Vanbreda Risk & Benefits
Plantin & Moretuslei 297
2140 Antwerpen
Tel: +32 3 217 55 20

QUESTIONNAIRE CYBER POLICY

This questionnaire allows insurer to gather the needed information to assess the risks related to the information systems of the company to be insured and to improve its offers in light of its clients' expectations. Please note that completing this questionnaire does not bind insurers nor the applicant company to conclude an agreement. However, the applicant company is bound to fairly complete this questionnaire. If the Information Systems Security Policy of the companies/subsidiaries to be insured varies from a company to another, please complete the questionnaire by each of them

1 IDENTIFICATION OF THE APPLICANT COMPANY

Company name

Address | Zip, City

Website(s) | Number of employees

Annual Turnover | Annual Gross Margin

Percentage of turnover generated from US/Canada: | EU: | Rest of World:

2 PROFILE OF THE COMPANY/COMPANIES TO BE INSURED

2.1 Activity to be insured

[Please describe the main activities of the company/companies to be insured. If these activities include e-commerce, please indicate the pourcentage of turnover generated]

2.2 Scope

[The companies and subsidiaries to be insured. If the company has subsidiaries outside EU, please provide the details]

2.3 Criticality of the Information Systems

[Please assess the outage period over which your company will suffer significant impact on its business.]

Application (or Activity)	Maximum outage period before adverse impact on business (RTO)				
	Immediate	> 12 h	> 24 h	> 48 h	> 5 days

2.4 Property insurance on all risk basis

[Please complete this section only if you expect property insurance on all risk basis.]

	Value (K€)
Fix equipments including IT infrastructure:	
Mobile equipments:	

3 INFORMATION SYSTEMS

	< 100	101 - 1000	> 1000
Number of Information Systems users			
Number of Laptops			
Number of Servers			

	YES	NO
Do you have an e-commerce or an online service website? If yes :	☐	☐
What is the revenue share generated or supported by the website? (estimate)	(% or M€)	

4 INFORMATION SYSTEMS SECURITY (ISS)

	4.1 Security Policy and risk management	YES	NO
1	An ISS policy is formalized and approved by the company management and/or security rules are defined and communicated to all staff and approved by the staff reprensentatives	☐	☐
2	Awareness training to the ISS is provided regularly to the users	☐	☐
3	You identified critical information systems risks and implemented appropriate controls for their mitigation	☐	☐
4	Regular audits of the ISS are conducted and audits recommendations are implemented	☐	☐
5	You inventory and classify information ressources according to their criticality and sensitivity and security requirements are defined accordingly	☐	☐

	4.2 Information systems protection	YES	NO
1	Access to information systems requires users identification and authentication, and password renewal and hardening	☐	☐
2	Access authorizations are based on user roles and a procedure for authorizations management is implemented according to the principle of least privilege	☐	☐
3	Secured configurations references are defined for workstations, laptops, servers and mobile devices	☐	☐
4	Centralized management and configuration monitoring of computer systems are in place	☐	☐
5	The laptops are protected by personal firewall	☐	☐
6	An antivirus software is installed on all systems and antivirus updates are monitored	☐	☐
7	The security patches are regularly deployed	☐	☐
8	A Disaster Recovery Plan is implemented, tested and, if necessary, updated at least annually	☐	☐
9	Data backups are performed dialy, backups are tested regularly and a backup copy is placed regularly in a remote location	☐	☐

	4.3. Network security and operations	YES	NO
1	Traffic filtering (firewall) between the internal network and internet is updated and outgoing and incoming traffic is monitored regularly	☐	☐
2	Intrusion detection/prevention system is implemented, updated and monitored regularly	☐	☐
3	Internal users have access to the Internet web sites browsing through a network device (proxy) equipped with web antivirus and websites filtering	☐	☐
4	A segmentation of the network is implemented to separate the critical areas (servers, administration ..) from less critical areas (such as users area …)	☐	☐

