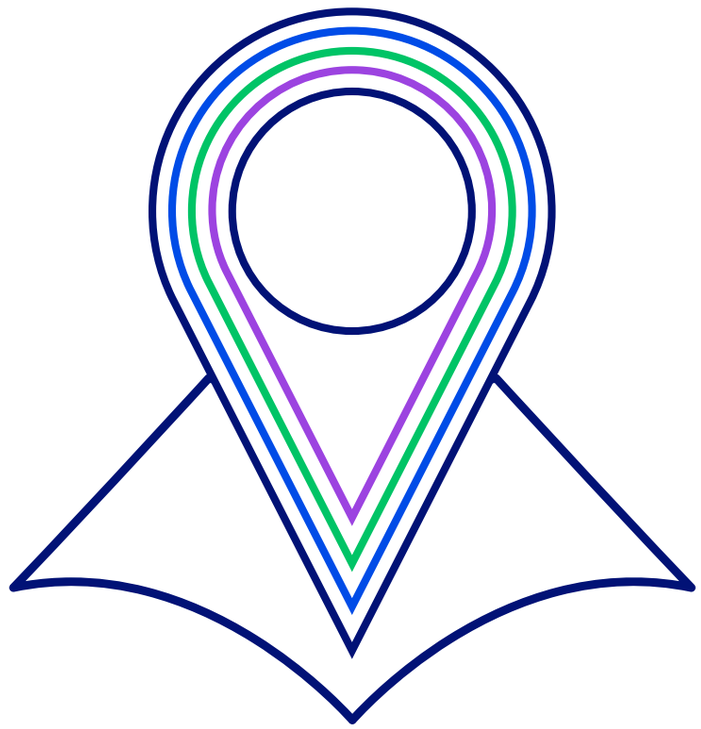
POLICY TOUR

CyberEdge Coverage

This policy tour provides a “click through” commentary of the CyberEdge wording including brand new additions, changes to existing features and general information on specific points. Please refer to the full policy wording and schedule for full details of cover, definitions, terms and conditions.

AIG®

Start



HOW TO USE THE POLICY TOUR:

Click on the icons to explore:

Information

New

Use the “NEXT” buttons to navigate directly to the next comment in the category

Select section to start

SECURITY AND PRIVACY LIABILITY COVERAGE

NETWORK INTERRUPTION COVERAGE

EVENT MANAGEMENT COVERAGE

CYBER EXTORTION COVERAGE

Security and Privacy Liability Coverage

1. Insurance Covers

1.1. Data Protection Investigation and Data Protection Fines

The Insurer will pay, to or on behalf of each Company, Loss resulting from a Regulatory Investigation first occurring during the Policy Period.

1.2. Cyber Liability

The Insurer will pay, to or on behalf of each Insured, Loss resulting from a Claim first made during the Policy Period for any:

(i) actual or alleged Breach of Confidential Information by an Insured or an Information Holder;

(ii) actual or alleged Security Failure; or

(iii) actual or alleged failure by a Company to notify a Data Subject or any Regulator of an unauthorised disclosure or transmission of Personal Information for which the Company is responsible in accordance with the requirements of any Data Protection Legislation,

which occurred or occurs prior to or during the Policy Period.

2. Definitions

The following definitions are specific to this Security and Privacy Liability Coverage Section. All other definitions set out within Section 10 (Definitions) of the General Terms and Conditions shall apply as stated.

Breach of Confidential Information

The unauthorised disclosure or transmission of Confidential Information.

Claim

(i) A written demand against an Insured;

(ii) civil, administrative or arbitral proceedings brought against an Insured; or

(iii) a PCI-DSS Assessment,

seeking any legal remedy.

Company Computer System

(i) Any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by a Company;

(ii) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system;

(iii) any employee "Bring Your Own Device" but only to the extent such device is used to access any of the foregoing computer hardware, software or components thereof or Data contained therein; or

(iv) any cloud service or other hosted computer resources, used by a Company and operated by a Third Party service provider under a written contract between such Third Party service provider and a Company.

Confidential Information

Corporate Information and Personal Information in a Company's or Information Holder's care, custody or control or for which a Company is legally responsible.

Corporate Information

A Third Party's items of information that are not available to the public (including trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports and documents) which are subject to contractual or legal protection.

Cyber Terrorism

The premeditated use of disruptive activities against a Company Computer System or network, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

Cyber Terrorism does not include any such activities which are part of or in support of any use of military force or war.

Damages

Damages that an Insured is legally liable to pay resulting from a Claim as ascertained by:

(i) judgments or arbitral awards rendered against that Insured; or

(ii) a settlement agreement negotiated by that Insured and which is approved by the Insurer.

Damages includes punitive or exemplary or multiple damages where lawfully insurable and any monetary amounts that an Insured is required by law or has agreed by settlement to deposit into a consumer redress fund.

