Privacy and Data Breach Protection

Modular application form

Instructions

The Hiscox Technology, Privacy and Cyber Portfolio Policy may be purchased on an a-la-carte basis. Some organizations may require coverage for their technology errors and omissions, while others only have a privacy/security exposure. As such, coverages designed to respond to various needs may be purchased on an individual basis, or combined in a single policy.

The table provided in section one of this application allows you to specify the coverages for which you are applying. Please check the box as appropriate and fill out the applicable application section noted in the last column of the table.

All applicants must complete sections 1 and 5 of this application.

Additional information

Please also supply the underwriters with the following information in addition to your application:

1. Loss runs for the last five years (if you currently carry coverage).
2. If any pending or prior litigation, please provide details regarding the issues at hand; including demand amounts, name of the plaintiff, amount of any settlements or payouts, and steps taken to mitigate similar issues in the future.
3. If you have coverage currently in place, please provide the Declarations Page of your current policy in order to evidence existing prior acts coverage. Any newly purchased coverage will be bound with a retroactive date of inception.

Coverage information

Coverage type	Coverage description
Privacy/Network Security	Privacy Protection provides insurance coverage for claims made against you that typically arise from your failure to protect sensitive information, including subsequent actions by a regulator.
Breach Costs	Breach Costs coverage provides insurance for the typical costs that you could incur arising from the failure to protect personal information. Coverage only applies to a breach first discovered by you during the policy period.
Multimedia	Multimedia Protection provides insurance coverage for claims made against you that arise from the content of your website, social media and other promotional material.
Hacker Damage	Hacker Damage coverage provides insurance for the costs to repair or replace your website, intranet, network, computer system, programs, or data following a hacking event.
Cyber Business Interruption	Cyber Business Interruption provides insurance coverage for your losses resulting from a hacker impairing the availability of your website, intranet, network, computer system, programs or data.
Cyber Extortion	Cyber Extortion provides insurance coverage for the costs of expert assistance and the payment of a ransom in the event that a hacker threatens to damage your website, intranet, network, computer system, any programs you use or data.

Application

If a policy is issued, it will provide coverage only for claims that are first made against the Insureds and reported to the Insurer during the policy period, or any extended reporting period, if applicable; or first party events first discovered by the Insured and reported to the Insurer during the policy period, or any extended reporting period, if applicable.

Notice: This application is for insurance in which the policy limit available to pay judgments or settlements shall be reduced by amounts incurred for defense costs. Further note that amounts incurred for defense costs shall be applied against the retention amount.

HISCOX

Privacy and Data Breach Protection
Modular application form

Section 1

1. Applicant details

Applicant name:

Address:

State: Zip code:

Website:

Subsidiaries for which you seek coverage, to be incorporated into this application (entities in which you directly or indirectly own more than 50% of the assets or outstanding voting shares or interests). Please specifically note the country for any subsidiaries located outside of the United States.

2. Prior coverage

Please indicate if you currently carry similar coverage:

Insurance carrier/coverage	Limit	Retention	Premium	Retroactive date
	$	$	$	

3. Cover required

Please indicate cover required:

US $1,000,000 ☐ US $2,000,000 ☐ US $3,000,000 ☐ US $4,000,000 ☐

US $5,000,000 ☐ US $10,000,000 ☐ Other – specify: $

Retention requested: $

Coverage type	Please check desired coverage modules	Required application section(s)*
Privacy/Network Security	☐	**2**
Breach Costs	☐	**2**
Cyber Extortion	☐	**2**
Multimedia	☐	**3**
Hacker Damage/Data Restoration	☐	**2, 4**
Cyber Business Interruption	☐	**2, 4**

***All applicants must complete sections 1 and 5**

4. Gross revenue*

Past full year ending / /	Current year	Estimate for coming year
$	$	$

*Inclusive of subsidiaries from item 1 above. Healthcare entities, please use net patient revenue. Not-for-profits, please use annual budget.

