



ZURICH[®]

Commercial Crime Insurance

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 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 an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and on what terms.

You have this duty until we agree to insure you.

You have the same duty before you renew, extend, vary or reinstate an insurance contract.

You do not need to tell us anything that:

- reduces the risk we insure you for; or
- is common knowledge; or
- we know or should know as an insurer; or
- we waive your duty to tell us about.

If you do not tell us something

If you do not tell us anything you are required to, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both. If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.

Privacy

Zurich is bound by the Privacy Act 1988 (Cth). We collect, disclose and handle information, and in some cases personal or sensitive (eg health) information, about you ('your details') to assess applications, administer policies, contact you, enhance our products and services and manage claims ('Purposes'). If you do not provide your information, we may not be able to do those things. By providing us, our representatives or your intermediary with information, you consent to us using, disclosing to third parties and collecting from third parties your details for the Purposes.

We may disclose your details, including your sensitive information, to relevant third parties including your intermediary, affiliates of Zurich Insurance Group Ltd, other insurers and reinsurers, our banking gateway providers and credit card transactions processors, our service providers, our business partners, health practitioners, your employer, parties affected by claims, government bodies, regulators, law enforcement bodies and as required by law, within Australia and overseas.

We may obtain your details from relevant third parties, including those listed above. Before giving us information about another person, please give them a copy of this document. Laws authorising or requiring us to collect information include the Insurance Contracts Act 1984, Anti-Money Laundering and Counter-Terrorism Financing Act 2006, Corporations Act 2001, Autonomous Sanctions Act 2011, A New Tax System (Goods and Services Tax) Act 1999 and other financial services, crime prevention, trade sanctions and tax laws.

Zurich's Privacy Policy, available at www.zurich.com.au or by telephoning us on 132 687, provides further information and lists service providers, business partners and countries in which recipients of your details are likely to be located. It also sets out how we handle complaints and how you can access or correct your details or make a complaint.

All questions in this Proposal form must be answered

1 Particulars of Proposer

(a) Name of the Proposer including all subsidiary and associated companies for which cover is requested

.....

(b) Principal address of the proposer

State

Postcode

(c) Please describe your activities

.....

(d) Number of employees

(e) Number of locations

(f) Number of (i) employees handling money or securities

(ii) other employees

(g) Number of (i) blue collar employees

(ii) white collar employees

.....

2 Employee controls

(a) Do you have established formal procedures for recruiting all employees and assessing their suitability for positions of trust? Yes ☐ No ☐

(b) Are all employees required to take an uninterrupted holiday of at least two weeks or half their annual entitlement (whichever is the lesser) in each calendar year during which they perform no duties and are required to stay away from your premises?

Yes ☐ No ☐

(c) Are wages/salaries independently checked against personnel records?

Yes ☐ No ☐

(d) Is there a separation as to the employees involved, in respect to adding new employees to the payroll list and those reconciling salary payments made?

Yes ☐ No ☐

3 Internal controls

(a) Are the duties of any employees segregated so that no one employee can control any of the following transactions from commencement to completion:

(i) Signing cheques above \$5,000?

Yes ☐ No ☐

(ii) Issuing funds transfer instructions?

Yes ☐ No ☐

(iii) Issuing amendments to funds transfer procedures?

Yes ☐ No ☐

(iv) Authorising capital expenditure above \$5,000?

Yes ☐ No ☐

(v) Investments?

Yes ☐ No ☐

(b) Are statements of account sent to customers/vendors regularly and, at a minimum, monthly?

Yes ☐ No ☐

(c) Are statements of account sent to customers/vendors independently of employees receiving payment?

Yes ☐ No ☐

(d) Is reconciliation of bank statements and client/vendor accounts carried out by employees not authorised to deposit/withdraw funds, issue fund transfer instructions or dispatch accounts to clients/vendors?

Yes ☐ No ☐

(e) In addition to any work carried out by the Internal Audit, is a complete inventory made with physical checks to stock and equipment?

Yes ☐ No ☐

If 'Yes', how often?

.....