Data Protection Fines

Any lawfully insurable fines or penalties which are adjudicated by a Regulator to be payable by a Company for a breach of Data Protection Legislation.

Data Protection Fines does not include any other type of civil or criminal fines and penalties.

Data Protection Legislation

The Data Protection Act 1998, the Data Protection Act 2018 and the General Data Protection Regulation (Regulation (EU) 2016/679) and any subsequent legislation that alters, repeals or replaces such legislation and all other equivalent laws and regulations relating to the regulation and enforcement of data protection and data privacy in any country.

Data Subject

Any natural person whose Personal Information has been either collected, stored or processed by or on behalf of a Company.

Defence Costs

Reasonable and necessary legal fees, costs and expenses which an Insured incurs with the prior written consent of the Insurer in relation to the investigation, response, defence, appeal or settlement of a Claim or Regulatory Investigation, including court attendance costs incurred by or on behalf of that Insured.

Defence Costs does not include the remuneration of any Insured, cost of their time or any other costs or overheads of any Insured.

Information Holder

A Third Party that:

(i) a Company has provided Personal Information or Corporate Information to; or

(ii) has received Personal Information or Corporate Information on behalf of a Company.

Insured

(i) A Company;

(ii) a natural person who was, is or during the Policy Period becomes a principal, partner, director, officer or Employee of a Company;

(iii) a natural person who is an independent contractor, temporary contract labourer, self–employed person, or labour–only sub–contractor, under the direction and direct supervision of a Company but only in relation to the services provided to that Company.

Insured includes the estate, heirs or legal representatives of a deceased, legally incompetent or bankrupt Insured referred to in (ii) above to the extent that a Claim is brought against them solely by reason of them having an interest in property that is sought to be recovered in a Claim against such Insured referred to in (ii) above.

Insured Event

A Claim or a Regulatory Investigation.

Loss

(i) For the purposes of Insurance Cover 1.1, Defence Costs and Data Protection Fines;

(ii) for the purposes of Insurance Cover 1.2, Damages, Defence Costs and any amounts payable in connection with a PCI-DSS Assessment.

Loss does not include:

(a) non–compensatory or multiple damages (except to the extent covered as Damages or as part of a PCI-DSS Assessment) or liquidated damages;

(b) fines or penalties (except Data Protection Fines to the extent covered in 1.1. (Data Protection Investigation and Data Protection Fines));

(c) the costs and expenses of complying with any order for, grant of or agreement to provide injunctive or other non–monetary relief; or

(d) an Insured's remuneration, cost of time or overheads.

PCI–DSS Assessment

Any written demand received by a Company from a Payment Card Association (e.g., MasterCard, Visa, American Express) or bank or servicer processing payment card transactions (e.g., an "Acquiring Bank" or "Payment Processor") for a monetary amount (including fraud recovery, operational reimbursement, reimbursement of card reissuance costs and contractual fines and penalties) where:

(i) a Company has contractually agreed to indemnify such Payment Card Association, bank or servicer processing payment card transactions for any monetary assessment made in connection with a Company's obligations under generally accepted and published Payment Card Industry Standards for data security, including such contractual obligations contained in a merchant services agreement or similar agreement; and

(ii) such monetary assessment arises out of a Breach of Confidential Information.

Personal Information

Any information relating to an identified or identifiable natural person.

Personal Information includes a natural person's name, online identifier, telephone number, credit card or debit card number, account and other banking information, medical information, or any other information about a natural person protected under any Data Protection Legislation.

Regulator

A regulator established pursuant to Data Protection Legislation in any jurisdiction and which is authorised to enforce statutory obligations in relation to the collecting, storing, processing or control of Confidential Information.

Regulator includes any other government agency or authorised data protection authority who makes a demand on the Insured in relation to Data Protection Legislation.

Regulatory Investigation

Any formal or official action, investigation, inquiry or audit by a Regulator against a Company once it is identified in writing by a Regulator, which arises out of the use or suspected misuse of Personal Information or any aspects of the control, collection, storing or processing of Personal Information or delegation of data processing to an Information Holder, which is regulated by Data Protection Legislation.

Regulatory Investigation does not include any industry-wide, non-firm specific, action, investigation, inquiry or audit.

Security Failure

(i) Any intrusion of, unauthorised access (including an unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) a Company Computer System, including that which results in or fails to mitigate any:

(a) denial of service attack or denial of access; or

(b) receipt or transmission of a malicious code, malicious software or virus;

(ii) the loss of Data arising from the physical theft or loss of hardware controlled by a Company; or

(iii) the unauthorised reprogramming or corruption of software (including firmware) which renders a Company Computer System or any component thereof non-functional or useless for its intended purpose.

3. Exclusions

The following Exclusions are specific to this Security and Privacy Liability Coverage Section. They apply in addition to the Exclusions in Section 11 (Exclusions) of the General Terms and Conditions.