HISCOX

Privacy and Data Breach Protection
Modular application form

5. Claims details*

Please check the box which applies:

a) Have **You** suffered any **First Party Loss** or has any **Claim**, including for breach of contract, whether successful or not ever been made against **You**? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

b) Are **You** aware of any matter which is likely to lead to **You** suffering a **First Party Loss** or a **Claim**, including for breach of contract, being made against **You**? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

c) Have **You** ever been subject to any complaints, including cease and desist orders concerning the content of **Your** website, advertising materials, social media or other publications or broadcasts? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

d) Have **You** ever been subject to an inquiry, investigation or action by any regulatory body or administrative agency? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

e) Has any customer or client alleged financial loss resulting from **Your** business activities over the last five years? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

* **You/Your**, **First Party Loss**, and **Claim** have the meaning as defined in the policy form. If you do not have a copy, please obtain from your insurance advisor.

6. Material dependencies

a) Do you utilize the services of independent contractors or subcontractors to perform your business activities? Yes ☐ No ☐

If Yes, please answer the following three questions

i) Do you always utilize a written contract with independent contractors/ subcontractors? Yes ☐ No ☐

ii) Do you require independent contractors/subcontractors to carry their own professional liability insurance? Yes ☐ No ☐

iii) What percentage of your business activities are contracted out? ____ %

b) Please identify any material supplier (not including utility services, telecommunication services and internet service providers) upon whom you depend to conduct your business activities:

Type	Supplier name	Written contract in place?	Are you able to contractually recover for direct losses arising from the failure of their services including from a data breach?
Data center/ co-location		Yes ☐ No ☐	Yes ☐ No ☐
Cloud computing		Yes ☐ No ☐	Yes ☐ No ☐
Payment processing		Yes ☐ No ☐	Yes ☐ No ☐
Records storage		Yes ☐ No ☐	Yes ☐ No ☐
Managed IT services		Yes ☐ No ☐	Yes ☐ No ☐
Other		Yes ☐ No ☐	Yes ☐ No ☐

HISCOX

Privacy and Data Breach Protection
Modular application form

Section 2 - Privacy and Security

7. Security history*

Please check the box which applies:

a) Have **You** ever been investigated in respect of the safeguards for sensitive information, including but not limited to protected health information, credit card information, or **Your** privacy practices? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

b) Have **You** ever reported any issues relating to a breach of healthcare information to the Office of Civil Rights or other similar regulatory body? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

c) Have **You** ever received complaints about how someone's personally identifiable information has been collected, used or handled? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

d) In the past five years, have **You** experienced a system intrusion, hacking incident, data theft, malicious code attack, cyber extortion threat or denial of service attack? Yes ☐ No ☐

If Yes, please specify details (attach additional information).

* **You/Your** has the meaning as defined in the policy form. If you do not have a copy, please obtain from your insurance advisor.

8. Regulatory

Please check the box which applies:

a) Have you confirmed your compliance with the following:

Payment Card Industry Data Security Standards (PCI/DSS) Yes ☐ No ☐ N/A ☐

PCI/DSS Certification Level: 1 ☐ 2 ☐ 3 ☐ 4 ☐ Date of last assessment: ☐

Health Insurance Portability and Accountability Act (HIPAA) Yes ☐ No ☐ N/A ☐

Gramm-Leach-Bliley Act (GLBA) Yes ☐ No ☐ N/A ☐

Drivers Privacy Protection Act (DPPA) Yes ☐ No ☐ N/A ☐

California's Song-Beverley Act and similar state statutes regarding the collection and use of personal information Yes ☐ No ☐ N/A ☐