5	Penetration testing is conducted regularly and a remediation plan is implemented	☐	☐
6	Vulnerability assessment is conducted regularly and a remediation plan is implemented	☐	☐
7	Procedures for incident management and change management are implemented	☐	☐
8	Security events (as virus detection, access attempts…) are logged and monitored regularly	☐	☐
9	A proactive monitoring against network intrusions is implemented and security events and alerts are prioritized and handled accordingly	☐	☐

	4.4. Physical security of computing room	YES	NO
1	Critical systems are placed in at least one dedicated computer room with restricted access and operational alarm postponed to a monitoring location	☐	☐
2	The Datacentre hosting critical systems has resilient infrastructure (redundancy of power supply, air conditioning, network connections …)	☐	☐
3	Critical systems are duplicated according Active/Passive or Active/Active architecture …	☐	☐
4	Critical systems are duplicated on two separate premises	☐	☐
5	Fire detection and automatic fire extinguishing system in critical areas are implemented	☐	☐
6	The power supply is protected by a UPS and batteries which are both maintained regularly	☐	☐
7	Power is backed up by an electric generator which is maintained and tested regularly	☐	☐

	4.5. Outsourcing	YES	NO
	[Please fill in if a function of the information system is out sourced]		
1	The outsoucing contract includes security requirements that should be observed by the service provider	☐	☐
2	Service Level Agreements are defined with the outsourcer to allow incident and change control and penalties are applied to the service provider in case of non compliance with the SLA	☐	☐
3	Monitoring and steering committee(s) are organized with the service provider for the management and the improvement of the service	☐	☐
4	You have not waived recourse against your service provider(s)	☐	☐

What are the outsourced Information Systems functions?	YES	NO	Service Provider (Outsourcer)
Desktop management	☐	☐	
Server management	☐	☐	
Network management	☐	☐	
Network security management	☐	☐	
Application management	☐	☐	
Use of cloud computing or Software as a service)?	☐	☐	
Other, to specify please:			

5 PERSONAL DATA HELD BY THE ORGANIZATION

5.1. Type and number of records

The Number of personal information records held for the activity to be insured : Total :

Per region : Europe(EU): USA/Canada: Rest of World:

categories of personal data collected/processed	YES	NO	Number of records
Commercial and marketing information	☐	☐	
Payment Card or financial transactions information	☐	☐	
Health information	☐	☐	

Other, to specify please :

Do you process data for : ☐ your own purpose ? ☐ on behalf third party ?

	5.2. Personal information protection policy	YES	NO
1	A privacy policy is formalized and approved by management and/or personal data security rules are defined and communicated to the concerned staff	☐	☐
2	The legal aspects of this policy are validated by the Legal Service and compliance with laws and regulations for the protection of personal data is monitored regularly	☐	☐
3	Awareness and training are provided to the personnel authorized to acces or process personal data	☐	☐
4	A personal data protection officer is designated in your organization	☐	☐
5	A confidentiality agreement or a confidentiality clause in the employment contract is signed by the concerned staff	☐	☐
6	Your practices of personal information processing have been audited by an external auditor, within two years	☐	☐
7	A Data Breach Response plan is implemented and communicated to the response team	☐	☐

	5.3. Collection of personal data	YES	NO
1	You notified to the Data Protection Authority (DPA) the personal data processing involved by your activity and you obtained the DPA authorization	☐	☐
2	You posted a privacy policy on your website which has been reviewed by a lawyer/legal department	☐	☐
3	You requested the consent of individuals before collecting their personal data and the concerned persons can access and if necessary correct or delete their personal data	☐	☐
4	In case of marketing operations, the concerned people are provided with an easy mean to opt out	☐	☐
5	You don't transfer Personal Data to third parties	☐	☐
	If data is transferred to third parties, please answer the following		
6	The third party (e.g processor) has a contractual obligation to process personal data only on your behalf and under your instructions	☐	☐
7	The third partly has a contractual obligation to set up sufficient security measures to protect personal data	☐	☐