The Insurer shall not be liable for Loss arising out of, based upon or attributable to:

3.1. Anti–Trust

Any actual or alleged antitrust violation, restraint of trade, unfair competition or unfair or deceptive business practices, including violation of any consumer protection law.

This Exclusion 3.1 shall not apply to a Regulatory Investigation alleging such unfair competition directly in connection with a Security Failure or Breach of Confidential Information.

3.2. Assumed Liability, Guarantee, Warranty

Any guarantee, warranty, contractual term or liability assumed or accepted by an Insured under any contract or agreement except to the extent such liability would have attached to the Insured in the absence of such contract or agreement.

This Exclusion 3.2 shall not apply to:

(i) a contractual obligation to prevent a Security Failure or Breach of Confidential Information;

(i) an obligation under a confidentiality or disclosure agreement held within contracts with a Third Party to prevent a Breach of Confidential Information; or

(ii) the obligation to comply with Payment Card Industry Data Security Standards.

3.3. Bodily Injury and Property Damage

Any:

(i) physical injury, mental illness, sickness, disease or death: however, this Exclusion 3.3 (i) shall not apply in respect of emotional distress or mental anguish arising solely out of an Breach of Confidential Information; or

(ii) loss, damage or destruction of tangible property.

3.4. Employment Practices Liability

Any of a Company's employment practices (including wrongful dismissal, discharge or termination, discrimination, harassment, retaliation or other employment–related claim).

This Exclusion 3.4 shall not apply to any Claim by an individual to the extent such individual is alleging:

(i) a Breach of Confidential Information in connection with such individual's employment or application for employment with a Company; or

(i) a failure to disclose a Security Failure or Breach of Confidential Information.

3.5. Government Entity or Public Authority

Any seizure, confiscation or nationalisation of a Company Computer System by order of any government entity or public authority.

3.6. Infrastructure

Any electrical or mechanical failure of infrastructure not under the control of a Company, including any electrical power interruption, surge, brownout or blackout, failure of telephone lines, data transmission lines, or other telecommunications or networking infrastructure.

This Exclusion 3.6 shall not apply to Loss arising out of, based upon or attributable solely to a Security Failure or Breach of Confidential Information that is caused by such electrical or mechanical failure of infrastructure.

3.7. Insured v Insured

Any Claim brought by or on behalf of an Insured against another Insured.

This Exclusion 3.7 shall not apply to an actual or alleged breach of Personal Information of any Employee, director, principal, partner or officer.

3.8. Patent/Trade Secret

Any:

(i) infringement of patents;

(ii) loss of rights to secure registration of patents; or

(iii) misappropriation of trade secrets by or for the benefit of a Company.

3.9. PCI-DSS Assessment

Any PCI-DSS Assessment, unless the specific Insured which is the subject of the PCI-DSS Assessment was validated as compliant with the generally accepted and published Payment Card Industry Standards for data security prior to and at the time of any Breach of Confidential Information which gives rise to such PCI-DSS Assessment occurring.

3.10. Securities Claims

Any:

(i) actual or alleged violation by an Insured of any law, regulation or rule relating to the ownership, purchase, sale or offer of, or solicitation of an offer to purchase or sell, securities; or

(ii) any actual or alleged violation by an Insured of any provision of the Securities Act of 1933, the Securities Exchange Act of 1934 (each a United States of America statute) or any similar law of any jurisdiction.

This Exclusion 3.10 shall not apply to any Damages or Defence Costs incurred in relation to a Claim solely alleging a failure to notify a Regulator of a Breach of Confidential Information where such failure to notify is in violation of any law.

3.11. War and Terrorism

Any war (whether war is declared or not), terrorism (except Cyber Terrorism), invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these events.

Network Interruption Coverage

1. Insurance Covers

1.1. Network Interruption Loss

The Insurer will, with regard to an Insured Event which first occurs during the Policy Period, pay to each Company:

(i) Network Loss which results from the Insured Event and which the Company incurs during the Insured Event (but, if the Insured Event lasts longer than 120 days, only during the first 120 days); and

(ii) Network Loss which results from the Insured Event and which the Company incurs during the 90 days following resolution of the Insured Event.

1.2. Interruption and Mitigation Costs

The Insurer will pay, to or on behalf of each Company, Network Interruption Costs incurred in mitigating the impact of an Insured Event which first occurs during the Policy Period.

1.3. Loss Preparation Costs

If Loss Preparation Costs Cover is Purchased, the Insurer will pay, to or on behalf of each Company, Loss Preparation Costs incurred as a result of an Insured Event which first occurs during the Policy Period.

2. Definitions

The following definitions are specific to this Network Interruption Coverage Section. All other definitions set out within Section 10 (Definitions) of the General Terms and Conditions shall apply as stated.

Company Computer System

(i) Any computer hardware, software or any other components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by a Company; or

(ii) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system.

