Cyber Proactive Response

Policy document

United States

Proactive services

As an added benefit to this policy proactive cyber attack prevention services are provided to you, working to identify vulnerabilities and risks targeting insureds and try to prevent them from turning into cyber incidents. For more information on how these services work, contact us or read this article.

CFC (the Coverholder identified on your Policy Certificate) strives to provide proactive support and advice on cyber risks and vulnerabilities that you may be exposed to throughout the duration of the policy. In certain circumstances such support may be provided by CFC Response.

Accessing proactive services

It is recommended that you download and activate the CFC Response app, including enabling notifications, in order to ensure full access to, and benefit from, CFC's Proactive services. While CFC will endeavour to provide these proactive services to you without the app, downloading the app will allow CFC to provide a deeper level of threat analysis. Your policy number provides you with free access to the app.

No impact on policy limits

Being alerted of a risk or vulnerability by CFC will not constitute a claim under your policy. CFC interactions with you to provide support and advice regarding cyber risks and vulnerabilities they have identified will not impact any coverage that you may be entitled to.

Proactive services tailored for you

CFC supports you by trying to identify risks and vulnerabilities that may lead to cyber incidents throughout the duration of the policy. If CFC becomes aware of a cyber risk or vulnerability to which you may be exposed, CFC will strive to provide proactive risk management services to you. These services can include:

A. sending threat alerts through the Response mobile application (or via another means of communication if you have not downloaded the Response mobile application);

B. providing initial advice to you about the risk or vulnerability, including threat intelligence; and

C. providing initial remote support and assistance to you to remedy the risk or vulnerability.

The Services at b. and c. above will be provided to you by CFC Response.

If a cyber event occurs

In the event that the risk or vulnerability CFC alerts you about results in a notifiable incident under the Policy, you should refer to the Policy Conditions or speak with your broker for information about notification requirements to CFC.

About CFC Response

CFC Response is a trading name of the below listed entities, all of which are affiliates of CFC:

1. CFC Security Inc, DE file number 7451204, principal place of business at 300 E. Highland Mall Blvd, Suite 300, Austin, Texas 78752 United States;
2. CFC Security Limited, registered company number 13497455 with registered address at 85 Gracechurch Street, London, EC3V 0AA; and
3. CFC Security Pty Ltd, principal place of business at 130 Bundall Road, Unit 22, Queensland, 4217, Australia, ACN: 096 518 820.

You may receive services from one or more of the above companies depending upon your geographical location.

By using CFC Response services, you agree to the relevant entity's terms and conditions, which can be found here. These terms outline the scope of services provided and any applicable limitations on liability. CFC is not responsible for services provided by CFC Response. Liability for these services is governed by the terms and conditions of the relevant CFC Response entity. If you have any questions about these terms, please contact CFC Response for clarification at enquiries@cfcresponse.com.

Our liability for proactive support services

CFC's Proactive services are designed to support cyber risk visibility and deliver timely alerts. These services do not replace the need for a comprehensive cybersecurity programme. Whilst CFC will endeavour to identify risks and vulnerabilities that may lead to cyber incidents throughout the duration of the policy to you, neither CFC nor CFC Response offers any guarantee that all such risks and vulnerabilities will be prevented, identified or resolved by CFC or CFC Response. You remain solely responsible for securing your systems and data.

PREAMBLE

As an added benefit to this Policy, proactive cyber attack prevention services are provided to **you**. These services are designed to help identify potential vulnerabilities and threats targeting **you** and aim to assist in reducing the likelihood of cyber incidents.

IMPORTANT: COVERAGE TRIGGERS. It is important for **you** to review this Policy carefully as the trigger for coverage, including when **you** must notify **us** of a claim, under each Section and Insuring Clause may differ.

This Policy is a contract of insurance between **you** and **us**. Your Policy contains all the details of the cover that **we** provide. This Policy consists of and must be read together with the Declarations page and any Endorsements. This Policy is not complete unless it is signed and a Declarations page is attached.

The sections of this Policy are identified by the blue lines across the page with white upper case print, these are for information purposes only and do not form part of the cover given by this Policy. Terms in bold upper case print are references to specific Insuring Clauses, Sections or Conditions. Other terms in bold lower case print are defined terms and have a special meaning as set forth in the Definitions section and elsewhere. Words stated in the singular will include the plural and vice versa.

In consideration of the **premium** and in reliance upon the information that **you** have provided to **us** prior to the commencement of this insurance, **we** agree to provide the cover as set out below:

INSURING CLAUSES

INSURING CLAUSE 1: CYBER INCIDENT RESPONSE

SECTION A: INCIDENT RESPONSE COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

a. gain access to **our** 24/7 **cyber incident response line**;
b. engage with **our claims manager** who will coordinate the initial response;
c. obtain initial advice and consultancy from **our claims manager**, including threat intelligence in relation to the **cyber event**; and
d. obtain initial remote support and assistance from **our claims manager** to respond to the **cyber event**.

