Your Cyber Respond Policy

Please keep this document safe and refer to it if you need to make a claim.

If you need this document in an alternative format, please speak to your insurance adviser.

| Retirement | Investments | Insurance | Health |

AVIVA

Policy Introduction

Welcome to Aviva. We are committed to providing a first-class service. Aviva has the experience and longevity of a company who can trace its roots back to the establishment of the Hand in Hand Fire & Life Insurance Society in London in 1696.

This is your Cyber Respond Insurance policy which sets out your insurance protection in detail.

Your premium has been calculated on the basis of the extent of cover you have selected which is specified in The Schedule, the information you have provided and the declaration you have made. Please read the policy and The Schedule carefully to ensure that the cover meets your requirements.

Contents

This policy consists of individual sections. You should read this policy in conjunction with The Schedule which confirms the sections you are insured under and gives precise details of the extent of your insurance protection.

The Contract of Insurance

The contract of insurance between you and us consists of the following elements, which must be read together:

- your policy wording;
- the information contained in the Statement of Fact issued by us;
- the policy schedule;
- any notice issued by us at renewal;
- any endorsement to your policy; and
- the information under the heading “Important Information” which we give you when taking out or renewing your policy.

In return for you having paid or agreed to pay the premium, we will provide the cover set out in this policy, to the extent of and subject to the terms and conditions contained in or endorsed on this policy.

Important

This policy is a legal contract. You must tell us about any material circumstances which affect your insurance and which have occurred either since the policy started or since the last renewal date.

A circumstance is material if it would influence our judgement in determining whether to provide the cover and, if so, on what terms. If you are not sure whether a circumstance is material ask your insurance adviser. If you fail to tell us it could affect the extent of cover provided under the policy.

You should keep a written record (including copies of letters) of any information you give us or your insurance adviser when you renew this policy.

Breach of Term

We agree that where there has been a breach of any term (express or implied) which would otherwise result in us automatically being discharged from any liability, then such a breach shall result in any liability we might have under this policy being suspended. Such a suspension will apply only from the date and time at which the breach occurred and up until the date and time at which the breach is remedied. This means that we will have no liability in respect of any loss occurring, or attributable to something happening, during the period of suspension.

Terms not relevant to the actual loss

Where there has been non-compliance with any term (express or implied) of this policy, other than a term that defines the risk as a whole, and compliance with such term would tend to reduce the risk of:

- loss of a particular kind, and/or
- loss at a particular location, and/or
- loss at a particular time,

then we agree that we may not rely on the non-compliance to exclude, limit or discharge our liability under this policy if you show that non-compliance with the term could not have increased the risk of the loss which actually occurred in the circumstances in which it occurred.

Making a Claim

Should you need to make a claim under this policy, please contact us on:

0800 051 4473

In all cases, please quote your policy number.

Calls to 0800 numbers from UK landlines and mobiles are free. For our joint protection telephone calls may be recorded and/or monitored.

Complaints Procedure

What to do if you are unhappy

If you are unhappy with any aspect of the handling of your insurance Aviva would encourage you, in the first instance, to seek resolution by contacting your insurance advisor. Contact details can be found on your insurance documents.

What will happen if you complain

If your complaint is not resolved quickly:

- Your complaint will be acknowledged promptly.
- A dedicated complaint expert will be assigned to review your complaint.
- A thorough and impartial investigation will be carried out.
- You will be kept updated of the progress.
- Everything will be done to resolve things as quickly as possible.
- A written response will be sent to you within eight weeks of receiving your complaint, this will inform you of the results of the investigation or explain why this isn't possible.

Where your concerns are unable to be resolved or have not been resolved within eight weeks, you may be able to ask the Financial Ombudsman Service (FOS) to carry out an independent review. Whilst firms are bound by their decision you are not. Contacting them will not affect your legal rights.

You can contact the **FOS** on **0800 023 4567** or visit their website at **www.financial-ombudsman.org.uk**, where you will find further information.