Cyber Terrorism

The premeditated use of disruptive activities against a Company Computer System or network, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

Cyber Terrorism does not include any such activities which are part of or in support of any use of military force or war.

Increased Costs of Working

Expenses (including overtime of Employees) incurred over and above normal operating expenses in order to ensure continuation of the normal business operations of a Company and to reduce its loss of business income.

Insured

A Company.

Insured Event

(i) If Security Failure Cover is Purchased, a Material Interruption to a Company Computer System that is caused by a Security Failure;

(ii) if System Failure Cover is Purchased, a Material Interruption to a Company Computer System that is caused by a System Failure;

(iii) if Voluntary Shutdown Cover is Purchased, a Material Interruption to a Company Computer System that is caused by a Voluntary Shutdown;

(iv) if OSP Security Failure Cover is Purchased, a Material Interruption to an OSP Computer System that is caused by an OSP Security Failure; and

(v) if OSP System Failure Cover is Purchased, a Material Interruption to an OSP Computer System that is caused by an OSP System Failure,

and in each case, only where the duration of the Material Interruption exceeds the applicable Waiting Hours Period specified in the schedule.

Loss

(i) For the purposes of Insurance Cover 1.1, Network Loss;

(ii) for the purposes of Insurance Cover 1.2, Network Interruption Costs;

(iii) for the purposes of Insurance Cover 1.3, Loss Preparation Costs.

Loss Preparation Costs

Reasonable and necessary professional fees and expenses incurred by a Company with the Insurer's consent, for the services of a third-party forensic accounting firm to establish, prove, verify or quantify Network Loss or Network Interruption Costs or prepare the proof of loss referred to in Condition 4.1 of this Network Interruption Coverage Section.

Loss Preparation Costs does not include any fees or expenses for consultation on coverage or negotiation of claims.

Material Interruption

(i) The suspension or degradation of a Company Computer System (for the purposes of Insured Event (i) – (iii)) or an OSP Computer System (for the purposes of Insured Event (iv) or (v)) causing the Company to be unable to continue the normal business operations of the Company; or

(ii) the deletion, damage, corruption, alteration or loss of or to Data on a Company Computer System (for the purposes of Insured Event (i) – (iii)) or an OSP Computer System (for the purposes of Insured Event

(iv) or (v)) causing the Company to be unable to access that Data and unable to continue the normal business operations of the Company.

Network Interruption Costs

The reasonable and necessary costs and expenses that a Company incurs to minimise the Network Loss, or reduce the impact of a Material Interruption; provided however that the amount of Network Loss prevented or reduced would be greater than the costs and expenses incurred.

Network Loss

(i) A Company's actual loss sustained resulting from the reduction in business income calculated by taking either Network Loss Option 1 or Network Loss Option 2; and

(ii) the Company's Increased Costs of Working (but only up to an amount equal to the reduction in business income that would have been incurred had the Company been unable to continue its normal operating procedure).

Network Loss Option 1 (Net Profit and Continuing Fixed Costs Calculation) is calculated as follows:

Take the net profit or loss which would have been earned or incurred had the Material Interruption not occurred and add the costs (including ordinary payroll) which necessarily continue during the Material Interruption.

Network Loss Option 2 (Gross Profits Calculation) is calculated as follows:

Take the revenue which would have been derived from the operation of the business had the Material Interruption not occurred and subtract the variable costs, and any other costs, which do not necessarily continue during the Material Interruption.

OSP Computer System

Any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by an Outsource Service Provider.

OSP Security Failure

Any intrusion of, unauthorised access (including any unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) an OSP Computer System, including that which results in or fails to mitigate any:

(i) denial of service attack or denial of access; or

(ii) receipt or transmission of a malicious code, malicious s software or virus.

OSP System Failure

Any unintentional and unplanned outage of an OSP Computer System such that the Outsource Service Provider is unable to provide to a Company the services described in a contract between a Company and an Outsource Service Provider pursuant to which an Outsource Service Provider provides services to a Company for a fee.

Outsource Service Provider

A Third Party that a Company has appointed to provide specified information technology services (such as the processing, hosting and storage of Data) based on an express contractual agreement, but only to the extent of the provision of such services.

Outsource Service Provider does not include:

(i) a public utility (including a provider of electricity, gas, water or telecommunication services);

(ii) an internet service provider (including any provider of internet connectivity); or,

(iii) a securities exchange or market.

Security Failure

(i) Any intrusion of, unauthorised access (including an unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) a Company Computer System, including that which results in or fails to mitigate any:

- **(a)** denial of service attack or denial of access; or,
- **(b)** receipt or transmission of a malicious code, malicious software or virus; or

(ii) the unauthorised reprogramming or corruption of software (including firmware) which renders a Company Computer System or any component thereof non-functional or useless for its intended purpose.

System Failure

Any unintentional and unplanned outage of a Company Computer System.

