

Network Security

PROPOSAL FORM

Important

Please answer all questions from each section and complete in block capitals. Tick the appropriate boxes where necessary and supply any further information requested. If there is insufficient space to complete any answer, please continue at the end of this form or on a separate sheet of paper. Whilst we ask for your website address this in no way derogates from your duty of utmost good faith in answering this proposal form. Even if some or all of the answers can be given by reference to your website, you should nonetheless set out your full answers here and also provide us with any other material information. Please take all reasonable care to answer all of the questions honestly and to the best of your knowledge. If you do not answer the questions correctly, your policy may be cancelled and any claim rejected or not fully paid. The completion and signature of this proposal does not bind the proposer or Travelers Insurance Company Limited to complete a contract of insurance. Please refer to the policy wording for details of the cover provided.

General Information

1. (a) Full name of proposer including trading names if any <i>(if not a limited company include full names of partners)</i>	Date established
(b) Registered address	Postcode
(c) Correspondence address <i>(if different from the above)</i>	Postcode
(d) Occupied as	
(e) Website address	

Risk Details

2. Please detail which of the following Personally Identifiable Information (PII) records are held along with the approximate number of records you hold for each.

(a) Credit or debit card details	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Number <input type="text"/>
(b) National Insurance Numbers	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Number <input type="text"/>
(c) Customer information (e.g. address, date of birth)	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Number <input type="text"/>
(d) Medical / health information	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Number <input type="text"/>
(e) Third party corporate information	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Number <input type="text"/>

3. Do you outsource any part of your IT network including data storage, data hosting and data processing in respect of PII records?

Yes No

(a) If "Yes" please give details of the estimated percentage outsourced %

(b) If "Yes" do you have a written contract with these third parties that indemnifies you for any IT system or data security breaches arising from their services?

Yes No

4. Do you use encryption tools to ensure the confidentiality and integrity of all PII records including those outsourced or on portable electronic equipment and removable media? Yes No

5. Does your business continuity plan and disaster recovery plan include:

(a) procedures to be followed in the event of a breach that involves information security or data? Yes No

(b) Alternative options for outsourcing providers in the event of your original provider being incapacitated? Yes No

6. Please provide an estimate of the length of time it would take to restore your operations following a computer attack or other corruption or loss of data

Up to ½ a day Up to 1 day More than 1 day

If "More than 1 day" please advise

7. Please provide an estimate of the length of time after which the inability of your staff to access your computer systems would have a significant impact upon your business

Immediately After 6 hours After 12 hours

After 24 hours After 48 hours

8. Do you have a dedicated IT manager? Yes No

If "No" who has responsibility for this function?

9. Do you have a bring your own device (BYOD) policy which is clearly communicated to all staff and which includes protocols for the encryption of data stored away from your network? Yes No

10. Do you implement a data protection / privacy policy for all staff who come into contact with PII records which is clearly communicated to all? Yes No

11. How often do you perform audits to ensure compliance with your data protection / privacy policies?

Annually Bi-annually Never

Other - please advise

12. Do you have a formal procedure for end of lifecycle destruction of paper and deletion of electronic records? Yes No

13. Is a login ID and password required to access secure areas of your website? Yes No

If "Yes" please advise

(a) Are such access rights granted only to those with specific need for such access? Yes No

(b) Do you have documented procedures for user ID and password management? Yes No

14. Within the last 5 years has a third-party audit / assessment of your network and security processes and practices been undertaken? Yes No

Date of last third party audit Type of audit / assessment

Were any vulnerabilities discovered as a result of the third party audit or assessment? Yes No

If "Yes" please advise what steps have been taken to address the vulnerabilities that were identified

Security of your Network

15. (a) Do you have a firewall installed on all external gateways and anti-virus software installed on all internal and external servers and gateways? Yes No
- (b) Are all updates and security related patches installed in accordance with the manufacturer's recommended time frame? Yes No
- (c) Is all critical data backed up at least weekly and stored securely off-site (including encryption of any PII records)? Yes No
- (d) Is the integrity of all back-ups verified on at least a monthly basis? Yes No

Loss History

16. Within the past 5 years have you sustained any systems intrusion, virus attack, hacking incident, data theft or any similar event? Yes No
If "Yes" please advise what steps have been taken to minimise a recurrence of such an event

17. Within the past 5 years have you notified customers or employees that their PII records may have been compromised? Yes No
If "Yes" please advise what steps have been taken to minimise a recurrence of such an event

18. After enquiry, is the proposer or any of the partners, directors or employees aware of any pending loss or circumstance which may give rise to a loss? Yes No
If "Yes" please provide full details

Declaration

Must be signed by a Partner or Director

I/We declare that to the best of my/our knowledge or belief, the statements and particulars given in this proposal are true and complete and that no material facts that are likely to influence the acceptance and assessment of this proposal have been withheld. (If you are in any doubt as to whether a fact is material, you should disclose it.)