Cyber Respond

We use some words or phrases with special meanings in this document. These will start with a capital letter each time they appear in the policy and we explain what they mean in the definitions section on page 10.

Cover

Where a Data Security Breach, Virus or Similar Mechanism, Hack, Denial of Service Attack or Cyber Extortion has first been discovered during the Period of Insurance, We will cover You for the resulting costs, necessarily and reasonably incurred with Our consent, of

(1) specialist consultants or consulting engineers to
   (a) investigate whether a Data Security Breach has occurred
   (b) mitigate any on-going loss
   (c) reinstate, recreate or restore Your data onto Data Storage Materials
   (d) repair or replace Your Computer Equipment including software and programs contained within
   (e) locate and remove a detectable Virus or Similar Mechanism contained in any of Your Computer Equipment.

(2) external legal advice to manage Your response to the cyber incident

(3) notifying any
   (a) Data Subject of the Data Security Breach
   (b) regulatory body of the Data Security Breach

   where You are required to do so by any law or regulation

(4) providing
   (a) a telephone help line to assist Data Subjects
   (b) a credit monitoring or credit protection service to the affected Data Subjects for a period of up to one year provided that the offer of such service must be accepted by the Data Subject within 12 months of the initial offer
   (c) identity fraud remediation services for Data Subjects

   after they have been notified of the Data Security Breach

(5) any additional expenditure to avoid or reduce interruption to or interference with The Business

(6) public relations consultants to provide advice to minimise adverse publicity.

The maximum We will pay in any Period of Insurance will be the Cover Limit subject to the Total Cover Limit stated in The Schedule.

External Cyber Crime (optional)

Cover

Where an act of theft, fraud or dishonesty committed by a Third Party with the deliberate intent to cause You loss is first discovered during the Period of Insurance, We will cover You for

(1) financial loss resulting from
   (a) Funds Transfer Fraud
   (b) Social Engineering Fraud
   (c) the unauthorised use of Your Computer Equipment

(2) costs and professional fees to substantiate the cause and the value of such loss, provided they are necessarily and reasonably incurred.

The maximum We will pay in any Period of Insurance will be the Cover Limit subject to the Total Cover Limit stated in The Schedule.

Theft of Personal Money

The cover under (1)(c) above is extended to cover The Insured for the loss of personal money from their personal bank account caused by a Third Party gaining unauthorised access to Your computer network.

The maximum We will pay in respect of this extension is subject to the Cover Limit and the Total Cover Limit stated in The Schedule.

Policy Conditions

Policy Conditions

The following policy conditions apply to all covers unless otherwise stated and in addition to the cover conditions contained in The Schedule.

Alteration of Risk

If there has been any alteration to The Business after the effective date of this insurance which increases the risk of loss, destruction or damage, or Your interest ceases except by will or operation of law, We will at Our option cancel the policy from the date of such alteration or when Your interest ceases, unless We accept the alteration.

Arbitration

If We accept liability but You disagree with the amount We offer to pay, the claim will be referred to an arbitrator who will be jointly appointed in accordance with statutory provisions.

Cancellation

(1) You may cancel this policy at any time after the date we have received the premium by providing at least 30 days' written notice to us.

(2) If there is a default under your Aviva credit agreement which finances this policy, we may cancel this policy by providing written notice to you in accordance with the default termination provisions set out in your Aviva credit agreement.

If your policy is cancelled under (1) or (2) above, we may, at our discretion, refund to you a proportionate part of the premium paid for the unexpired period. This is provided that, during the current Period of Insurance, there has been no:

(a) claim made under the policy for which we have made a payment

(b) claim made under the policy which is still under consideration

(c) incident which you are aware of and which is likely to give rise to a claim and which has already been, or is yet to be, reported to us

(3) Where there is no Aviva credit agreement to finance this policy, we will cancel this policy from the inception date if the premium has not been paid and no return premium will be allowed. Such cancellation will be confirmed in writing by us to your last known address.