Voluntary Shutdown

A voluntary and intentional shutdown or impairment of a Company Computer System by or at the direction of:

(i) the Chief Information officer or Chief Information Security Officer of a Company (or the equivalent position regardless of title) who has at least 5 years' experience in an Information Security or Technology role; or

(ii) an information technology services firm appointed by a Company that has been approved in advance of such appointment by the Insurer,

after the discovery of a Security Failure, with the reasonable belief that such shutdown or impairment would limit the Loss that would otherwise be incurred as a result of that Security Failure.

3. Exclusions

The following Exclusions are specific to this Network Interruption Coverage Section. They apply in addition to the Exclusions in Section 11 (Exclusions) of the General Terms and Conditions.

The Insurer shall not be liable for Loss:

3.1. Betterment

Consisting of the costs of:

(i) updating, upgrading, enhancing or replacing any component of a Company Computer System or an OSP Computer System to a level beyond that which existed prior to the occurrence of a Material Interruption: however, this exclusion shall not apply to the extent that the replacement of a component of a Company Computer System is:

(a) required to end the Material Interruption; and

(b) no longer available and can only be reasonably replaced with an upgraded or enhanced version; or

(ii) removing software program errors or vulnerabilities.

3.2. Bodily Injury and Property Damage

Arising out of, based upon or attributable to any:

(i) physical injury, mental illness, sickness, disease or death; or

(ii) loss, damage or destruction of tangible property.

3.3. Business Conditions

Consisting of loss of earnings, or costs or expenses, attributable to unfavourable business conditions.

3.4. Government Entity or Public Authority

Arising out of, based upon or attributable to any seizure, confiscation or nationalisation of a Company Computer System by order of any government entity or public authority.

3.5. Infrastructure

Arising out of, based upon or attributable to any electrical or mechanical failure of infrastructure not under the control of a Company (or, where OSP Security Failure Cover or OSP System Failure Cover is Purchased, an Outsource Service Provider), including any electrical power interruption, surge, brownout or blackout, failure of telephone lines, data transmission lines, or other telecommunications or networking infrastructure.

3.6. Liability

Arising out of, based upon or attributable to any:

(i) written demand, civil, administrative or arbitral proceedings, made by any Third Parties seeking any legal remedy; or

(ii) penalties paid to Third Parties.

3.7. Patent

Arising out of, based upon or attributable to any infringement of patents.

3.8. Trading Losses

Consisting of trading losses, liabilities or changes in trading account value.

3.9. War and Terrorism

Arising out of, based upon or attributable to any war (whether war is declared or not), terrorism (except Cyber Terrorism), invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these events.

4. Conditions

The following conditions are specific to this Network Interruption Coverage Section and shall apply in addition to the conditions set out within the General Terms and Conditions.

4.1. Proof of Loss

In addition to the requirements to give notice to the Insurer under Section 8.1 (Notice and Reporting) of the General Terms and Conditions, and before coverage under this Network Interruption Coverage Section shall apply, a Company must also:

(i) complete and sign a written, detailed and affirmed proof of loss after the resolution of the Material Interruption, which will include:

- **(a)** a full description of the Network Interruption Costs or Network Loss and the circumstances of such Network Interruption Costs or Network Loss;
- **(b)** a detailed calculation of any Network Loss;
- **(c)** all underlying documents and materials that reasonably relate to or form a part of the basis of the proof of the Network Interruption Costs or Network Loss; and

(ii) upon the Insurer's request promptly respond to requests for information.

All adjusted claims are due and payable 45 days after:

- **(a)** the presentation of the satisfactory written proof of Network Loss and Network Interruption Costs as provided for in (i) and (ii) above; and
- **(b)** the subsequent written acceptance thereof by the Insurer.

Network Loss shall be reduced by any amounts recovered by a Company (including the value of any service credits provided to a Company) from any party (including any Outsource Service Provider).

The costs and expenses of establishing or proving Network Loss and/or Network Interruption Costs under this Network Interruption Coverage Section, including those associated with preparing the proof of loss, shall be the obligation of the Company and are not covered under this policy except as covered under 1.3 (Loss Preparation Costs) of this Network Interruption Coverage Section.

4.2. Appraisal

If a Company and the Insurer disagree on the extent of Network Loss or Network Interruption Costs, either may make a written demand for an appraisal of such Network Loss or Network Interruption Costs. If such demand is made, each party will select a competent and impartial appraiser. The appraisers will then jointly select an expert who has not less than 10 years' standing and who is a partner in a major international accounting firm, experienced in assessing loss of this nature. Each appraiser will separately state the extent of Network Loss or Network Interruption Costs. If they fail to agree, they will submit their differences to the expert. Any decision by the expert will be final and binding.

The Company and the Insurer will:

(i) pay their own costs, including the costs of their respective chosen appraiser, and

(ii) bear the expenses of the expert equally.