4 Computer security

(a) Does your computer system offer a remote access facility? Yes ☐ No ☐

If 'Yes', Is this restricted solely to providing information or to providing an electronic mail function?

Yes ☐ No ☐

(b) Are passwords used to afford varying levels of entry to the computer system depending on the need and authorisation of the user?

Yes ☐ No ☐

(c) Are passwords regularly changed when there is any turnover in knowledgeable personnel?

Yes ☐ No ☐

(d) Does the system force regular changes to user passwords?

Yes ☐ No ☐

If 'Yes', how often?

.....

(e) Are all source documents secured to prevent unauthorised modifications or use of data before entering the computer system? Yes ☐ No ☐

.....

5 Electronic fund transfer procedures

- (a) Are electronic fund transfers made independently of transfers made on your behalf by your treasury department? Yes ☐ No ☐
If 'Yes', please go to question (b), if 'No', go to question (g).
- (b) What is the annual volume (currency) of funds transfer instructions given to financial institutions?
- (c) How are fund transfer instructions issued;
- | | |
|---|--|
| (i) by letter | Yes ☐ No ☐ |
| (ii) on voice instructions | Yes ☐ No ☐ |
| (iii) via facsimile | Yes ☐ No ☐ |
| (iv) via telex | Yes ☐ No ☐ |
| (v) via computer link to cash management system | Yes ☐ No ☐ |
| (vi) via electronic mail link | Yes ☐ No ☐ |
| (vii) other (please give details) | |
- (d) Are banks required, by formal agreement, to authenticate any instructions received from you, before payment? Yes ☐ No ☐
- (e) If transfer instructions are made by voice instructions, please provide full details of the authentication process (use of code words, passwords etc).
- (f) If transfer instructions are made by facsimile or telex are these tested? Yes ☐ No ☐
- (g) If instructions are given to your own treasury department please provide full details of how these instructions are issued.

6 Audit

1. Is there an internal audit department? Yes ☐ No ☐
- (a) Is there an audit and control procedures manual? Yes ☐ No ☐
- (b) How many people are employed in the internal audit department?
- (c) Please describe how the audit plan is developed and agreed
- (d) Are audits made on a surprise basis? Yes ☐ No ☐
- (e) Are auditors forbidden to originate entries? Yes ☐ No ☐
- (f) Does the audit plan include random and surprise checks on raw materials, work in progress, finished goods and stocks? Yes ☐ No ☐
- (g) What is the minimum audit frequency for any location/operation?
- Please describe the activities carried out at this operation/location.
- (h) What is the maximum audit frequency for any location/operation?
- Please describe the activities carried out at this operation/location.
- (i) Please describe your procedures for follow up and monitoring of audit recommendations to ensure full implementation.

6 Audit (continued)

2. State the name of the independent firm of Chartered Accountant or professional auditors or other competent authority who fully audit your accounts annually.

.....
(a) What is the frequency of audit?

.....
(b) Are all premises, including computer centre and facilities included in the audit?

Yes ☐ No ☐

.....
(c) Do they regularly review the system of internal control and furnish written reports on such to the Board of Directors?

Yes ☐ No ☐

.....
(d) Have all control and procedural recommendations made been adopted or resolved?

Yes ☐ No ☐

If 'No', please provide details.

7 Physical exposure and credit cards

(a) Do you issue credit/charge cards to employees? Yes ☐ No ☐ If 'Yes'

(i) What is the maximum credit limit?

.....
(ii) Are employees directly responsible to the credit card company for settling monthly statements?

Yes ☐ No ☐

.....
(iii) When an employee leave the company is the credit/charge card issuer immediately advised that the card should be cancelled and that the employee is responsible for all outstanding debts?

Yes ☐ No ☐

(b) What is the maximum value of money, securities, precious metals and/or Jewellery on any of your premises?

(i) During business hours?

.....
(ii) Outside of business hours?

(c) What is the maximum value of stock held at any one location?

(d) Is access to all business premises controlled?

Yes ☐ No ☐

(e) Are premises occupied outside business hours?