(4) We may also cancel this policy at any time by providing at least 30 days' written notice to your last known address.

We will refund a proportionate part of the premium for the unexpired period provided that, during the current Period of Insurance, there has been no:

(a) claim made under the policy for which we have made a payment

(b) claim made under the policy which is still under consideration

(c) incident which you are aware of and which is likely to give rise to a claim and which has already been, or is yet to be, reported to us

Other Insurance

Where any loss, destruction or damage covered by this policy is also covered by another insurance policy (or would be covered if this policy didn't exist), We will only pay our proportionate share of the loss. This means We will not pay more than the percentage of the claim We are responsible for, even if the other insurer refuses the claim. We will calculate the percentage of the claim We are responsible for based on the policy limit(s) of each contributing insurer covering the same loss.

If the other policy is subject to a condition of average and this policy is not, this policy will then become subject to the same condition of average.

Discharge of Liability

We may at any time pay the Total Cover Limit or a smaller amount for which a claim can be settled after deduction of any sum already paid. We will not make any further payment except for costs and expenses incurred prior to the payment of the claim.

Fraud

If a claim made by You or anyone acting on Your behalf is fraudulent or fraudulently exaggerated or supported by a false statement or fraudulent means or fraudulent evidence is provided to support the claim, We may:

(1) refuse to pay the claim,

(2) recover from You any sums paid by Us to You in respect of the claim,

(3) by notice to You cancel the cover with effect from the date of the fraudulent act without any return of premium.

If We cancel the policy under (3) above, then We may refuse to provide cover after the time of the fraudulent act. This will not affect any liability We may have in respect of the provision of cover before the time of the fraudulent act.

If this policy provides cover to any other person other than You and a claim made by such person or anyone acting on their behalf is fraudulent or fraudulently exaggerated or supported by a false statement or fraudulent means or fraudulent evidence is provided to support the claim, We may:

(1) refuse to pay the claim,

(2) recover any sums paid by Us to You in respect of the claim (from You or such person depending on who received the sums or who benefited from the cover provided),

(3) by notice to You and such person cancel the policy provided for such person with the effect from the date of the fraudulent act without any return of premium in respect of such cover.

If We cancel a person's cover under (3) above, then We may refuse to provide cover after the time of the fraudulent act. This will not affect any liability We may have under such cover occurring before the time of the fraudulent act.

Fair presentation of risk

Important note

The Insurance Act 2015 sets out the duty on a policyholder to make a fair presentation of the risk to the insurer. This duty applies before the start of the period of insurance (including any renewal) and if any change is needed during that period.

The Act also sets out what can happen if a fair presentation of risk is not made. This can include the insurer cancelling the cover (sometimes back to its start date), keeping any premiums paid and not paying any claim in full. The wording below summarises the relevant parts of the Act. It is not intended to replace them.

If You have failed to make a fair presentation of the risk then, depending on the nature of that failure:

- We may cancel Your cover and refuse to pay any claim, or
- We may not pay any claim in full, or
- the extent of cover may be affected.

If We cancel Your cover then You will be entitled to a refund of the premium, unless We are legally entitled to keep the premium under the Insurance Act 2015.

This clause applies in addition to any provisions in this policy relating to underinsurance.

Our Rights

In the event of a claim, We may

(1) enter the Building or The Premises

(2) take possession of, or require to be delivered to Us, the Computer Equipment which We will deal with in a reasonable manner without incurring liability or reducing Our rights.

We will not pay any claim if You, or anyone acting on Your behalf, do not comply with Our requirements or hinder or obstruct Us. You are not entitled to abandon property to Us.

Reinstatement

When We decide, or are required to reinstate or replace Your data, You will at Your expense provide plans, documents, books, and/or any information which We require. We will not be obliged to reinstate data exactly but only in a satisfactory manner as circumstances allow.

The maximum amount We will pay is the Total Cover Limit.

