|  |  |  |
| --- | --- | --- |
| **1. Your business** | Your business name: |       |
|  |  |
|  | Main address: |       |
|  |  |
|  | Postcode: |       |  |
|  |  |  |  |
|  | Year business established: |       |  |
|  |  |  |
|  |  |  |  |
|  | Website: |       |
|  |  |  |
| 1.1 Subsidiary or associated companies | Do you require cover for any subsidiary or associated companies? | Yes [ ]  No [ ]  |
| If Yes, you must ensure that all other information you give in this proposal form incorporates that for the subsidiary or associated companies, including income and claims information. |
|  | Subsidiary details: |
|  | Subsidiary name | Address  | Turnover derived from entity | Connected to corporate entity  |
|  |       |       |       | Yes [ ]  No [ ]  |
|  |       |       |       | Yes [ ]  No [ ]  |
|  |       |       |       | Yes [ ]  No [ ]  |
|  |  |
| 1.2 Your employees | Your total number of employees (including subsidiaries):  |       |
|  |  |
| 1.3 Security | Do you have someone in charge of information security (e.g. CISO)? |
|  | Yes | [ ]  | No | [ ]  |  |
|  | Internal | [ ]  | External | [ ]  |  |
|  | Full time | [ ]  | Part time | [ ]  |  |
|  |  |
| 1.4 Business activities | In the last 12 months, have you or any of your subsidiaries agreed to, begun or completed a merger, acquisition or consolidation? |  |
| Yes [ ]  No [ ]  |
|  |  |
| 1.5 Your income  | Please provide your turnover including fee income: |
|  | Region | Current year turnover  | Projected year turnover  |
| United Kingdom  | £      | £      |
| European Union  | £      | £      |
|  | USA and Canada  | £      | £      |
|  | Rest of the World  | £      | £      |
|  | Web Sales | £      | £      |
|  |  |
| 1.6 Personal data | How many records do you hold, process or transact? Please split into the following categories:  |
|  | Type of data | Number of records | Percentage USA/Canada |
|  | Personal data |       |      % |
|  | Personal health data |       |      % |
|  | Biometric or genetic data |       |      % |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Personal financial data |       |      % |
|  | PCI (payment card information) |       |      % |
|  | Third-party confidential corporate information |       |      % |
|  |  |
|  | a. | Are you GDPR-compliant? | Yes [ ]  No [ ]  |
|  | b. | If you have international subsidiaries, do you ensure they comply with local data protection legislation? | Yes [ ]  No [ ]  N/A [ ]  |
|  | c. | Do you have a fully implemented data retention and deletion policy? | Yes [ ]  No [ ]  |
|  | d. | Do you share data with any third parties? | Yes [ ]  No [ ]  |
|  |  | If Yes to 1.6 d., do you: |  |
|  |  | i. | obtain express consent from the data subject? | [ ]  Yes [ ]  No |
|  |  | ii. | ensure an appropriate contract is in place with the third party which contains a hold harmless clause or indemnity from the third party for claims that may arise from a personal data breach or misuse of the data provided to them? | Yes [ ]  No [ ]  N/A [ ]  |
|  | e. | How much do you spend on IT security on an annual basis? |       |
|  |  |  |  |
| 1.7 Payment card information | If you accept credit or debit card payments in your facilities or via the web, please answer the following questions: |  |
|  | a. | are you GDPR-complaint? | Yes [ ]  No [ ]  |
|  | b. | are you compliant with the most recent applicable Payment Card Industry Data Security Standards (PCI DSS)? | Yes [ ]  No [ ]  N/A [ ]  |
|  |  | If Yes to 1.7 b: |  |
|  |  | i. | please select certification level:  |  |  |
|  |  |  | level 1 (6m+ annual transactions) | [ ]  |  |
|  |  |  | level 2 (1m-6m annual transactions) | [ ]  |  |
|  |  |  | level 3 (20k-1m annual transactions) | [ ]  |  |
|  |  |  | level 4 (0-20k annual transactions) | [ ]  |  |
|  |  | ii. | when was your last assessment? |   /  /      |
|  |  | iii.  | do you outsource all of your payment processing? | Yes [ ]  No [ ]  |
|  |  | iv.  | do you ever store or transmit credit card details on your network, even momentarily? | Yes [ ]  No [ ]  |