SECTION B: LEGAL AND REGULATORY COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

a. obtain legal advice to determine the correct course of action;
b. draft **privacy breach** notification letters, substitute notices, website notices or e-mail notification templates;
c. notify any appropriate governmental, regulatory, law enforcement, professional or statutory body;
d. respond to any **regulatory investigation**; and
e. defend any regulatory action.

SECTION C: IT SECURITY AND FORENSIC COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

a. engage with an external IT security consultant to identify the source and scope of the **cyber event**;
b. obtain initial advice to remediate the impact of the **cyber event**;
c. conduct a forensic investigation of **your computer systems** where reasonable and necessary or as required by law or a regulatory body (including a requirement for a PCI Forensic Investigator);
d. contain and remove any malware discovered on **your computer systems**; and
e. engage with an IT security consultant to provide expert witness testimony at any trial or hearing arising from the **cyber event**.

SECTION D: CRISIS COMMUNICATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

a. engage with a crisis communications consultant to obtain specific advice in direct relation to the **cyber event**;
b. coordinate media relations in response to the **cyber event**;
c. receive training for relevant spokespeople with respect to media communications in direct relation to the **cyber event**; and
d. formulate a crisis communications plan in order to reduce damage to **your** brand and reputation as a direct result of the **cyber event**.

SECTION E: PRIVACY BREACH MANAGEMENT COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered during the **period of the policy** to:

a. print and post appropriate notices for any individual affected by the actual or suspected **cyber event** or to send e-mail notices or issue substitute notices, including any **privacy breach** notification that **you** are not legally obliged to make;
b. provide credit monitoring services, identity monitoring services, identity restoration services or identity theft insurance to affected individuals;
c. set up a call center to manage inbound and outbound calls in direct relation to the **cyber event**; and
d. provide translation services to manage communications with affected individuals.

SECTION F: THIRD PARTY PRIVACY BREACH MANAGEMENT COSTS

We agree to pay on behalf of any **third party** any reasonable sums necessarily incurred as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

a. print and post appropriate notices for any individual affected by the actual or suspected **cyber event** or to send e-mail notices or issue substitute notices;
b. provide credit monitoring services, identity monitoring services, identity restoration services or identity theft insurance to affected individuals;
c. set up a call center to manage inbound and outbound calls in direct relation to the **cyber event**; and
d. provide translation services to manage communications with affected individuals;

provided that **you** are contractually required to indemnify the **third party** against this **cyber event** and they have a legal obligation to notify affected individuals.

SECTION G: POST BREACH REMEDIATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, with **our claims manager** following a **cyber event** covered under INSURING CLAUSE 1 for the following services in order to mitigate the potential of a future **cyber event**:

a. complete an information security risk assessment;
b. conduct an information security gap analysis;
c. develop an information security document set; and
d. deliver an information security awareness training session.

INSURING CLAUSE 2: CYBER CRIME

SECTION A: FUNDS TRANSFER FRAUD

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of any **third party** committing:

a. any unauthorized electronic transfer of **company** funds from a bank;
b. theft of the **company's** money or other financial assets from a bank by electronic means;
c. theft of money or other financial assets from **your** corporate credit cards by electronic means; or

d. any phishing, vishing or other social engineering attack against any **employee** or **senior executive officer** that results in the transfer of **company** funds to an unintended **third party**.

SECTION B: INVOICE MANIPULATION

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy**, as a direct result of theft committed by a **third party** of a **client's** money or other financial assets, that the **client** intended to send to **you** for the provision of goods and services, but which **you** did not receive as a result of fraudulent electronic communications designed to impersonate a **senior executive officer** or **employee**, including the creation of fraudulent invoices or change of banking details.

SECTION C: NEW VENDOR FRAUD

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of a fraudulent **third party** posing as a legitimate vendor of goods or services with whom **you** are transacting for the first time, resulting in **you** paying for goods or services that **you** did not receive.

SECTION D: PHYSICAL GOODS FRAUD

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of a **third party** committing any phishing, vishing or other social engineering attack against an **employee** or **senior executive officer** that results in **you** sending the **company's** tangible property or goods to an unintended **third party**.

However, **we** will not make any payment under this Section for **loss** as a result of a legitimate customer not paying or refusing to pay for tangible property or goods that **you** have sent to them.