Red Flag Rules Yes ☐ No ☐ N/A ☐

Other: ☐ Yes ☐ No ☐ N/A ☐

9. Privacy/security practices

Please check the box which applies:

a) Is there an individual in your organization specifically assigned responsibility for your privacy and security practices? Yes ☐ No ☐

b) Is there an individual in your organization specifically assigned responsibility for monitoring changes in statutes and regulations related to your handling and use of sensitive information? Yes ☐ No ☐

c) Do you have a written, published privacy policy? Yes ☐ No ☐

d) Has the privacy policy been reviewed by a suitably qualified attorney? Yes ☐ No ☐

e) Has a third-party audited your privacy practices in the last two years? Yes ☐ No ☐

f) Have you identified, located and secured all sensitive information in your care, custody or control? Yes ☐ No ☐

g) If applicable, do you contractually indemnify your customers/clients for costs they incur as a result of a breach suffered by you? Yes ☐ No ☐

h) Do you have formalized data destruction procedures in place for data and documents no longer needed by **your** organization? Yes ☐ No ☐

i) What is your sensitive data retention policy? How long do you retain personally identifiable information?

Hours: ☐ Days: ☐ Weeks: ☐

Months: ☐ Years: ☐ Indefinitely: ☐

10. Sensitive information

Please provide the type and amount of information (in both electronic and non-electronic form) you process or store. If you do not know exact amounts, please provide estimates;

Type of sensitive information transmitted, processed or stored:

A) number of records transmitted or processed per year

B) maximum number of records stored at any one time

Social security number or individual taxpayer identification number	A)	
	B)	
Financial account record (e.g. bank accounts)	A)	
	B)	
Payment card data (e.g. credit or debit card)	A)	
	B)	
Drivers license number, passport number or other state or federal identification number	A)	
	B)	
Protected health information (PHI)	A)	
	B)	
Other - Please specify:	A)	
	B)	

11. Encryption/compensating controls

Please check the box which applies:

a) Regarding the sensitive information in item 14 above, do you encrypt this information:

While at-rest in your databases/on your network? Yes ☐ No ☐ N/A ☐

In internal and external email transmissions? Yes ☐ No ☐ N/A ☐

On wireless networks? Yes ☐ No ☐ N/A ☐

In file transfers? Yes ☐ No ☐ N/A ☐

On mobile computing devices including laptops and smart phones? Yes ☐ No ☐ N/A ☐

On mobile storage devices including USB flash drives and DVDs? Yes ☐ No ☐ N/A ☐

Other: ☐ Yes ☐ No ☐ N/A ☐

b) In lieu of or in addition to encryption, what compensating controls have you implemented to protect any sensitive information that you process, transmit or store:

12. Security controls

Please check the box which applies:

a) Have you installed and do you maintain a firewall configuration to protect data? Yes ☐ No ☐

b) Do you regularly scan your network for weaknesses, including for SQL injection vulnerabilities? Yes ☐ No ☐

c) Do you use anti-virus software and regularly apply updates/patches? Yes ☐ No ☐

d) Do you have a defined process implemented to regularly patch your systems and applications? Yes ☐ No ☐

e) Have you installed and do you maintain an Intrusion Detection System (IDS) to monitor your network for malicious activities or policy violations? Yes ☐ No ☐

f) Have you installed and do you maintain a Data Loss Prevention (DLP) system to identify, monitor, and protect sensitive data while in use, in motion, and at rest on your network? Yes ☐ No ☐

g) Have you installed physical controls to protect sensitive systems and sensitive, physical information under your care, custody or control? Yes ☐ No ☐

Please provide details regarding any measures you have taken to protect and secure your network and sensitive information (both in digital and physical form):

13. Payment card information

a) Do you accept credit card payments in your facilities or via the web? If yes, please answer the following four questions. Yes ☐ No ☐

b) Do you outsource all of your payment processing? Yes ☐ No ☐

c) If you outsource payment processing, do you require the processor to indemnify you for their security breaches? Yes ☐ No ☐

d) Do you ever store or transmit credit card details on your network? Yes ☐ No ☐

e) Do you ensure that credit card details are masked or encrypted at all times when stored, displayed, or transmitted from your system? Yes ☐ No ☐

14. Backup storage controls

a) Is all sensitive information stored on back up tapes/cassettes/disks, etc. encrypted as a standard practice? Yes ☐ No ☐

b) If you maintain your own backup tapes/cassettes/disks, etc., are these stored in a physically secured location? Yes ☐ No ☐

c) If you utilize any third-party transportation or storage company, do you require them to indemnify you if they lose your data or your data is breached while in their care, custody or control? Yes ☐ No ☐

