Allianz

Allianz Trade

Fidelity Insurance
Risk questionnaire

This questionnaire forms the basis for an offer of insurance cover and for the contractual arrangements if and when an insurance contract is concluded. All information supplied hereunder will be treated as confidential.

1 Company

Company (full legal name)

Address | Postcode/place

Contact person | E-mail

2 General information

Business activity/sector

Currency ☐ CHF ☐ EUR ☐ USD

Total Assets | Annual turnover

Has a loss been made in the last two years, or do the last annual financial statements show an over-indebtedness? ☐ Yes ☐ No

3 Structure of the company and affiliated (co-insured) companies

Firms in which the company holds a direct and indirect share of more than 50% of equity or over which it exercises a controlling influence.

Number of companies to be co-insured | In which countries?

4 People in a position of trust

Members of senior management (who individually own less than 20% of the share capital of the Company)	Switzerland	Abroad
Number of employees	Switzerland	Abroad
Of which commercial employees	Switzerland	Abroad
Number of temporary employees	Switzerland	Abroad
Number of external staff/staff of contracted companies (security, maintenance, cleaning, etc.)	Switzerland	Abroad

5 Scope of insurance

Preferred policy start date

Preferred sum insured in CHF

Requested excess/self-retention (amount per event)

Does your Company currently hold (or has held in the past) a crime insurance policy? ☐ Yes ☐ No

With which insurer? In force until

Reason for cancelation/non-renewal

6 Cyber Insurance

Does your Company currently hold (or has held in the past) a cyber insurance policy? ☐ Yes ☐ No

With which insurer? In force until

Sum insured Excess/Self-retention

7 Loss experience

Irrespective of any previous insurance:
Have crime losses (such as theft, fraud, bribery, unlawful misappropriation, damage to property/data, etc.) been discovered in the last five years? ☐ Yes ☐ No

If yes, please describe the background, perpetrator, loss amount and results of investigations, if known:

What measures were taken to prevent similar occurrences?

8 Corporate governance and auditors

Are all business activities reviewed at least once a year by external auditors? ☐ Yes ☐ No

Following the last review, were all of the external auditors' recommendations regarding internal controls implemented? ☐ Yes ☐ No

If not, please provide a detailed explanation:

9 Control systems

Does the company have an internal audit department? ☐ Yes ☐ No

Does the company always procure satisfactory, written references directly from previous employers for the three years immediately prior to hiring an employee? ☐ Yes ☐ No

Are employees with cash handling and payments/cheque processing responsibilities obliged to make daily deposits? ☐ Yes ☐ No

Do all suppliers/service providers have written contracts? ☐ Yes ☐ No

Does the company have clearly defined delegations of authority for the execution of payment transfers, specifically structured by payment amount? ☐ Yes ☐ No

Are changes to supplier data – particularly bank accounts – subject to specific control processes? ☐ Yes ☐ No
Are they recorded in writing? ☐ Yes ☐ No

Are certain areas of responsibility outsourced to external companies (e.g. accounting, IT, etc.)? ☐ Yes ☐ No

If yes, please provide details on nature and extent.

Do certain employees have company credit cards? ☐ Yes ☐ No

If yes, how many? Up to which limits?

Do identical accounting standards apply throughout the company? ☐ Yes ☐ No

Are there specific control processes for international payments? ☐ Yes ☐ No

Average amount for outgoing payments per month?

Is an independent physical count of stock, raw materials, work in progress and/or finished goods undertaken on a regular basis? ☐ Yes ☐ No

If yes, how often?

Are all administrative employees obliged to take at least two weeks of uninterrupted vacation every calendar year? ☐ Yes ☐ No

Are there control mechanisms in place for enquiries from new customers (KYC check)? ☐ Yes ☐ No

Do you have a whistleblowing service accessible to all staff? ☐ Yes ☐ No

If no, please explain what measures are available to staff in the event that they wish to raise a concern:

10 Division of responsibilities and authorities

Are duties segregated so that no individual can carry out the following activities from commencement to completion without referral to others?		
Executing payment transfers or payments of more than CHF 5,000?	☐ Yes	☐ No
Sending and receiving account statements?	☐ Yes	☐ No
Changing the bank details of suppliers/business partners?	☐ Yes	☐ No
Opening new company bank accounts?	☐ Yes	☐ No
Repaying cash and/or returning goods?	☐ Yes	☐ No

11 IT security

Are different passwords used for different levels of authorisations?	☐ Yes	☐ No
Are all access rights (both physical and to IT systems) withdrawn immediately when an employee leaves the company?	☐ Yes	☐ No
Are passwords changed at pre-defined intervals?	☐ Yes	☐ No
Does your company trade in cryptocurrencies or accept them as a valid means of payment?	☐ Yes	☐ No
Are the security warnings of the National Cyber Security Centre (NCSC) (or a comparable foreign institute) observed and are the recommended security measures implemented immediately, if necessary?	☐ Yes	☐ No
Are attacks on the IT system detected and logged through scanning, monitoring and incident response activities, so that appropriate countermeasures can be taken immediately?	☐ Yes	☐ No
Are all programs/software/IT applications protected against unauthorised changes?	☐ Yes	☐ No
Do all IT systems and Networks used by the Company have a safeguard/firewall against unauthorised access?	☐ Yes	☐ No
Is the protection/firewall updated on an ongoing basis?	☐ Yes	☐ No
Is your IT system protected by virus scanning and repair software?	☐ Yes	☐ No
Is all software updated continuously to protect against damage from viruses?	☐ Yes	☐ No
Is data secured/backed up on a daily basis, and the latest release status of each program secured/backed up?	☐ Yes	☐ No
In doing so, is a copy stored in such a way that, if the original data is hacked, the copy is unlikely to be affected at the same time?	☐ Yes	☐ No
Are the services of external cloud providers used?	☐ Yes	☐ No

12 Social engineering fraud *

If a line manager gives instructions for an above-average or unusual payment, do staff subsequently double-check it by personally consulting the line manager?	☐ Yes	☐ No
Do line managers double-check enquiries from (people who claim to be) bank employees requesting a confirmation or bank details?	☐ Yes	☐ No
Does the company personally double-check with suppliers/providers if it appears that they have given instructions to change their bank details or delivery address?	☐ Yes	☐ No
Are measures taken at the company to raise awareness of the risks of social engineering among employees?	☐ Yes	☐ No

* The term "social engineering" refers to processes by which fraudsters exploit people's willingness to help, gullibility or uncertainty in order to obtain confidential data or manipulate the victims into taking certain actions.

13 Additional notes/enclosures

By signing below, the undersigned confirms that all information is complete and truthful to the best of his/her knowledge. Missing or incorrect information can lead to the termination of the insurance contract and the release of the insurer from its obligation to pay indemnity.
All data collected will be treated strictly confidential and will not be made accessible to third parties with the exception of the involved insurers (including reinsurers).

Place/date Signature

Save Send

Version 2023/06