other third parties to provide products or services? Yes ◯ No ◯

4 Organisation and Governance

(a) Does a senior executive have formal, enterprise-wide responsibility for records and information management? Yes ◯ No ◯

If 'Yes', please indicate the job title of the executive

◯ Chief Privacy Officer ◯ Chief Information Security Officer

◯ Other Title

(b) Are security risk assessments conducted on at least an annual basis to validate that organisational security policies are being followed? Yes ◯ No ◯

(c) Are privacy risk assessments conducted on at least an annual basis to validate that organisational privacy policies are being followed? Yes ◯ No ◯

(d) Are the results of risk assessments shared with executive management and key issues and exposures formally tracked until remediated and resolved? Yes ◯ No ◯

(e) Has the applicant identified all relevant legal, regulatory and industry supported compliance frameworks that are applicable to the applicant's organisation and do the applicant's policies reflect these requirements? Yes ◯ No ◯

(f) Does the applicant have a formal policy covering records and information management in place? Yes ◯ No ◯

(g) Has the applicant formally documented and operationalised the following policies (please check all that apply)?

◯ Access Control ◯ Alerting ◯ Asset Management

◯ Data Classification ◯ Data Disposal ◯ Human Resources Security

◯ Logging ◯ Media Handling ◯ Monitoring

◯ Network Security ◯ Physical Security ◯ Privacy

◯ Security ◯ Vendor Management ◯ Vulnerability Management

(h) Is a list maintained of all vendors with whom personal information is shared or to whom network access is provided? Yes ◯ No ◯

(i) Do all vendor contracts convey security and privacy obligations and expectations, including the maintenance of professional liability and network risk coverage? Yes ◯ No ◯

4 Organisation and Governance (continued)

(j) In all cases, does the applicant's hiring process include the following investigations: criminal convictions, educational background and work history? Yes ◯ No ◯

If hiring procedures are only required in some cases, please describe when such procedures are required

(k) Is the applicant subject to the Payment Card Industry Data Security Standard (PCI DSS v3.0)? Yes ◯ No ◯

If 'Yes', please indicate merchant level

◯ 1 ◯ 2 ◯ 3 ◯ 4

(l) Has the applicant achieved PCI compliance? Yes ◯ No ◯

If 'Yes', please provide the date of the latest certification

(m) What percentage of the applicant's most recent PCI audit was identified as adequate or in place? %

(n) For those standards that were identified as inadequate or not in place, how many have been successfully implemented since the last audit?

5 Network security

(a) Are systems, applications and supporting infrastructure that collect, process, or store personal information segregated from the rest of the network? Yes ◯ No ◯

(b) Is firewall technology used at all internet points of presence and do formal firewall configuration standards exist? Yes ◯ No ◯

(c) Are firewalls installed between all wireless networks and system components that process or store personal information? Yes ◯ No ◯

(d) Are wireless transmissions protected using WPA/WPA2, IPSEC, or SSL? Yes ◯ No ◯

(e) Are intrusion detection and prevention systems (network and host based) utilised and are the signatures and anomalies updated on a frequent basis? Yes ◯ No ◯

(f) Does a formal change management process exist that takes into account security and privacy risks for things such as application deployments (code and content) and system or infrastructure changes (e.g. patch installation, firewall rule-set changes)? Yes ◯ No ◯

(g) Are internal and external vulnerability scans and penetration tests (network and application layer) conducted on a periodic basis and the vulnerabilities identified, tracked and remediated? Yes ◯ No ◯

(h) Do all users of systems, applications and supporting infrastructure that collect, process, or store personal information have a unique ID? Yes ◯ No ◯

(i) Is 2-factor authentication utilised for all remote access (e.g. VPN) to the internal network? Yes ◯ No ◯

(j) Do password policies and procedures exist that outline strong password requirements (e.g. change of passwords on a periodic basis, use of numeric and alphabetic characters, prohibition of previously used passwords)? Yes ◯ No ◯

(k) Is user access to systems, applications and supporting infrastructure that collect, process, or store personal information removed in a timely manner upon employee termination, job change, or cancellation of a third party vendor agreement? Yes ◯ No ◯

(l) Do removable media handling procedures exist for the internal or external distribution of media that contain personal information? Yes ◯ No ◯

6 Data management

(a) Does an inventory exist of all systems, applications and supporting infrastructure (e.g. servers, databases) that collect, process, or store personal information? Yes ◯ No ◯

(b) Do security configuration standards and procedures exist for new system components (e.g. operating systems, software applications, network devices)? Yes ◯ No ◯

(c) Do procedures exist to monitor for new vulnerabilities within system components and apply the latest security patches within one month? Yes ◯ No ◯

(d) Does the applicant utilise anti-virus software on all systems commonly affected by viruses, particularly personal computers and servers? Yes ◯ No ◯

6 Data management (continued)

(e) Does the applicant's anti-virus programs detect, remove, and protect against other forms of malicious software, including spyware and adware? Yes ◯ No ◯

(f) Do procedures exist to operationalise the proper disposal of personal information and data and have they been implemented in compliance with the organisation's confidential data disposal policy? Yes ◯ No ◯

(g) Is commercial grade technology employed to encrypt all sensitive business and consumer information:

Transmitted within the applicant's organisation or to other public networks? Yes ◯ No ◯

At rest in relational databases and other network locations? Yes ◯ No ◯

Maintained on employee laptops and other mobile equipment? Yes ◯ No ◯

Physically transmitted by hard drive, tape or other media within the applicant's organisation or to third parties, including data storage management companies? Yes ◯ No ◯

7 Incident response

(a) Are system and security logs in place on all systems that collect, process, or store personal information? Yes ◯ No ◯

(b) Are automated tools in place that aggregate and correlate log information and send out alerts based upon identified thresholds? Yes ◯ No ◯

(c) Has a formal data breach plan been prepared and implemented? Yes ◯ No ◯

If 'Yes', does this plan include (please check all that apply):

◯ formal assignment of responsibility for the applicant organisation's response?