| 1.8 Accreditation information | What security standards has your organisation been accredited with any information security standards? |
|  | Cyber Essentials [ ]  Cyber Essentials Plus [ ]  ISO 27001 [ ]  NIST CSF [ ]   |
|  |  |
|  |  |
| **2. Security controls** | a. | Do you have a formal password policy that explains good password hygiene, such as not using obvious or repeated passwords, for all systems providing access to personal or confidential information? | Yes [ ]  No [ ]  |
|  | b. | Do users of your computer system have least privilege access based on their role? | Yes [ ]  No [ ]  |
|  | c. | Do you have a policy to ensure access is immediately revoked or amended for joiners, movers and leavers? | Yes [ ]  No [ ]  |
|  | d. | How many administrator accounts do you have in your active directory?  |       |
|  | e. | Do you utilise multi-factor authentication for all remote, privileged, administrator and supplier access to your computer system? MFA is defined as a multi-step login process that requires users to enter more information than just a username and password to gain access to your computer system. Users are required to enter an additional factor to prove their identity by using a security key, one time password provided to them via text message (SMS) or an application, or biometric data.    | Yes [ ]  No [ ]  |
|  | f. | Do you have a policy preventing employees from connecting to your computer system via a personal device? | Yes [ ]  No [ ]  |
|  | g. | Do you ensure employees undergo training, which covers, as a minimum, data privacy, phishing and IT security, at least annually, to increase knowledge and awareness? | Yes [ ]  No [ ]  |
|  | h. | Do you update all systems within 14 days of a high, important or critical patch first being made available by the relevant software (including operating system) provider? | Yes [ ]  No [ ]  |
|  | i. | Are incident logs monitored on a regular basis? | Yes [ ]  No [ ]  |
|  | j. | Do you have a formal change control policy for major systems including testing, authorisation, change control and rollback procedures? | Yes [ ]  No [ ]  |
|  | k.  | Is data encrypted: |  |
|  |  | i. | at rest? | Yes [ ]  No [ ]  |
|  |  | ii. | in transit? | Yes [ ]  No [ ]  |
|  |  | iii. | on back-ups? | Yes [ ]  No [ ]  |
|  |  | iv. | on portable devices? | Yes [ ]  No [ ]  |
|  | l.  | Do you utilise: |  |
|  |  | i. | SIEM (security incident and event management) software? | Yes [ ]  No [ ]  |
|  |  | ii. | PAM tool (privileged access management tool)? | Yes [ ]  No [ ]  |
|  |  | iii. | intrusion detection and prevention software? | Yes [ ]  No [ ]  |
|  |  | iv. | threat intelligence? | Yes [ ]  No [ ]  |
|  |  | v. | endpoint protection? | Yes [ ]  No [ ]  |
|  |  | vi. | MDM (mobile device management)? | Yes [ ]  No [ ]  |
|  |  | vii. | pen testing at least annually? | Yes [ ]  No [ ]  |
|  |  | viii.  | vulnerability scanning regularly | Yes [ ]  No [ ]  |
|  | If you have answered No to any of the above, please provide additional information as to what systems, policies or procedures you do have in place: |
|  |       |
|  |  |

|  |  |
| --- | --- |
| **3. Third-party access**  | Only complete if you have access to third-party computer networks or systems or provide services to third parties via API – e.g. SaaS). |
|  | a. | Is there a maintained inventory of all APIs?  | Yes [ ]  No [ ]  |
|  | b.  | Do you assess API configurations for misconfigurations and vulnerabilities? | Yes [ ]  No [ ]  |
|  | c. | Do you configure all API requests to pass through a Layer 7 firewall? | Yes [ ]  No [ ]  |
|  | d. | Which of the following security controls are in place on your APIs (tick box): |  |
|  |  | packet inspection | [ ]  |  |
|  |  | whitelisting – blacklisting | [ ]  |  |
|  |  | rate limiting | [ ]  |  |
|  |  | input validation | [ ]  |  |
|  |  | logging and monitoring | [ ]  |  |
|  |  | encryption | [ ]  |  |
|  |  | behavioural based detection | [ ]  |  |
|  | e. | What authentication methods or mechanisms are used to authorise API requests? |
|  |  |       |