Sanctions

We shall not provide cover nor be liable to pay any claim or provide any benefit under this policy if to do so would expose Us to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions laws or regulations of the European Union, United Kingdom or United States of America or any of its states.

Severability of Interest

If The Policyholder comprises more than one party, each operating as a separate and distinct entity, this policy shall apply in the same manner and to the same extent to each party as if they were separately and individually insured.

Provided that for the purposes of the Total Cover Limit and/or any amount payable stated in The Schedule or elsewhere in this policy (as the case may be), all of the parties insured under this policy shall be treated as one party so that there shall be a single contract of insurance between.

(1) Aviva as one party

and

(2) The Policyholder as the other party.

Subrogation

Anyone making a claim under this policy must, at Our request and expense, do everything We reasonably require to enforce a right or remedy or obtain relief or indemnity from other parties to which We will become entitled or subrogated because of payment for or making good loss, destruction, damage, accident or injury. We may require You to carry out such actions before or after We make any admission of or payment of a claim.

Policy Exceptions

Policy Exceptions

The following policy exceptions apply to all covers unless otherwise stated.

We will not provide cover in respect of

Consequential Loss

any consequential loss or liability except as provided for under Cover (5)

Cyber Operation

any loss or liability arising directly or indirectly out of a Cyber Operation that has a major detrimental impact on

(1) the functioning of a sovereign state due to disruption to the availability, integrity or delivery of an Essential Service in that sovereign state; or

(2) the security or defence of a sovereign state

If a Designated Official of a Relevant State attributes a Cyber Operation to another sovereign state, or asserts that a Cyber Operation has been carried out on behalf of or in support of a sovereign state, then for the purposes of this exception a Cyber Operation shall be deemed to have taken place, and this exception will apply. A Cyber Operation shall still be deemed to have taken place and this exception will still apply if any other sovereign state, including a Relevant State, contradicts or denies the attribution or assertion.

In the absence of attribution by a Designated Official of a Relevant State We may apply this exception in reliance on any reasonable inference as to the attribution of the Cyber Operation to another sovereign state or those acting in support of or on behalf of a sovereign state.

Defined Contingency

loss, destruction or damage to Computer Equipment software or programs caused by or consisting of a Defined Contingency regardless of any other contributory cause.

Electronic Risks

any loss arising from pre-existing faults in or the unsuitability of programs or computer systems or software unless caused by Virus or Similar Mechanism, Hack or Denial of Service Attack.

Excess

The Excess

However, the Excess will not apply in respect of initial advice provided by our Claims Service Provider.

Existing Circumstances

circumstances which, at the inception of this policy, The Insured knew or ought to have known about and which may give rise to a claim

Extortion

any payment made to a Cyber Extortionist following a Cyber Extortion.

Fines and Penalties

any fine, regulatory or statutory payment and/or any liquidated damages, or any amount payable under any penalty clause.

Fraud and Dishonesty

any fraud, dishonesty, insolvency, financial default, malicious or illegal act, by The Insured other than an Employee who is not a director acting intentionally and outside of their scope of authority.

Manufacturing and Transport

any loss arising from equipment controlling or monitoring

(1) any manufacturing or other industrial process

(2) any vehicle, aircraft or waterborne vessel

Motor Vehicle

any loss arising from or to any vehicle licensed for road use or which requires a Certificate of Motor Insurance

Nuclear

death or disablement, loss or destruction of or damage to any property, any loss or expense whatsoever, any consequential loss or any legal liability directly or indirectly caused by or contributed to by or arising from

(1) (a) ionising radiations or contamination by radioactivity from nuclear fuel or from nuclear waste from the combustion of nuclear fuel

(b) the radioactive, toxic, explosive or other hazardous or contaminating properties of any nuclear installation, reactor or other nuclear assembly or nuclear component thereof