Event Management Coverage

1. Insurance Covers

1.1. Event Management

The Insurer will pay to or on behalf of each Company:

(i) Legal Expenses;

(ii) IT Expenses;

(iii) Data Recovery Expenses;

(iv) Reputation Protection Expenses;

(v) Notification Expenses;

(vi) Credit Monitoring and ID Monitoring Expenses; and

(vii) (if First Response Cover is Purchased) First Response Expenses,

incurred solely as a result of an Insured Event which has occurred, or the Company reasonably believes has occurred, before or during the Policy Period and which, during the Policy Period, the Company first becomes aware of such Insured Event.

First Response Expenses will only be paid by the Insurer to the extent that they are incurred during the period of hours stated for the First Response Cover in the schedule, which shall commence when the Responsible Officer of the Policyholder first notifies the First Response Advisor of the Insured Event by contacting the Emergency Number specified in the schedule.

No Retention shall apply to First Response Expenses.

2. Definitions

The following definitions are specific to this Event Management Coverage Section. All other definitions set out within Section 10 (Definitions) of the General Terms and Conditions shall apply as stated.

Breach of Confidential Information

The unauthorised disclosure or transmission of Confidential Information.

Company Computer System

(i) Any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by a Company;

(ii) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system; or

(iii) any employee "Bring Your Own Device" but only to the extent such device is used to access any of the foregoing computer hardware, software or components thereof or Data contained therein.

Confidential Information

Corporate Information and Personal Information in a Company's or Information Holder's care, custody or control or for which a Company is legally responsible.

Corporate Information

A Third Party's items of information that are not available to the public (including trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports and documents) which are subject to contractual or legal protection.

Credit Monitoring and ID Monitoring Expenses

The reasonable and necessary fees, costs and expenses incurred by a Company, with the Insurer's prior written consent, for Credit Monitoring and ID Monitoring Services provided to those Data Subjects whose Confidential Information is reasonably believed to have been disclosed or transmitted.

Credit Monitoring and ID Monitoring Services

Credit or identity theft monitoring services to identify possible misuse of any Personal Information as a result of an actual or suspected Breach of Confidential Information.

Cyber Terrorism

The premeditated use of disruptive activities against a Company Computer System or network, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

Cyber Terrorism does not include any such activities which are part of or in support of any use of military force or war.

Data Recovery Expenses

The reasonable and necessary fees, costs and expenses incurred by a Company on actions taken to:

(i) identify lost, damaged, destroyed or corrupted Data;

(ii) determine whether any lost, damaged, destroyed or corrupted Data can be restored, repaired, recollected or recreated; and

(iii) restore, recreate, repair or recollect lost,damaged, destroyed or corrupted Data to substantially the form in which it existed immediately prior to the Insured Event, including where necessary the cost to restore Data from backups or the recreation of Data from physical records.

Data Subject

Any natural person whose Personal Information has been either collected, stored or processed by or on behalf of a Company.

First Response Advisor

The law firm specified in the schedule, or other law firms instructed by such specified law firm, or any replacement firm nominated by the Insurer in the event of a conflict of interest, with respect to whom a Company shall enter into a Relevant Engagement.

First Response Expenses

The reasonable and necessary fees, costs and expenses of:

(i) the First Response Advisor providing First Response Legal Services;

(ii) the First Response IT Specialist providing IT Services; and

(iii) the Public Relations Advisor, if its appointment is considered necessary by the First Response Advisor or the Insurer, providing Reputation Protection Services.

First Response IT Specialists

The firm specified in the schedule, or any replacement firm appointed by the Insurer in the event of a conflict of interest.

First Response Legal Services

(i) legal advice and support provided pursuant to a Relevant Engagement;

(ii) coordinating the First Response IT Specialist, and, if considered necessary by the First Response Advisor or Insurer, the Public Relations Advisor; and

(iii) preparation and notification to any relevant Regulator.

Information Holder

A Third Party that:

(i) a Company has provided Personal Information or Corporate Information to; or

(ii) has received Personal Information or Corporate Information on behalf of a Company.

Insured

A Company.

Insured Event

(i) A Breach of Confidential Information;

(i) a Security Failure; or

(ii) in respect of Data Recovery Expenses only, an Operational Failure.

IT Expenses

The reasonable and necessary fees, costs and expenses of an IT Specialist providing IT Services.

IT Services

The services of:

(i) substantiating whether an Insured Event has occurred, how it occurred and whether it is still occurring;

(i) identifying any compromised Data resulting from an Insured Event;

(ii) establishing the extent to which Confidential Information may have been compromised; or

(iii) containing and resolving an Insured Event and making recommendations to prevent or mitigate a future occurrence of the same or similar event.

IT Specialist

An information technology services firm appointed by a Company that has been approved in advance of such appointment by the Insurer.

Legal Expenses

The reasonable and necessary fees, costs and expenses of a Response Advisor providing the Legal Services.

Legal Services

The services of:

(i) co–ordinating the IT Specialist or Public Relations Advisor;

(ii) advising, notifying and corresponding on any notification requirements with any relevant Regulator; or

(iii) monitoring complaints raised by Data Subjects and advising a Company on responses to an Insured Event for the purposes of minimising harm to the Company, including actions taken to maintain and restore public confidence in the Company,

in dealing with any actual or suspected Breach of Confidential Information or Security Failure.

Loss

Legal Expenses, IT Expenses, Data Recovery Expenses, Reputation Protection Expenses, Notification Expenses, Credit Monitoring and ID Monitoring Expenses and First Response Expenses.

Notification

(i) Setting up and operating call centres;

(ii) preparing and notifying;

- **(a)** those Data Subjects whose Confidential Information is reasonably believed to have been disclosed or transmitted; or
- **(b)** any relevant Regulator; or

(iii) investigating and collating information,

with regard to any actual or suspected Breach of Confidential Information.

Notification Expenses

The reasonable and necessary fees, costs and expenses incurred by a Company on Notification.

Operational Failure

The loss or damage to Data caused by:

(i) a negligent or unintentional act or failure to act by:

- **(a)** an Insured;
- **(b)** an employee of an Insured; or
- **(c)** a third party service provider to an Insured;

(ii) the loss or theft of electronic equipment; or

(iii) a magnetic event other than:

- **(a)** the use of electromagnetic or directed-energy weapons; or
- **(b)** the natural deterioration of the storage media or data.

Personal Information

Any information relating to an identified or identifiable natural person.

Personal Information includes a natural person's name, online identifier, telephone number, credit card or debit card number, account and other banking information, medical information, or any other information about a natural person protected under any Data Protection Regulation.

Public Relations Advisor

A consultant appointed by the Insurer or the Response Advisor, or any other consultant appointed by a Company that has been approved by the Insurer in advance of such appointment, to provide Reputation Protection Services.

Regulator

A regulator established pursuant to Data Protection Legislation in any jurisdiction and which is authorised to enforce statutory obligations in relation to the collecting, storing, processing or control of Confidential Information.

Regulator includes any other government agency or authorised data protection authority who makes a demand on a Company in relation to Data Protection Legislation.

Relevant Engagement

A written agreement between the First Response Advisor and a Company governing the provision of the First Response Legal Services to the Company.

Reputation Protection Expenses

The reasonable and necessary fees, costs and expenses of a Public Relations Advisor providing Reputation Protection Services.

Reputation Protection Services

Advice and support (including advice concerning media strategy and independent public relations services, and the design and management of a communications strategy) in order to mitigate or prevent the potential adverse effect, or reputational damage, from media reporting of an Insured Event.

Response Advisor

Any law firm appointed by the Insurer, or any other law firm appointed by a Company that has been approved in advance of such appointment by the Insurer.

Security Failure

(i) Any intrusion of, unauthorised access (including an unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) a Company Computer System, including that which results in or fails to mitigate any:

- **(a)** denial of service attack or denial of access; or
- **(b)** receipt or transmission of a malicious code, malicious software or virus;

(ii) The loss of Data arising from the physical theft or loss of hardware controlled by a Company; or

(iii) the unauthorised reprogramming or corruption of software (including firmware) which renders a Company Computer System or any component thereof non-functional or useless for its intended purpose.

3. Exclusions

The following Exclusions are specific to this Event Management Coverage Section. They apply in addition to the Exclusions in Section 11 (Exclusions) of the General Terms and Conditions.

The Insurer shall not be liable for any Loss:

3.1. Betterment

Consisting of the costs of:

(i) updating, upgrading, enhancing or replacing a Company Computer System to a level beyond that which existed prior to the occurrence of an Insured Event; and

(ii) removing software program errors or vulnerabilities.

3.2. Bodily Injury and Property Damage

Arising out of, based upon or attributable to any:

(i) physical injury, mental illness, sickness, disease or death; or

(ii) loss, damage or destruction of tangible property.

3.3. Government Entity or Public Authority

Arising out of, based upon or attributable to any seizure,confiscation or nationalisation of a Company Computer System by order of any government entity or public authority.

3.4. Infrastructure

Arising out of, based upon or attributable to any electrical or mechanical failure of infrastructure not under the control of a Company, including any electrical power interruption, surge, brownout or blackout, failure of telephone lines, data transmission lines, or other telecommunications or networking infrastructure.

This Exclusion 3.4 shall not apply to Loss arising out of, based upon or attributable solely to a Security Failure or Breach of Confidential Information that is caused by such electrical or mechanical failure of infrastructure.

3.5. Internal/Staff Costs

Consisting of the costs of payroll, fees, benefits, overheads or internal charges of any kind incurred by a Company.

3.6. Patent/Trade Secret

Arising out of, based upon or attributable to any:

(i) infringement of patents;

(ii) loss of rights to secure registration of patents; or

(iii) misappropriation of trade secrets by or for the benefit of a Company.

3.7. War and Terrorism

Arising out of, based upon or attributable to any war (whether war is declared or not), terrorism (except Cyber Terrorism), invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these events.

4. Conditions

The following conditions are specific to this Event Management Coverage Section and shall apply in addition to the conditions set out within the General Terms and Conditions.

4.1. First Response Notification

The cover provided for First Response Expenses is granted solely with respect to a Breach of Confidential Information or Security Failure first discovered during the Policy Period and a Company shall, as a condition precedent to the obligations of the Insurer in respect of such First Response Expenses, notify the Insurer by contacting the Emergency Number specified in the schedule as soon as reasonably practicable after the Breach of Confidential Information or Security Failure first occurs.

Cyber Extortion Coverage

1. Insurance Covers

1.1 Cyber Extortion

The Insurer will pay, to or on behalf of each Company, Loss that the Company incurs solely as a result of an Extortion Threat which first occurs during the Policy Period.

2. Definitions

The following definitions are specific to this Cyber Extortion Coverage Section. All other definitions set out within Section 10 (Definitions) of the General Terms and Conditions shall apply as stated.

Breach of Confidential Information

The unauthorised disclosure or transmission of Confidential Information.

Company Computer System

(i) Any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by a Company;

(ii) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system; or

(iii) any employee "Bring Your Own Device" but only to the extent such device is used to access any of the foregoing computer hardware, software or components thereof or Data contained therein.

Confidential Information

Corporate Information and Personal Information in a Company's or Information Holder's care, custody or control or for which a Company is legally responsible.

Corporate Information

A Third Party's items of information that are not available to the public (including trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports and documents) which are subject to contractual or legal protection.

Cyber Extortion Expenses

The reasonable and necessary fees, costs and expenses of any firm appointed by the Insurer or any other firm appointed by the Company that has been approved by the Insurer in advance of such appointment to provide the Cyber Extortion Services.

Cyber Extortion Services

(i) Conducting an investigation to determine the validity, cause and scope of an Extortion Threat;

(ii) advising on the response to an Extortion Threat;

(iii) containing or resolving the disruption of the operations of a Company Computer System caused by the Extortion Threat; or

(iv) assisting a Company in negotiating a resolution to an Extortion Threat.

Cyber Terrorism

The premeditated use of disruptive activities against a Company Computer System or network, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

Cyber Terrorism does not include any such activities which are part of or in support of any use of military force or war.

Extortion Threat

Any threat or connected series of threats, for the purpose of demanding money, securities or other tangible or intangible property of value from a Company, to:

(i) commit or continue a Breach of Confidential Information;

(ii) commit or continue an intentional attack against a Company Computer System (including through the use of ransomware); or

(iii) disclose information concerning a vulnerability in a Company Computer System.

Information Holder

A Third Party that:

(i) a Company has provided Personal Information or Corporate Information to; or

(ii) has received Personal Information or Corporate Information on behalf of a Company.

Insured

A Company.

Insured Event

An Extortion Threat.

Loss

(i) Any payment of cash, monetary instrument, cryptocurrencies (including the costs to obtain such cryptocurrencies) or the fair market value of any property which a Company has paid, to prevent or end an Extortion Threat; and

(ii) Cyber Extortion Expenses.

Personal Information

Any Data relating to an identified or identifiable natural person.

Personal Information includes a natural person's name, online identifiers, telephone number, credit card or debit card number, account and other banking information, medical information, or any other information about a natural person protected under any Data Protection Legislation.

3. Exclusions

The following Exclusions are specific to this Cyber Extortion Coverage Section. They apply in addition to the Exclusions in Section 11 (Exclusions) of the General Terms and Conditions.

The Insurer shall not be liable for any Loss:

3.1. Anti-terrorism legislation

To the extent that the provision of such payment to or on behalf of a Company would expose the Insurer, its parent company or its ultimate controlling entity to any applicable anti-terrorism legislation or regulation under United Nations resolutions laws or regulations of the European Union, or the United States of America or the United Kingdom.

3.2. Bodily Injury and Property Damage

For any:

(i) physical injury, mental illness, sickness, disease or eath; or

(ii) loss, damage or destruction of tangible property.

3.3. Government Entity or Public Authority

Arising out of, based upon or attributable to a regulatory or enforcement threat or demand by any government entity or public authority.

3.4. Patent

Arising out of, based upon or attributable to any infringement of patents.

3.5. War and Terrorism

Arising out of, based upon or attributable to any war (whether war is declared or not), terrorism (except Cyber Terrorism), invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these events.

This marketing material is intended for insurance brokers and other insurance professionals for their information.
For full terms, conditions and benefits related to AIG products, please refer to the policy and associated documents.

GBL00003622 1024