SECTION E: THEFT OF PERSONAL FUNDS

We agree to reimburse any **senior executive officer** for personal financial loss first discovered by them during the **period of the policy** as a direct result of any **third party** compromising the **company's** network security, which results in:

a. theft of money or other financial assets from a personal bank account of the **senior executive officer**; or
b. identity theft of the **senior executive officer** as a result of a **privacy breach** suffered by **you**.

However, **we** will not make any payment under this Section for any cryptoasset, including cryptocurrency, utility tokens, securities token or ecosystem tokens, belonging to the **senior executive officer**.

SECTION F: CORPORATE IDENTITY THEFT

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of the fraudulent use or misuse of **your** electronic identity, including the:

a. establishment of credit or loans in **your** name;
b. unauthorized electronic signing of any contract or agreement in **your** name;
c. costs associated with the removal of websites designed to impersonate **you**; or
d. the reliance by a **third party** on a fraudulent version of **your** digital identity to execute transactions of **your** funds or other financial assets.

SECTION G: THEFT OF FUNDS HELD IN ESCROW

We agree to reimburse **you** for **loss** (including compensation that the **company** is legally obliged to pay) first discovered by **you** during the **period of the policy** as a direct result of **you** having to reimburse a **client** for theft of the **client's** money or other financial assets from a bank account held in **your** name, provided that the theft was committed by a **third party** by electronic means, including any phishing, vishing or other social engineering attack against **you**.

SECTION H: THEFT OF CLIENT FUNDS

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of **you** having to reimburse a **client** for theft of the **client's** money or other financial assets from a **client's** bank account that **you** had access to, provided that the theft was as a result of a social engineering attack committed against **you** by a **third party**.

SECTION I: CUSTOMER PAYMENT FRAUD

We agree to reimburse **you** in the event of fraudulent electronic communications or websites designed to impersonate **you** or any of **your** products, first discovered by **you** during the **period of the policy**, for **loss** directly attributable to:

a. reimbursing **your** customers for their financial loss arising directly from the fraudulent communications, including fraudulent invoices manipulated to impersonate **you**, where goods or services have not been provided to the customers by **you** or on **your** behalf; and
b. the cost of creating and issuing a specific press release or establishing a specific website to advise **your** customers and prospective customers of the fraudulent communications.

SECTION J: TELEPHONE HACKING

We agree to reimburse **you** for **loss** associated with the cost of unauthorized calls or unauthorized use of **your** bandwidth first discovered by **you** during the **period of the policy** as a direct result of **your** telephone system being hacked by a **third party**.

SECTION K: UNAUTHORIZED USE OF COMPUTER RESOURCES

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of **cryptojacking** or **botnetting**.

INSURING CLAUSE 3: CYBER EXTORTION

We agree to pay on behalf of the **company** any ransom in response to an extortion demand made against **you** and first discovered by **you** during the **period of the policy** as a direct result of any actual or threat of:

a. introduction of malware, including ransomware, into **your computer systems**;
b. prevention of access to **your computer systems** or any **third party** systems hosting **your** applications or data;
c. disclosure of **your** confidential information or confidential information entrusted to **you**; or
d. damage to **your** brand or reputation by posting false or misleading information about **you** on social media sites.

We will also pay on behalf of the **company** the reasonable and necessary costs incurred to respond to the extortion demand (including costs incurred to procure cryptocurrency for the purposes of paying the ransom or in negotiating with the individual or organization making the extortion demand against **you**).

INSURING CLAUSE 4: SYSTEM DAMAGE AND BUSINESS INTERRUPTION

SECTION A: SYSTEM DAMAGE AND RECTIFICATION COSTS

We agree to reimburse **you** for the additional cost of employing:

a. contract staff or overtime costs for **employees** to rebuild **your** data, including the cost of data re-entry or data re-creation;
b. specialist consultants, including IT forensic consultants, to recover **your** data or applications; and
c. specialist consultants or overtime costs for **employees** working within **your** IT department to reconstitute **your computer systems** to the position they were in immediately prior to the **cyber event**;

as a direct result of a **cyber event** first discovered by **you** during the **period of the policy**.

SECTION B: HARDWARE REPLACEMENT COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred to replace any computer hardware or tangible equipment forming part of **your computer systems** that have been rendered unusable as a direct result of a **cyber event** first discovered by **you** during the **period of the policy**, provided that replacing the computer hardware or tangible equipment is a more cost effective solution than installing new firmware or software onto **your** existing hardware.

For the purposes of this Section, **we** will also pay the reasonable costs necessarily incurred to purchase and install temporary computer hardware or tangible equipment that are necessary in the interim for the sole purpose of facilitating the recovery of **your** data or systems during the remediation phase of the **cyber event**.