(2) the use of any weapon or device

(a) dispersing radioactive material and/or ionising radiation, or

(b) using atomic or nuclear fission and/or fusion or other like reaction

(3) the radioactive, toxic, explosive or other hazardous or contaminating properties of any radioactive matter but this will not apply in respect of radioactive isotopes at The Premises (other than nuclear fuel or nuclear waste) used in the course of The Business for the purposes for which they were intended

Terrorism

any Damage, or the threat thereof, or any consequence resulting directly or indirectly from or in connection with any of the following regardless of any other cause or event contributing concurrently or in any other sequence to the loss

(1) Terrorism

(2) civil commotion in Northern Ireland

(3) any action taken in controlling, preventing, suppressing, or in any way relating to (1) and/or (2) above

In any action, suit or other proceedings where We allege that any Damage, or the threat thereof, or any consequence whatsoever results from (1) and/or (2) and/or (3) and is therefore not covered by this policy, the burden of proving that any such Damage, or the threat thereof, or any consequence whatsoever is covered under this policy will be upon You.

However We will provide cover for Cyber Terrorism as insured by this policy other than in respect of Damage which results directly from

(a) fire, explosion, flood, escape of water from any tank, apparatus or pipe (including any sprinkler system),

(b) impact of any aircraft or any aerial devices or articles dropped from them,

(c) impact of any sea-going or water-going vessel or of any vehicle whatsoever or of any goods or cargo carried in or on such vessel or vehicle

(d) war, invasion, act of a foreign enemy, hostilities or a warlike operation or operations (whether war be declared or not), civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power

(e) a Cyber Operation

Utility and Service Provider

any loss or liability arising directly or indirectly out of any failure, interruption, disturbance, degradation, corruption, impairment or outage of any utility provider, internet service provider, telecommunications provider, domain name service, certificate authority or content delivery network.

However, We will cover Your direct losses if such services are under Your direct operational control.

War

any consequence whatsoever which is the direct or indirect result of any of the following, or anything connected with any of the following, whether or not such consequence has been contributed to by any other cause or event

(1) (a) war, invasion, act of a foreign enemy, hostilities or a warlike operation or operations (whether war be declared or not), civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power

(b) mutiny or military uprising, martial law

(2) nationalisation, confiscation, requisition, seizure, damage or destruction by or by order of any government or any local or public authority, and

(3) any action taken in controlling, preventing, suppressing or in any way relating to (1) and/or (2) above

Policy Definitions

Policy Definitions

The following policy definitions apply to all covers unless otherwise stated. A defined word or phrase will start with a capital letter each time it appears in the policy, except when used in the sections of this policy headed 'Policy Introduction', 'Contents', 'Contact Details for Claims and Help', 'Complaints Procedure' and 'Important Information' and in headings and titles.

Claims Service Provider

The company appointed by Us to handle Your claim notification.

Computer Equipment

Mainframes, personal computers, servers, laptops, handheld computers, smartphones and other equipment including

(1) hard or solid-state drives

(2) satellite and telecommunications links and computerised telephone exchanges

(3) electronic access equipment

(4) Data Storage Materials

used for processing, communicating and storing electronic data Excluding

(a) equipment held as stock

(b) customer's equipment

(c) items whose primary purpose is surveying, measuring, metering, recording or radio communication.

Cover Limit

The maximum amount We will pay under each cover, as stated in The Schedule.

Cyber Extortion

A demand for payment as a pre-condition to resolving a Virus or Similar Mechanism, Hacking or Denial of Service Attack which, at the time the demand is made:

(1) prevents access to Data, or

(2) involves a credible threat made against You to

  (a) destroy, use or reveal to third parties Personal Data or sensitive business Data, or

  (b) cause Damage to Your Computer Equipment.

Cyber Extortionist

Any party committing or being an accessory to a Cyber Extortion

Cyber Operation

The use of any Computer Equipment by, on behalf of, or in support of a sovereign state to disrupt, deny, degrade, exfiltrate, manipulate or destroy any data or Computer Equipment in or of another sovereign state.