I/We agree to inform Travelers Insurance Company Limited of any change to any material fact.

I/We also declare that if any information on this proposal has been written by another person on my/our behalf, that person acted as my/our agent for that purpose.

I/we have read the above and declare that to the best of my/our knowledge and belief the statements are true and complete.

Signature of the proposer
(Partner/Director)

	Date
--	------

Print name and position held

--

For and on behalf of
(Insert name of Company/Firm)

--

NO COVER IS IN FORCE UNTIL THIS PROPOSAL HAS BEEN ACCEPTED BY THE COMPANY AND THE PREMIUM PAID, EXCEPT AS PROVIDED BY AN OFFICIAL COVERING NOTE ISSUED BY THE COMPANY.

PLEASE RETAIN A COPY OF THIS COMPLETED PROPOSAL FORM FOR YOUR RECORDS.

Using Personal Information

How we treat information about you and your rights under the Data Protection Act 1998

Travelers Insurance Company Limited may collect certain personal information about our policyholders, prospective policyholders, any person connected to policies held by our policyholders, or connected to prospective policyholders ('Data Subjects').

Data

In order to provide cover under an insurance policy, to assess or pay a claim we need to collect and process personal information about:

- a) the person or property that we are being asked to insure,
- b) any third-party claimant, i.e. someone making a claim against our customer,
- c) property - for which repair or replacement costs are being sought under our customer's insurance policy - belonging to our customer or a third-party.

We will seek different information depending upon the kind of insurance cover we are being asked to provide or the kind of claim we are being asked to assess or pay.

Some of the information we collect may be classified as 'sensitive personal data', which is information that may contain information about physical or mental health, religious beliefs and criminal and disciplinary offences (including convictions).

Purpose

Personal information or sensitive personal data may be collected and or used in a number of ways including: -

- a) considering an application for insurance,
- b) underwriting or binding of an insurance policy,
- c) conducting our relationship with policyholders and persons associated with such policies, including third party claimants,
- d) policy administration,
- e) claims administration,
- f) preventing and detecting fraud, including providing information to the relevant authorities.

Third Parties and Jurisdiction

In the case of policies that have been issued, we may pass information to members of the Travelers group, our reinsurers, professional advisers, loss adjusters or agents if necessary for the performance of the insurance contract or as required by law (including providing the information to government or regulatory authorities). This may involve the transfer of your information to countries which do not have data protection laws equivalent to those in the European Union in which case we shall ensure that the information is appropriately protected. In particular, medical information may be processed in the United States of America for the purposes of assessing and processing a claim.

We may also share the information with, and obtain information about you and/or your employees or agents from credit reference agencies and/or fraud prevention agencies.

Claims Data

Insurance companies share claims data:

- a. to ensure that more than one claim cannot be made for the same personal injury or property damage,
- b. to check that claims information matches what was provided when insurance cover was taken out, and
- c. when required, to act as a basis for investigating claims when our recorded information is incorrect or when we suspect that insurance fraud is being attempted.

You should provide us with the correct information if you are making a claim under your own policy or, if you are a third party, a policy held by one of our customers.

Marketing

With consent of the data subject, personal data may be processed for the purposes of marketing similar goods and services. Data subjects will be asked to provide any necessary consent at the time their data is collected, but are able to subsequently opt out of any marketing at any time.

Please note that the provisions relating to consent, and subsequent opt-out, do not apply to corporate entities (which includes their employees).

Right of access and correction

Data subjects have a right of access to, and correction of, information that we hold about them. If they would like to exercise either of these rights, they should contact our Data Protection Compliance Officer at:

Travelers Insurance Company Limited
Exchequer Court
33 St Mary Axe
London EC3A 8AG

By providing personal information you agree that all persons to whom the information relates consent to the processing and transfer of information described in this notice. You also confirm that you have taken all necessary steps to inform them of disclosure of information to us for the purposes described above.

Please use this space to disclose any further relevant information or if there is insufficient space available to answer any of the questions fully, clearly identifying the question number in each case.