|  | f. | Is there an identity and access management (IAM) system used to define and enforce access control to the API? | Yes [ ]  No [ ]  |
|  |  |  |
| **4. Outsourcing**  | a. | Do you outsource any of your information processing or operational systems? | Yes [ ]  No [ ]  |
|  |  | If Yes, please provide details of what functions you outsource below: |
|  |  | Outsource service provider  | Service they provide  | Due diligence undertaken | Contractual indemnity for data breach or network loss | Annual audits undertaken  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  |  |       |       | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  | Yes [ ]  No [ ]  |
|  | b. | When a critical vulnerability is identified, do you conduct due diligence on companies who hold or process your data on your behalf to ensure they do not have an exposure or if they do, do you ensure it has been patched in accordance with vendor guidelines? | Yes [ ]  No [ ]  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **5.** **Business interruption** | a. | Are full system back-ups taken at least weekly and stored either off site or disconnected from your network? | Yes [ ]  No [ ]  |
|  | b. | Do you test the efficacy of your back-ups, including but not limited to their ability to be restored, at least once every six months? | Yes [ ]  No [ ]  |
|  | c. | Do you have a business continuity plan (BCP), disaster recovery plan (DRP) and/or incident response plan (IRP) that takes account of loss of system functionality and/or loss of data? |  |
|  |  | BCP [ ]  DRP [ ]  IRP [ ]  No [ ]  |  |
|  | d. | Are they tested at least annually? | Yes [ ]  No [ ]  |
|  |  | If No, when was it last tested? |   /  /      |
|  | e. | Does your business continuity plan (BCP), disaster recovery plan (DRP) and/or incident response plan (IRP) take into account a failure of your critical providers? | Yes [ ]  No [ ]  |
|  |  | If No, how would you be able to continue to trade? |
|  |  |       |
|  | f. | What are your recovery point objectives (RPO) and recovery time Objectives (RTO) for critical systems? |
|  |  | RPO:  |
|  |  | 0-1 hour [ ]  1-4 hours [ ]  4-8 hours [ ]  8-12 hours [ ]  12-24 hours [ ]  48+ hours [ ]  |
|  |  | RTO:  |
|  |  | 0-1 hour [ ]  1-4 hours [ ]  4-8 hours [ ]  8-12 hours [ ]  12-24 hours [ ]  48+ hours [ ]  |
|  | g. | How immediate is a loss of revenue likely to be suffered? |
|  |  |       |
|  | h. | Do you have any operational technology? (Operational technology is the use of hardware and software to monitor and/or control physical processes). | Yes [ ]  No [ ]  |
|  |  | If so, is the operational technology and information technology segregated? | Yes [ ]  No [ ]  |
|  |  | If No, how do you prevent lateral movement of malware from one environment to another? |  |
|  |  |       |
|  | Please confirm the answers provided to questions **5. Business Interruption** also apply to the operational technology. | Yes [ ]  No [ ]  |
|  | If the answers to questions differ please provide information below: |
|  |       |
|  |  |
| **6.** **Crime**  | Optional, only complete this section if crime cover is required.Cover required (tick boxes): |
|  | a. | financial social engineering fraud (transferring of funds to a fraudster) | Yes [ ]  No [ ]  |
|  | b. | client social engineering fraud (your customer transfers of funds to a fraudster which you were meant to receive) | Yes [ ]  No [ ]  |
|  | c. | dishonest acts by employees (a dishonest, fraudulent or malicious act by an employees alone or acting in collusion) | Yes [ ]  No [ ]  |
|  | d. | loss of assets (the loss, destruction or damage to the businesses money, securities or property from an actual or attempted theft) | Yes [ ]  No [ ]  |
|  | e. | electronic theft (the criminal taking or misappropriation using electronic means of money, securities, or property belonging to you) | Yes [ ]  No [ ]  |
|  | f. | fraudulent use of your identity (the fraudulent or dishonest use of the electronic identity of your business) | Yes [ ]  No [ ]  |
|  | g. | telephone toll fraud (fraudulent use of phoneline, VOIP or mobiles) | Yes [ ]  No [ ]  |