◯ identification of an external forensic investigation resource?

◯ a communications plan for customers or other affected individuals?

◯ a preferred credit monitoring services vendor, with pre-negotiated rates?

8 Business continuity planning

(a) Does a business continuity and disaster recovery plan exist? Yes ◯ No ◯

(b) Are the business continuity and disaster recovery plans tested at least annually and updated accordingly? Yes ◯ No ◯

(c) Are system backup and recovery procedures documented and tested for all mission-critical systems? Yes ◯ No ◯

(d) Are the applicant's systems backed up on a daily or more regular basis? Yes ◯ No ◯

9 Incident history

(a) In the past three years, has the applicant sustained any significant systems intrusion, data theft or other loss of data? Yes ◯ No ◯
**If 'Yes', please attach a detailed description of the circumstance(s)*

(b) In the past three years, has the applicant been notified by any third party that Personally Identifiable Information has been compromised from the applicant's systems? Yes ◯ No ◯
**If 'Yes', please attach a detailed description of the circumstance(s)*

(c) In the past three years, has the applicant notified customers that their Personally Identifiable Information was compromised from the applicant's systems? Yes ◯ No ◯
**If 'Yes', please attach a detailed description of the circumstance(s)*

(d) Has the applicant ever been the subject of an investigation by a regulatory or other government agency arising out of a privacy issue? Yes ◯ No ◯
**If 'Yes', please attach a detailed description of the circumstance(s)*

10 Internet Media

(a) Are policies or procedures in place to screen internet content for potential infringement of third party intellectual property rights? Yes ◯ No ◯

(b) Are policies or procedures in place to screen internet content for elements that may lead to personal injury torts including but not limited to libel, slander, and defamation? Yes ◯ No ◯

(c) Does the applicant require contractors, vendors or others who provide the organisation with copyrightable material to perform any of the following (check all that apply): Yes ◯ No ◯

◯ Legally assign or license their rights to any copyrightable material

◯ Warrant that their work does not violate another party's IP rights

◯ Indemnify the applicant for IP infringement claims

◯ Hold the applicant harmless for IP infringement claims

(d) Does the applicant's web site(s) allow third party networking capabilities including but not limited to social networking or blogs? Yes ◯ No ◯

(e) Does the applicant maintain coverage through the advertising injury or personal injury coverage part of the applicant's Commercial General Liability policy? Yes ◯ No ◯

(f) In the past three years, has the applicant received notice of the applicant's infringement on any third party intellectual property rights? Yes ◯ No ◯

**If so, please provide an attachment with a description of such infringement.*

11 Applicant history

Prior Coverage

Please list any similar insurance carried during the past three (3) years

If none, check here ◯ NA

Policy Period	Carrier	Limit of Liability	Deductible	Premium	Retroactive date
		$	$	$	
		$	$	$	
		$	$	$	

Claims history

(a) In the past three years, has the applicant been declined any similar security and privacy insurance, or has the applicant's insurer cancelled any previous security and privacy insurance? Yes ◯ No ◯

**If 'Yes', please attach a detailed description of the circumstances*

(b) Have any claims been made against the applicant or any of its former or current directors, officers, employees, subsidiaries or independent contractors with regard to the coverage sought in the past three years? Yes ◯ No ◯

**If 'Yes', please attach a detailed description of the claim(s)*

(c) Is the applicant or any of its former or current directors, officers, employees, subsidiaries or independent contractors aware of any acts, errors, omissions or other circumstances, which may reasonably result in a claim relative to the insurance sought? Yes ◯ No ◯

**If 'Yes', please attach a detailed description*

12 Declaration

The undersigned represents that every effort has been made to facilitate the proper completion of this application. The discovery of any fraud, intentional concealment, or misrepresentation of any material fact will render this policy, if issued, void at inception. Receipt and review of this application does not bind Zurich to provide this insurance.

It is agreed by the undersigned and Zurich that the particulars and statements made in this application, together with all attachments to this application and any other materials submitted to Zurich (all of which attachments and materials shall be deemed attached to the policy as if physically attached thereto) shall be the representations of the applicant and the prospective Insureds. It is further agreed by the undersigned and the prospective Insureds that this policy, if issued, is issued in reliance upon the truth of such representations that are incorporated into and made part of this policy.

After inquiry of all prospective Insureds, the undersigned authorised officer of the applicant represents that the statements set forth in this application and its attachments and other materials submitted to Zurich are true and correct and that no material or relevant facts have been suppressed or misstated. Signing of this application does not bind the applicant or the Insurer.

The undersigned further declares that any event taking place between the date this application was signed and the effective date of the insurance applied for which may render inaccurate, untrue, or incomplete any information in this application, will immediately be reported in writing to Zurich and Zurich may withdraw or modify any outstanding quotations and /or authorisation or agreement to bind the insurance.

Applicants name Title

Applicant signature Date

✗ / /

Please submit the following information with this proposal

1. Copy of most recent financial statements (annual report)
2. Five (5) years of loss runs valued within the past six (6) months
3. List of all litigation threatened or pending which could potentially affect the coverage for which you are applying
4. Copy of the privacy policies currently in use throughout the applicant's organisation
5. Executive Summary of most recent Network Security Audit or PCI DSS Audit (if applicable)

Save File Print Form