Yes ☐ No ☐

(f) Are all premises fitted with alarms which are maintained in proper working order.

Yes ☐ No ☐

If 'Yes', are these connected to:

(i) Back to base monitoring services?

Yes ☐ No ☐

(ii) Police station?

Yes ☐ No ☐

(g) Have any security surveys been carried out in the last three years whose recommendations have not been taken up?

Yes ☐ No ☐

If 'Yes', please describe those recommendations.

8 Outsourcing

Do you outsource services to third party companies (e.g. payroll, computing or accountancy services) under a written contract? Yes ☐ No ☐

If 'Yes', do you:

(i) carry out checks to satisfy yourself as to the honesty, competence and financial stability of those companies?

Yes ☐ No ☐

(ii) retain the right to audit those services?

Yes ☐ No ☐

9 Fraudulent Impersonation Extension

Crime Insurance Optional Extension of Cover – Fraudulent Impersonation

Do you wish to apply for the Fraudulent Impersonation Optional Extension to the Crime Insurance policy?

Yes ☐ No ☐

If 'Yes', please answer the following, if 'No' go to Question 10

Internal controls – vendors

(a) Do you have procedures to verify the identity and authenticity of new vendors before entering into transactions with them? Yes ☐ No ☐

If 'Yes', do you follow any of the following procedures?

(i) Investigate new vendors through a credit reporting agency? Yes ☐ No ☐

(ii) Verify and confirm the vendor's bank account information (account numbers, routing numbers, bank name and address) by calling the vendor's bank directly? Yes ☐ No ☐

Please provide details of any other procedures not listed above that you have in place to verify the identity and authenticity of new vendors

If 'No' to any of the above, explain the reason for not following these procedures

(b) Do you accept requests for funds transfer, payment, delivery or change in method, destination or bank account information instructions from vendors:

(i) over the telephone? Yes ☐ No ☐

(ii) by telefacsimile? Yes ☐ No ☐

(iii) by electronic mail? Yes ☐ No ☐

(iv) by text message? Yes ☐ No ☐

(v) by other methods? Yes ☐ No ☐

If 'Yes' to (v), please provide details of those other methods

(c) Do you have procedures to verify the authenticity of invoices or other form of payment requests received from a vendor? Yes ☐ No ☐

If 'Yes', do you follow any of the following procedures?

(i) Verify invoices or other form of payment requests against inventory, supplies, goods or services rendered by vendor prior to making payment to a vendor? Yes ☐ No ☐

(ii) Maintain a record of such requests and verification on file? Yes ☐ No ☐

Please provide details of any other procedures to verify the authenticity of invoices or other form of payment requests received from a vendor

If 'No' to any of the above, explain the reason for not following these procedures

9 Fraudulent Impersonation Extension (continued)

- (d) Do you have procedures in place to verify and authenticate any request for funds transfer, payment, delivery or change of a vendor's bank account information or methods or destinations of payment? Yes ☐ No ☐

If 'Yes', do you follow any of the following procedures?

- (i) Call the vendor at a telephone number previously provided by the vendor to verify and authenticate the request? Yes ☐ No ☐
- (ii) Send an email to a pre-determined address and require response from vendor to verify and authenticate the request? Yes ☐ No ☐
- (iii) Send notice of receipt of the request to a person at the vendor, other than the person who sent the request, and receiving confirmation of request for change before making the requested change? Yes ☐ No ☐
- (iv) Require review and approval of any changes of the vendor's bank account information by a supervisor and with an individual at the vendor other than the individual sending request before the change is made in your records? Yes ☐ No ☐
- (v) Run exception reports showing all changes to vendor or supplier details? Yes ☐ No ☐
- (vi) Maintain a record of such requests, verification and authentication on file? Yes ☐ No ☐

Please provide details of any other procedures not listed above that you have in place to verify the authenticity of such instructions

If 'No' to any of the above, explain the reason for not following these procedures

Internal controls – employees

- (e) Is there a written policy regarding fund or securities transfers? Yes ☐ No ☐

- (f) Who within the organisation has the ability and authority to initiate a payment, funds or securities transfer?