Cyber Terrorism

Any act or series of acts or threat thereof of any person or group of persons, whether acting alone or on behalf of or in connection with any organisation through the use of computer systems, to destruct, disrupt or subvert any computer system, computer network and/or its content, with the intention to cause harm or committed for religious, ideological or political purposes (including, but not limited to, the influencing of any government and/or to put the public in fear).

Data

All information which is electronically stored or represented, or contained on any current and back-up disks, tapes or other materials or devices used for the storage of data including but not limited to operating systems, records, programs, software or firmware, code of series of instructions.

Data Security Breach

Loss, theft or accidental release of

(1) Personal Data involving one or more Data Subjects which creates a risk of financial harm to the Data Subject or which triggers an obligation under any law or regulation to notify the Data Subject of such loss, theft or accidental release

(2) Other Data.

Data Storage Materials

Any materials or devices used for the storage or representation of Data including but not limited to disks, tapes, CD-ROMs, DVDs, memory sticks, memory cards or other materials or devices which may or may not also constitute Computer Equipment.

Data Subject

An individual who is the subject of Personal Data.

Defined Contingency

Fire, lightning, explosion, aircraft and other aerial and/or spatial devices or articles dropped from them, earthquake, riot, civil commotion, strikers, locked out workers or persons taking part in labour disturbances, storm, flood, escape of water from any tank apparatus or pipe, impact by any road vehicle or animal, theft or attempted theft.

Denial of Service Attack

Any actions or instructions with the ability to damage, interfere with, or otherwise affect the availability of Computer Equipment or Data, including but not limited to the generation of excess traffic into network addresses, the exploitation of system or network weaknesses, and the generation of excess or non-genuine traffic within, between or amongst networks.

Designated Official

Any person holding one of the following positions, or equivalent, within a sovereign state

(a) Head of government

(b) Interior minister

(c) Foreign minister

(d) Defence minister

(e) Official representative of a national intelligence or security service

Employee(s)

Any person who is

(1) under a contract of service or apprenticeship with You, borrowed by or hired to You, a labour master or supplied by a labour master, employed by labour only sub-contractors, self-employed, under a work experience or training scheme, a voluntary helper while working under Your control in connection with The Business

(2) an outworker or homeworker when engaged in work on Your behalf.

Essential Service

A service which is essential for the maintenance of critical societal or economic activities of a sovereign state, including but not limited to financial institutions and associated financial market infrastructure, transport network, health services or utility services.

Excess

The amount specified in Your policy or The Schedule which We will deduct from each and every claim. You will repay any such amount paid by Us.

External Cyber Crime

Acts of theft, fraud or dishonesty committed by a Third Party with the deliberate intent to cause You loss as a result of

(1) Funds Transfer Fraud

(2) Social Engineering Fraud

(3) the unauthorised use of Your Computer Equipment.

Funds Transfer Fraud

An electronic instruction sent to a financial institution at which You hold an account, instructing it to move a fixed amount out of Your account, without Your knowledge or consent.

Hack/Hacking

Unauthorised access to or malicious use of any computer or other equipment, component, system or item which processes, stores or retrieves data whether Your property or not.

Period of Insurance

From the effective date until the expiry date, both shown in The Schedule, or any subsequent period for which We accept payment for renewal of this policy.

Personal Data

Data which relates to a natural person who can be identified from that data which is in Your possession.

Relevant State

Any sovereign state

(1) in which the Data or Computer Equipment affected by a Cyber Operation is physically located or stored

(2) which is a permanent member of the United Nations Security Council

(3) which is a member of the Five Eyes intelligence alliance

(4) which is a member of the North Atlantic Treaty Organisation.

Social Engineering Fraud

A Third Party directly or indirectly inducing or deceiving an Employee into delivering, paying or transferring money, securities or insured property by impersonating or falsely claiming to be another person or organisation including, but not limited to, Employees, directors, creditors, clients, law enforcement agencies or financial institutions.

Terrorism

Any act or acts caused or occasioned by any person(s) or group(s) of person(s) or so claimed for political, religious, ideological or similar purposes.