| 6.1. Employee information | a. | Location | Number of employees | Number of locations | Wage roll for last financial year |
|  |  | United Kingdom |       |       |       |
|  |  | European Union |       |       |       |
|  |  | USA and Canada |       |       |       |
|  |  | Rest of world |       |       |       |
|  | b. | Do you have purchasing, stock, inventory, payroll and accounts payable procedures and controls in place, that are consistent across all of your locations and audited annually? | Yes [ ]  No [ ]  |
| 6.2 Funds transfers | a. | What is the approximate number of funds transfers to third parties in the past year? |       |
|  |  |  |
|  | b. | Please confirm the average and maximum value of funds you transfer? |       |
|  |  |  |
|  | c. | What is the minimum funds transfer value that requires dual authorisation? |       |
|  |  |  |
|  | d. | When you receive a change of supplier or customer bank details do you verify this by a call back to a known contact? | Yes [ ]  No [ ]  |
|  | e. | Do you check invoices against the purchase order and authorised supplier list prior to authorising payment? | Yes [ ]  No [ ]  |
|  | f. | Are all employees with payment authority trained to spot and prevent fraud including payment diversion fraud? | Yes [ ]  No [ ]  |
|  | g. | Are all funds transfers undertaken via your banks online service which requires multifactor authentication to access the account? | Yes [ ]  No [ ]  |
|  | h. | Are payments ever accepted using ‘cardholder not present’ method? | Yes [ ]  No [ ]  |
|  |  | If Yes: |  |
|  |  | i. | what is the maximum value you will accept via this method? |       |
|  |  | ii. | do you ensure funds have cleared before issuing goods? | Yes [ ]  No [ ]  |
| 6.3 People and supplier management  | a. | Do you perform pre-employment reference checks for all employees? | Yes [ ]  No [ ]  |
| b. | Do you have a procedure that allows employees to report suspicious activities? | Yes [ ]  No [ ]  |
|  | c. | Do you have a system in place to detect ghost employees? | Yes [ ]  No [ ]  |
|  | d. | Are wages checked against personnel records to ensure that there are no past or fictitious employees or excessive payments on the monthly basis? | Yes [ ]  No [ ]  |
|  | e. | Are employees who receive cash in their role required to bank monies received on the day of receipt? | Yes [ ]  No [ ]  |
|  | f. | Do you have a centralised supplier list? | Yes [ ]  No [ ]  |
|  | g. | Do you have a policy which has been distributed to all employees regarding conflicts of interest and gifts? | Yes [ ]  No [ ]  |
|  | h. | Is any one individual permitted to: |  |
|  |  | i. | process financial transactions and disburse assets? | Yes [ ]  No [ ]  |
|  |  | ii. | open a bank account? | Yes [ ]  No [ ]  |
|  |  | iii. | set up a new payee? | Yes [ ]  No [ ]  |
|  |  | iv. | authorise supplier payments and reconciling supplier accounts? | Yes [ ]  No [ ]  |
|  |  | v. | deposit or withdraw funds and reconcile bank statements with customer accounts or supplier accounts? | Yes [ ]  No [ ]  |
|  |  | vi. | conduct due diligence and appoint new suppliers? | Yes [ ]  No [ ]  |
|  |  | vii. | to award a contract or tender? | Yes [ ]  No [ ]  |
|  |  | viii. | issue a refund over £1,000? | Yes [ ]  No [ ]  |
|  |  | If the answer is Yes to any of the above, please provide additional information: |
|  |  |       |
| 6.4 Stock and physical controls | Please confirm values of the following: |
|  | Maximum value per location during business hours | Maximum value per location outside of business hours | Maximum value in transit |
|  | Money |       |       |       |
|  | Stock, materials, works in progress or scrap |       |       |       |
|  | Precious metals or jewellery |       |       |       |
|  | Registered securities |       |       |       |
|  | a. | Is there controlled access to all locations? | Yes [ ]  No [ ]  |
|  | b. | Are all locations connected to an intruder alarm? | Yes [ ]  No [ ]  |
|  |  | If Yes, are the connected to a police station or central monitoring system? | Yes [ ]  No [ ]  |