- (g) Can funds or securities transfer authority be delegated to anyone verbally or in writing? Yes ☐ No ☐

- (h) Do you accept requests for payment, funds transfer, delivery or change in method, destination or bank account information instructions from authorised employees:

- (i) over the telephone? Yes ☐ No ☐
- (ii) by telefacsimile? Yes ☐ No ☐
- (iii) by electronic mail? Yes ☐ No ☐
- (iv) by text message? Yes ☐ No ☐
- (v) by other methods? Yes ☐ No ☐

If 'Yes' to (v), please provide details of those other methods

- (i) Once a request is initiated, to whom does it go for verification, authentication and processing?

- (j) Whose signatures of approval are needed to release the funds or securities?

- (k) Please provide details of the dollar amount and the level of approval needed to release the funds or securities

- (l) Is there segregation of duties between the person(s) who is/are authorised to receive payment or funds/securities transfer requests and the individuals(s) authorised to process the requests? Yes ☐ No ☐

- (m) What is the average length of the entire funds transfer process from the receipt of instruction until the funds or securities are disbursed?

9 Fraudulent Impersonation Extension (continued)

(n) If online banking software is used to perform funds transfer functions, is access to the portal restricted to specific users and terminals? Yes ☐ No ☐

(o) Do the procedures for international funds transfers differs in any way from the domestic procedures? Yes ☐ No ☐

If 'Yes', please advise in what way(s) they differ and how many international funds transfers are processed each month

(p) Do those employees responsible for executing payment, funds or securities transfers receive training on social engineering scams? Yes ☐ No ☐

If 'Yes',

(i) how often is this training updated?

(ii) do you test employees randomly with simulated bait e-mails, calls, telefacsimile, or other means that are generated by you or a third party contracted to perform such testing? Yes ☐ No ☐

(iii) how are employees subsequently trained to be aware of suspicious e-mails, calls, or telefacsimile that were subject of testing?

(iv) Is there an internal department or person to whom employees can direct suspicious e-mails, calls, or telefacsimile to maintain a record of and further investigate? Yes ☐ No ☐

If 'Yes' to (iv), please provide details

Loss experience

List all social engineering/fraudulent impersonation losses discovered by the Proposer in the last six (6) years

Tick if none: ☐

Date of Loss	Description of Loss	Total Amount of Loss	Amount paid by insurance	Date Paid
		\$	\$	
		\$	\$	
		\$	\$	
		\$	\$	

Please attach a description of the corrective measures taken to mitigate future losses of this type

10 Claims experience

(a) Please give brief details of any loss or losses you have sustained (whether insured or uninsured), during the past **five years** which would have impacted upon the coverage you are now seeking had it have been in force at the time of such loss or losses.

Nature of loss	Date of discovery	Location	Amount, Actual or Estimated (prior to application of any deductible)
			\$
			\$
			\$
			\$
			\$

Unless the information has already been provided, please attach full details of the circumstances surrounding each loss and the corrective measures taken to prevent reoccurrence.

(b) Has any Proposal for insurance of this nature been declined by any insurance company or has any policy been cancelled or renewal thereof refused? Yes ☐ No ☐

Signing this Proposal does not bind the Proposer to complete this insurance.

11 Declaration

We declare that the statements and particulars in this Proposal are true and that no material facts have been mis-stated or suppressed after enquiry. We agree that this Proposal, together with any other information supplied shall form the basis of any contract of insurance effected thereon. We undertake to inform Insurers of any material alteration of those facts occurring before completion of the contract of insurance.

A material fact is one which would influence the acceptance or assessment of the risk.

For and on behalf of all Insureds:

Signed	Date
X	/ /

Title	Company

Please enclose with this Proposal form

Your latest Annual Report & Accounts or audited Financial Statement.

Any other attachments which support you answers in this Proposal.

If you have answered 'No' to any question please provide details of what alternative control procedure you have in place. If the question is not applicable please indicate such and do not leave the answer blank.