The Business

Activities directly connected with the business specified in The Schedule.

The Insured

You and any director, partner or Employee of Yours

Each covered party will be subject to the terms of this policy so far as they apply. The total amount which We will pay will not exceed the Total Cover Limit stated in The Schedule regardless of the number of parties claiming to be covered.

The Premises

The premises specified in The Schedule.

The Schedule

The document(s) which specifies details of The Policyholder, The Premises, Cover Limit, Total Cover Limit, Excess(es), Period of Insurance and any Endorsements and Conditions applying to this policy.

Third Party

Any person who is not

(1) an Employee, equity partner, director or member of Yours or of a subsidiary or a parent or related or group company of Yours

(2) working in collusion with an Employee, equity partner, director or member of Yours or of a subsidiary or a parent, or related or group company of Yours

(3) an external auditor or accountant, insurance intermediary, financial adviser, factor, commission merchant, consignee or other similar agent or representative whose services are employed by You.

Total Cover Limit

The maximum amount, as stated in The Schedule, which We will pay in any Period of Insurance

All claims arising out of one cause, whether or not all such claims are made against You in the same Period of Insurance, will be treated as one claim at the time the first claim is made. Any claim subsequently arising from any circumstance notified to Us shall be deemed to have been made during the Period of Insurance in which the notice of such circumstances was first received by Us.

Virus or Similar Mechanism

Program code, programming instruction or any set of instructions with the ability to damage, interfere with, or otherwise adversely affect Computer Equipment or Data, whether involving self-replication or not, including, but not limited to trojan horses, worms and logic bombs.

We/Us/Our/Aviva

Aviva Insurance Limited.

You/Your/The Policyholder

The person, persons, company, companies, partnership, partnerships or unincorporated association, named in The Schedule as The Policyholder.

Appendix - Customer Obligations

The following Conditions apply in addition to any Conditions stated in Your policy wording. If in relation to any claim You have failed to fulfil the following conditions, We will not pay that claim.

Applicable to all Sections

Access and Passwords

Access to Computer Equipment must be authenticated by the use of individual identification and passwords. Any default or manufacturers' passwords or access codes must be changed and kept secure.

Data Backup

You must maintain adequate backup copies by backing up all data no less frequently than every 7 days. The integrity of any data backup must be validated using operating system routines or checks.

Backups must be stored securely and separately from the original data or programs by:

(a) holding a copy offline, such as backup tape or disconnected service such as a USB device or external hard drive; or

(b) using a specific cloud service that is separate from your main network; or

(c) replicating to another of your networks that is separated and disconnected from your main network.

Data Disposal

All Personal Data and other sensitive business Data must only be disposed of in a secure manner by:

(a) shredding any paper copies

(b) ensuring any Computer Equipment has all Data erased before disposal.

Protection - Firewall

You must ensure that Computer Equipment that is connected to the internet or any other external network is protected against unauthorised access by an active firewall

Protection - Software Updates

You must install any updates for firmware, operating systems, software and programs within 14 days of an update being released by the manufacturer or provider where:

(a) the update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'; or

(b) the update addresses vulnerabilities with a Common Vulnerability Scoring System (CVSS) v3 score of 7 or above.

Protection - Virus or Similar Mechanism

You must install anti-virus software and ensure that it is updated at intervals of at least once a month if not automatically and in full and effective operation at the time of a loss.

Applicable to the External Cyber Crime Section

You must

(a) ensure that Partners, directors and Employees are trained in the dangers of Social Engineering Fraud, and keep a record of such training

(b) have a documented policy, which states that details of any new payee requests or amended payment instructions are always checked verbally by using details held on file or a published website and do not solely rely on the new instruction. This policy must be accepted by all Partners, directors and Employees, with such acceptance recorded.

Aviva Insurance Limited.

Registered in Scotland, No. 2116. Registered Office: Pitheavlis, Perth, PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

BCOAG16627 10.2023