	5.4. Personal information protection controls	YES	NO

1	Access to personal data is restricted to only those users who need it to perform their task and access authorizations are reviewed regularly	☐ ☐
2	Personal data is encrypted when stored into the information systems and personal data backups are encrypted	☐ ☐
3	Personal data is encrypted when transmitted over the network	☐ ☐
4	Mobiles and Laptops' hard disks are encrypted	☐ ☐
5	The copy in removable storage or the email transmission of non encrypted personal data, are prohibited	☐ ☐

		YES	NO
	The personal records you hold contain **Payment Card Information** (PCI)	☐	☐

	< 20K	20K to 1M	1M to 6M	> 6M
If Yes Number of card transactions per year	☐	☐	☐	☐

1	The payment processor (yourself or third party) is PCI DSS compliant If No :	☐	☐
2	PCI is stored encrypted or only a part of payment card numbers is stored	☐	☐
3	PCI retention time does not exceed the duration of payment and legal/regulatory requirements	☐	☐
4	Payment card data processing is externalized , If Yes :	☐	☐
5	You require the payment processor to indemnify you in case of security breach	☐	☐
6	Please indicate payment processor name, PCI retention time and any additional security measures :		

5.5. Incidents

[Please provide the incidents that had a significant impact regarding personal data during the last 12 months.]

Date	Description of the incident

Comment:

Person to contact for additional information

Name	
Title	
Phone	
E-Mail	
Completed by	

The undersigned hereby certifies that all statements made in this questionnaire are complete and correct. Any changes that happen after submission of the questionnaire or during the term of the insurance should be notified to the insurerimmediately.

The personal data relating to the signatory (name, surname, function and signature) are mandatory and will be processed by the insurer for the assessment of the company application. These data will be processed by the authorized underwriters and personnel of the insurer in charge of the management of Data Risks Protection applications and offers.

Signatory Name	Function
Date	Signature

6 DEFINITIONS

You :
The company/companies to be insured

Your :
of the company/the companies to be insured

Personal data :
Any computerized information relating to an individual who is or can be identified, directly or indirectly. e.g. name,surname, email address, phone number, function, family situation, credit card information ...
Information relating to a company are not personal data (e.g. the company turnover is not a personal data).

Record :
It is all the personal information that concern one individual. The number of records in a file of personal data corresponds to the number of individuals concerned in this file.

Sensitive data :
racial/ethnic origins;political/philosophical/religious opinions or trade union affiliation of persons, data relating to their health or sexual life, social security number, data relating to criminal offences and convictions, data relating to social difficulties of persons,biometric data.

Data Subject/Person concerned :
Any individual whose personal data are collected/processed by the company to be insured (e.g. clients, prospects, internet users..) EXCEPT its own employees.

Data Processing :
Any operation or set of operations carried out on computerized personal data. E.g. The management of clients implies to collect personal data relating to clients, to enter them in a computer, to store them on servers.

Data Protection Authority :
A data protection authority is an independent body which is in charge of: • monitoring the processing of personal data within its jurisdiction (country, region or international organization); • providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data; • hearing complaints lodged by citizens with regard to the protection of their data protection rights.

The right to information :
Anyone who implements personal data collection/processing must inform data subjects of: • the identity of the controller, • the purpose of collecting information, • the compulsory or optional nature of the responses, • the consequences of the lack of response, • recipients of information, • the rights of the person (to access, correct or delete his personal data), • any transfer of data to a country outside the European Union

PCI DSS : Payment Card Industry Data Security Standard
A Data Security Standard for Payment Card Information protection. The sensitive card payment information to be protected is card number, expiration date, cryptogram and card holder name.

PCI DSS level
The merchants are classified into four PCI DSS levels depending of card transactions volume over a 12 month volume period.

Level 1 : Merchants processing over 6 million card transactions annually

Level 2 : Merchants processing over 1 to 6 million card e-commerce transactions annually

Level 3 : Merchants processing over 20000 to 1 million card e-commerce transactions annually

Level 4: Merchants processing less than 20000 card e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually