

CYBER COVER  
PROPOSAL FORM



4 3 7 1 5 5 7 3 5 5 6 2 7 1 8 9 6 3 4 5

7 4 3

4 7 8

3 4 0

5 3 9

5 7

0 3

4 5 4 6 5 9 8

**NIG**

7 0 4 3 8 0

2 4

6 6 9 2 7 3 5 7 9

**CYBER**

3 6 8 5 4 4

7 9 4 2 0 3 4

8 3

0 7

4 1 4 9 6 3 0 7 0

**COVER**

7 8

7 0 6

9 4

7 7

3 4

3 6 5 0 3

4 4 6

4 7 4

1 0 0

8 6 4 5 9 1 7 2 8

7 7

2 3





## F Section 5 – Hardware

Cover required

Yes  No

a Computer equipment, servers and network infrastructure at the premises

Yes  No

New replacement value: £

b Portable computer equipment (laptops, palmtops, tablets, smartphones)

Yes  No

New replacement value: £

c Electronic office equipment (TVs, video/dvd equipment, conference equipment, shredders, faxes, photocopiers)

Yes  No

New replacement value: £

## G Section 6 – Data Corruption and Extra Cost

Cover required

Yes  No

Limit for each occurrence required

£

Indemnity period required

months

(12 months is the standard period)

## H Excesses

	Standard excesses	Please indicate below if a different Excess/Time Excess is required:
Sections 5 & 6 (Hardware, data corruption and extra cost):		
Fire, lightning, explosion, aircraft	£0	
Smartphones	£50	
All other occurrences	£100	
Claims under section 1 (Cyber crime):	£100	
Claims under section 2 (Cyber liability):	£1,000	
Claims under section 3 (Data-breach expense):	£1,000	
Claims under section 4 – (Cyber Event Loss of Business Income)		
Time excess:	6 hours	

## I Your Business and IT infrastructure

a Company type (sole trader / partnership / limited company / subsidiary company):

b What are your usual business working hours (daily/weekly)?

c Number of employees:

d Annual business income:

e Is your information security management system certified to ISO 27001? Yes  No

If no, are you working towards ISO 27001 certification? Yes  No

f Are you using the 'Cyber Essentials' scheme guidelines to help improve the security of your computer systems? Yes  No

g Do you outsource any data storage or hosting of any systems (for example, outsourced email system or cloud storage provider)? Yes  No

(If yes, please tell us who your Service Providers are and where their servers are located)

h Do you take credit/debit card payments? Yes  No

(If yes, which payment processor do you use?)

i Do you or your Service Providers transfer data outside of the European Economic Area (EEA)? Yes  No

j If you or your Service Providers do transfer data outside of the EEA, do the countries where you transfer data to have strict legislation in place concerning data privacy similar to the Data Protection Act in the UK?

k Are all of your servers located in a purpose built server room? Yes  No

(If no, please provide details of where they are located)

l Please describe what security and environment protection you have in place for your servers:

m Are data back-ups taken at least every 7 days? Yes  No

(If no, please tell us how often you back-up data and how these back-ups are stored)

n Are all PCs and servers protected with up-to-date anti-virus software with updates at least every 7 days? Yes  No

(If no, please tell us how you protect your computer system from viruses and hacking)

## I Your Business and IT infrastructure *continued*

**o** Do you have a firewall in place which controls access to your network? Yes  No

**p** Do you have an email and internet usage policy that has been shared with all your employees? Yes  No

(If **no**, please tell us how your business manages internet usage and prevent access to inappropriate or potentially damaging websites)

**q** Please tell us details of any IT support companies which you currently use:

**r** Have you ever had an IT security audit carried out by an external company? Yes  No

(If **yes**, please provide details of who carried out the audit, when it was completed, what were the recommendations and have they been implemented)

**s** Do you allow your employees to access your computer system from home or other offsite locations? Yes  No

(If **yes**, please tell us how you manage and control access to make sure your network is secure)

Please complete the sections for which you require cover:

## J Section 1 – Cyber Crime

**a** When recruiting new employees do you undertake background checks before employment is offered (Criminal Record Bureau (CRB), Identity, Qualifications, Disciplinary)? Yes  No

(If **no**, please tell us what background checks you use instead)

**b** Do you have controls in place (such as limited access and unique passwords) to prevent access to company payment processes and bank accounts? Yes  No

**c** Do you have a computerised telephone system? Yes  No

(If **yes**, please tell us what security measures are in place to prevent unauthorised access to your telephone system. For example: the system is password protected and the password has been changed and set by you)

## K Section 2 – Cyber Liability & Section 3 – Data-Breach Expense

- a** If you store personal data or credit and debit card information, please provide an estimate of how many individuals this relates to: (for example, how many card transactions do you process per year)

- b** Please provide details of any data encryption you use to protect sensitive data (particularly when sending to third parties, storing on portable devices or transferring to portable media such as flash drives or disks):

Please tell us about the type of data you hold by ticking the boxes which apply to you from the following categories:

- c** Business to business information with personal data relating to employees only Yes  No

(For example manufacturing / wholesaling with no information relating to retail customers i.e. no credit / debit card information or bank account information)

- d** Business to customers Yes  No

(For example retail with bank account details, credit and debit card information but no NI numbers, passport numbers or health information)

- e** Professional services Yes  No

(For example passport numbers, personal information such as health care information, legal profession, property rental information, housing associations, financial status information)

- f** Education Yes  No

(For example schools / universities, personal information relating to young people)

- g** Local authorities / medical profession Yes  No

(For example councils, hospitals, doctors surgeries, healthcare clinics)

- h** Does your business do any of the following?

- Operate a website for business purposes Yes  No
- Publish online marketing material such as on a website or by email Yes  No
- Electronic publishing, marketing, distribution of copyrighted material of others Yes  No
- Use social media such as Facebook or Twitter to promote your business Yes  No

(If **yes**, please provide details about how you manage and control business usage. For example, how you use these, what type of information do you publish, are your employees allowed to upload content or use online chat, how do you control and check the information before it is published).

**K** Section 2 – Cyber Liability & Section 3 – Data-Breach Expense *continued*

**n** Are you responsible for any corporate data that is protected under confidentiality agreements? Yes  No

**o** If someone claims that information you have published is damaging to their reputation or breaches intellectual property rights or claims you have used their copyrighted material, do you have procedures in place to take action? Yes  No

(For example does your business have 'take-down' procedures in place?)

**p** Do you have connections with any legal or professional IT company who would be able to assist you with liability claims and investigations relating to liability which would be insured by this section? Yes  No

(If yes, please tell us who they are)

**q** Do you have a Chief Information Officer / Chief Security Officer who is responsible for data security and privacy issue? Yes  No

**r** Do you have a comprehensive and fully documented data privacy and information security policy and do you provide staff training on data privacy and security? Yes  No

**s** Do you have a hardware destruction policy to protect data when documents are disposed of or hardware / drives are sold to third parties or where they are being disposed of at the end of their useful life? Yes  No

**L** Section 4 – Cyber Event Loss of Business Income

**a** How quickly would you suffer a loss of income as a result of a failure of your computer system? Hours  Days

**b** Do you generate income directly via a website? Yes  No

**c** If you do generate income via a website, how reliant are you on that website to generate income?

**d** Please tell us how reliant you are on your computer system to generate revenue:

**e** Please tell us how reliant you are on third party / hosted / outsourced computer systems to generate revenue:

**f** Please comment on recovery and contingency plans which you have in place to avoid business interruption due to IT system failure, and/or alternative working arrangements:

**g** Are your plan/s regularly tested and updated? Yes  No



**M** Section 5 – Hardware (and software)

**a** Briefly describe the computer equipment and network setup

(For example PCs and servers connected by a network)

**b** If you need cover for portable computer equipment, what type of portable computer equipment do you have?

(For example laptops, palmtops, tablets and smartphones etc.)

**c** Briefly describe the software and operating systems you use, particularly those which are specialised or important to your business:

**d** Please provide full address & postcode for the sites where computer equipment is kept which is owned, leased or occupied by you?

**e** Other than portable equipment, do you require cover for any hardware/software which is not located at premises owned, leased or occupied by you?

Yes  No

(If **yes**, please provide address details and details of who owns/occupies those premises)

**f** Please provide brief details if any premises owned, leased or occupied by you:

**i** is not built of brick, stone or concrete with tile, asphalt, metal or concrete roof

**ii** is not occupied solely as offices and/or the area occupied communicates with any trade premises

**iii** has a history of flooding or water damage (including internal pipes/tanks)

**iv** allows access to the general public or other tenants have access to areas occupied by you. (If other tenants have access, please tell us who they are and how access is restricted.)

**g** Please provide brief details of security measures which are in place at your premises (for example: alarms, CCTV, types of window and door locks, shutters).

(If you have multiple premises, please tell us what protections are specific to each location)

## **M** Section 5 – Hardware (and software) *continued*

**h** Please provide brief details of fire protections you have in place at your premises

(E.g. automatic fire alarms, smoke and heat detection, gas suppression systems, sprinklers, fire doors and fire resistant construction etc specific to each location)

## **N** Section 6 – Data Corruption and Extra Cost

**a** Briefly describe the functions of your internal IT network and what type of data you hold:

**b** What operating systems do you use?

**c** Please provide a general overview of your network security and the measures you have to make sure data is secure:

**d** Briefly describe your data backup procedures:

**e** Provide details of any warm start / hot start facility or alternative computer systems or premises which you could use to continue operating if your own premises or computer system was unavailable:

## **O** General information

**a** How long have you been in business?

**b** During the last 5 years, have you or any director, officer or key person, whether in your/their name, the name of the Business proposed or in the name of any other business in which any of you have had an interest, had any claims or incidents that could have resulted in a claim under this policy?

For example, claims or incidents relating to:

**i** Hardware / software damage or data loss

Yes

No

**ii** Loss of income as a result of computer system issues

Yes

No

**iii** Financial crime or fraud, theft of money or assets online or telephone system hacking

Yes

No

**O** General information *continued*

iv Claims or complaints from third parties against you for data privacy, intellectual property or reputational damage issues.

Yes  No

(If yes, please tell us about these claims or incidents in the table below)

Date of claim or incident	Brief details of claim or incident	Total amount of loss arising from the claim or incident

c Have you or any director, officer or key person, whether in your/their own name, in the name of the Business proposed or in the name of any other business in which any of you have had an interest:

- i been refused insurance or had any special term(s) or condition(s) imposed by an insurer in the last 5 years? Yes  No
- ii been convicted of or have any prosecution pending for any criminal offence(s) (for example criminal damage, arson, fraud, theft or handling stolen goods)? Yes  No
- iii been convicted of or have any prosecution(s) pending for any offence involving insurance fraud? Yes  No
- iv gone into bankruptcy, insolvency, liquidation, receivership or a similar procedure in the last 5 years or have such a procedure pending? Yes  No
- v been criticised, fined, disciplined, suspended or expelled by any industry, trade association or regulatory body or have any such procedure pending? Yes  No

If you have answered 'yes' to any of these questions then please provide full details in 'Other information'.

**P** Other information

Please use this space to tell us about any other information you think may be relevant to us in relation to your proposal for Cyber Insurance

**Q Declaration**

---

I/We declare that:

- a** if any answer has been printed or written by any other person, he/she shall be my agent for that purpose. I also confirm that any data which I have supplied in this form about other persons is given with their knowledge and authorisation
- b** to the best of my/our knowledge and belief the information given in this form is correct and complete in every detail
- c** I/we accept and conform to the terms, conditions and exceptions of the policy (a specimen of which is available on request) in the standard form issued by the Company for the Insurance now proposed and I will pay the premiums thereon.

Signature:

Name:

Date:

Your company position:



NIG policies are underwritten by U K Insurance Limited.

Registered office: The Wharf, Neville Street, Leeds, LS14AZ.

Registered in England and Wales, registration number 1179980.

U K Insurance Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

Phone calls may be recorded.

NIG101009B/05/18