|  | c. | How often are stock checks completed? |       |
|  |  |  |  |
|  | d. | Do you have an internal audit committee or department? | Yes [ ]  No [ ]  |
|  |  | If Yes, please confirm the total number of employees in the committee or department: |  |
|  |  |       |
|  |  | Do they: |  |
|  |  | i. | monitor the effectiveness of their internal controls and report to the board? | Yes [ ]  No [ ]  |
|  |  | ii. | audit all locations annually? | Yes [ ]  No [ ]  |
|  |  | iii. | audit all cash management procedures? | Yes [ ]  No [ ]  |
|  |  | iv. | carry out random checks? | Yes [ ]  No [ ]  |
|  | e. | Do external auditors audit all locations at least annually? | Yes [ ]  No [ ]  |
|  | f. | Have all recommendations by external auditors been complied with since your last audit? | Yes [ ]  No [ ]  N/A [ ]  |

|  |  |  |
| --- | --- | --- |
|  |  | If No, please provide details of outstanding actions: |
|  |  |       |
|  |  |
| **7. Claims, losses and circumstances** | a. | Have you suffered any loss or has any claim, whether successful or not, been made against you? | Yes [ ]  No [ ]  |
|  | b. | Are you aware of anything that may lead to a claim, loss or other liability that might be covered under the policy? | Yes [ ]  No [ ]  |
|  | c. | Have you ever been investigated in respect of personal data, including but not limited to payment card information, or your privacy practices? | Yes [ ]  No [ ]  |
|  | d. | Have you been asked to supply any regulator or similar body with information relating to personal data or your privacy practices? | Yes [ ]  No [ ]  |
|  | e. | Have you ever been asked to sign a consent order or equivalent in respect of personal data or privacy practices? | Yes [ ]  No [ ]  |
|  | f. | Have you ever received a complaint relating to the handling of someone’s personal data? | Yes [ ]  No [ ]  |
|  | If you have answered Yes to any of the above, please specify details (attach additional information if required): |
|  |       |
|  |  |
| **8.** **Cover required** | Please indicate the limit required:  |
|  |       |
|  | Excess requested: |
|  |       |
|  |  |
| **9. Declaration** | Please read the declaration carefully and sign at the bottom. |
|  |  |
| 9.1 Material information | In deciding whether to accept the insurance and in setting the terms and premium, we have relied on the information you have given us.You must:  |
|  |  | give a fair presentation of the risk to be insured (a fair presentation is one which clearly discloses in a reasonably clear and accessible manner all material facts which you (including your senior management and those responsible for arranging this insurance) know or ought to know following a reasonable search); |
|  |  | take care when answering any questions we ask by ensuring that all information provided is true, accurate and complete; and |
|  |  | conduct a reasonable search of information available (including information held by third parties) and disclose all material facts and circumstances in a reasonably clear and accessible manner, whether or not those facts and circumstances are the subject of a specific question in this proposal form. |
|  | **A material fact or circumstance is one which is likely to influence our acceptance or assessment of this proposal. If you are in any doubt as to what constitutes a material fact or circumstance you should consult your insurance broker.** |

|  |  |
| --- | --- |
| 9.2 Using your personal information | Hiscox is a trading name of a number of Hiscox companies. The specific company acting as a data controller of your personal information will be listed in the documentation we provide to you. If you are unsure you can also contact us at any time by telephoning 01904 681198 or by emailing us at dataprotectionofficer@hiscox.com. We collect and process information about you in order to provide insurance policies and to process claims. Your information is also used for business purposes such as fraud prevention and detection and financial management. This may involve sharing your information with, and obtaining information about you from, our group companies and third parties such as brokers, loss adjusters, credit reference agencies, service providers, professional advisors, our regulators or fraud prevention agencies. We may record telephone calls to help us monitor and improve the service we provide. For further information on how your information is used and your rights in relation to your information please see our privacy policy at www.hiscox.co.uk/cookies-privacy. |