15. Access control

a) Do you track and monitor all access to sensitive information on your network? Yes ☐ No ☐

b) Do you restrict access to all sensitive information stored by you on a business need-to-know basis? Yes ☐ No ☐

c) Do you have procedures in place to restrict or remove login credentials of employees immediately following an employee's departure from your organization? Yes ☐ No ☐

Please proceed to any subsequent section for which you wish to apply, otherwise please proceed to Section 5.

Section 3 - Multimedia

16. Media exposures and controls

Please check the box which applies:

a) Do you have written clearance procedures in place regarding use, licensing, and consent agreements for third party content used by you on your website or in your promotional materials? Yes ☐ No ☐ N/A ☐

b) Do you have written guidelines for your use of social media and its use by your employees? Yes ☐ No ☐ N/A ☐

c) Does your website feature opt in/opt out procedures when collecting individual users' information? Yes ☐ No ☐ N/A ☐

d) Has legal counsel verified that your domain names(s) and meta tags do not infringe on any third party's copyright or trademark? Yes ☐ No ☐ N/A ☐

e) Do you solicit/promote your business via unsolicited email blasts? Yes ☐ No ☐ N/A ☐

f) Do you host any user-generated content or social media networks? Yes ☐ No ☐ N/A ☐

If yes, have you ensured DMCA policies/protections are in place? Yes ☐ No ☐ N/A ☐

g) Do you have a formalized take-down procedure for comments or content placed on your social media sites by third-parties? Yes ☐ No ☐ N/A ☐

Please provide details regarding any publishing or broadcasting you perform beyond advertising your own business (e.g. publishing of a trade journal):

Please proceed to any subsequent section for which you wish to apply, otherwise please proceed to Section 5.

Section 4 - Business Interruption and Hacker Damage

17. Redundancy

Please check the box which applies:

a) Do you maintain redundant backups of sensitive and critical system information? Yes ☐ No ☐ N/A ☐

b) Do you have backups stored off-site? Yes ☐ No ☐ N/A ☐

c) Are restore procedures documented and tested? Yes ☐ No ☐ N/A ☐

d) Do you have scheduled backup procedures in place? Yes ☐ No ☐ N/A ☐

How often is sensitive information backed up?

Daily ☐ Weekly ☐ Monthly ☐ Annually ☐

e) Do system backups reside with third-parties? Yes ☐ No ☐ N/A ☐

How quickly can you obtain backups stored by third-parties?

24-hours ☐ One week ☐ One month ☐ Unknown ☐

18. Business interruption

a) For Cyber Business Interruption only, what is your average revenue generated through your website or network?

Daily ☐ Weekly ☐ Monthly ☐

Section 5 - Execution

Please provide us with details of any other information which may be material to our consideration of your application for insurance. If you have any doubt over whether something is relevant, please let us have details. Feel free to attach an addendum to this application if insufficient space is provided below:

Notice to New York applicants: any person who knowingly and with intent to defraud any insurance company or other person, files an application for insurance containing any false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

Declaration

I declare that (a) this application form has been completed after reasonable inquiry, including but not limited to all necessary inquiries of my fellow principals, partners, officers, directors and employees, to enable me to answer the questions accurately and (b) its contents are true and accurate and not misleading.

I undertake to inform you before the inception of any policy pursuant to this application of any material change to the information already provided or any new fact or matter that may be material to the consideration of this application for insurance.

I agree that this application form and all other information which is provided are incorporated into and form the basis of any contract of insurance.

Signature of Principal/Partner/Officer/Director as authorized representative of the Applicant

Date (mm/dd/yyyy)

NOTE: Hiscox policyholders may qualify for various complimentary value-added services. Please provide the contact details of the individual who may be contacted by Hiscox or its partners regarding these services:

Name: Phone:

Email:

A copy of this application should be retained for your records.