|  |  |
| 9.3 Declaration | I/we confirm that the information given in this proposal form and any supplementary information provided is true, accurate and complete.I/we have made a fair presentation of the risk and have disclosed all facts and circumstances which would be material to your acceptance or assessment of the risk in a reasonably clear and accessible manner, whether or not those facts or circumstances were the subject of a specific question in this proposal form. I/we confirm that I/we have conducted a reasonable search of the information available to me/us (including information held by third parties) in order to reveal those facts and circumstances. If there are any material facts or circumstances not covered by a specific question on this proposal form, I/we have listed these on a separate sheet of paper which is signed and dated and attached to this proposal form.I/we understand that if I/we deliberately or recklessly failed to present the risk to you fairly, you may treat this insurance as if it never existed and refuse to make any payment under it. I/we understand that I/we must reimburse all payments already made by you and that you will also be entitled to retain all premiums paid. I/we understand that if I/we failed to present the risk to you fairly but that failure was not deliberate or reckless, the remedy available to you will depend upon what you would have done if I/we had made a fair presentation of the risk. I/we understand that you may:  |
|  |  | treat this insurance as if it never existed and refuse to make any payment under it. I/we must reimburse all payments already made by you. You will refund any premium I/we have paid; or |
|  |  | amend the terms and conditions of this insurance and apply those amended terms and conditions from the start of the period of insurance. I/we understand that this may result in a particular claim or loss not being paid. I/we will reimburse you for any payment already made that would not have been paid if such terms had been in effect; and/or |
|  |  | reduce the amount of any claim in proportion to the premium that you would have charged if I/we had fairly presented the risk to you. I/we understand that this remedy may apply in addition to those shown in b. above. |
|  | Please note that the signing of this proposal form does not bind you to complete or us to accept this insurance.The person signing this proposal form is duly authorised to do so on behalf of the proposer. |
|  |       |
|  | Name of director/officer/board member/senior manager |
|  |  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |   /  /      |
|  | Signature of director/officer/board member/senior manager |  | Date |
|  |  |
|  | **A copy of this proposal should be retained for your records.** |
| 9.4 Complaints | Hiscox aims to ensure that all aspects of your insurance are dealt with promptly, efficiently and fairly. At all times Hiscox are committed to providing you with the highest standard of service. If you have any concerns about your policy or you are dissatisfied about the handling of a claim and wish to complain you should, in the first instance, contact Hiscox Customer Relations in writing at:Hiscox Customer RelationsThe Hiscox BuildingPeasholme GreenYork YO1 7PRor by telephone on 0800 116 4627/01904 681 198or by email at customer.relations@hiscox.com.Where you are not satisfied with the final response from Hiscox, you also have the right to refer your complaint to the Financial Ombudsman Service. For more information regarding the scope of the Financial Ombudsman Service, please refer to www.financial-ombudsman.org.uk. |