SECTION C: INCOME LOSS AND EXTRA EXPENSE

We agree to reimburse **you** for **your income loss** and **extra expense** sustained during the **indemnity period** as a direct result of an interruption to **your business operations** caused by **computer systems** downtime arising directly out of a **cyber event**, **system failure** or **operator error**, which is first discovered by **you** during the **period of the policy**, provided that the **computer systems** downtime lasts longer than the **time franchise**.

SECTION D: EMERGENCY AND ADDITIONAL OPERATIONAL CONTINUITY COSTS

We agree to reimburse **you** for any reasonable sums necessarily incurred during the **indemnity period** that are in addition to **your** normal operating expenses and the **extra expense** recoverable under **INSURING CLAUSE 4** (**SECTION C** only):

a. to source **your** products or services from alternative sources in order to meet contractual obligations to supply **your** customers;
b. to employ contract staff or overtime costs for **employees** in order to continue **your business operations**;
c. to employ specialist consultants, including IT forensic consultants to diagnose the source of the **computer systems** downtime; and
d. for **employees** working overtime within **your** IT department to diagnose and fix the source of the **computer systems** downtime;

to mitigate an interruption to **your business operations** caused by **computer systems** downtime arising directly out of a **cyber event**, **system failure** or **operator error** which is first discovered by **you** during the **period of the policy**, provided that the **computer systems** downtime lasts longer than the **time franchise**.

For the avoidance of doubt, these additional costs need not be less than **your** expected **income loss** had these measures not been taken.

SECTION E: VOLUNTARY AND REGULATORY SHUTDOWN

We agree to reimburse **you** for **your income loss** and **extra expense** sustained during the **indemnity period** as a result of an interruption to **your business operations** where:

a. it is reasonable and necessary to deliberately take **your computer systems** offline in order to manage a **cyber event** and to mitigate a wider loss, provided that the **cyber event** was first discovered by **you** during the **period of the policy**; or
b. a governmental entity or regulatory body with jurisdiction over **you** expressly requires **you** to take **your computer systems** offline during the **period of the policy** in response to a **cyber event**;

provided that the length of time that **your computer systems** are offline exceeds the **time franchise**.

SECTION F: DEPENDENT BUSINESS INTERRUPTION

We agree to reimburse **you** for **your income loss** and **extra expense** sustained during the **indemnity period** as a direct result of an interruption to **your business operations** arising directly out of any sudden, unexpected and continuous outage of computer systems used directly by a **supply chain partner** which is first discovered by **you** during the **period of the policy**, provided that the computer systems downtime lasts longer than the **time franchise** and arises directly out of a **cyber event**, **system failure** or **operator error**.

SECTION G: CONSEQUENTIAL REPUTATIONAL HARM

We agree to reimburse **you** for **your income loss** sustained during the **reputational harm period** as a direct result of the loss of current or future customers, caused by damage to **your** reputation as a result of a **cyber event** first discovered by **you** during the **period of the policy**.

SECTION H: LOST OR MISSED BIDS

We agree to reimburse **you** for **your income loss** sustained during the **reputational harm period** as a result of **your** failure to make or win a bid or request for proposal (RFP) for a contract arising directly from a **cyber event** first discovered by **you** during the **period of the policy**.

SECTION I: CLAIM PREPARATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred to determine the amount of **your income loss** sustained following an interruption to **your business operations** covered under INSURING CLAUSE 4. **We** will only pay these costs where they are incurred with an expert appointed by the **claims manager**.

INSURING CLAUSE 5: NETWORK SECURITY & PRIVACY LIABILITY

SECTION A: NETWORK SECURITY LIABILITY

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including the establishment of any consumer redress fund and associated expenses) as a result of any **claim** arising out of a **cyber event** first discovered by **you** during the **period of the policy** that results in:

a. the transmission of malware to a **third party's** computer system;
b. **your computer systems** being used to carry out a denial of service attack;
c. **your** failure to prevent unauthorized access to information stored or applications hosted on **your computer systems** or a **third party's** computer systems; or
d. identity theft, experienced by **your employees**, **senior executive officers** or any **third party**.

We will also pay **costs and expenses** on **your** behalf.

SECTION B: PRIVACY LIABILITY

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including the establishment of any consumer redress fund and associated expenses) as a result of any **claim** arising out of a **cyber event** first discovered by **you** during the **period of the policy** that results in:

a. an actual or suspected disclosure of or unauthorized access to any Personally Identifiable Information (PII), including payment card information or Protected Health Information (PHI);
b. **your** failure to adequately warn affected individuals of a **privacy breach**, including the failure to provide a data breach notification in a timely manner;
c. a breach of any rights of confidentiality as a direct result of **your** failure to maintain the confidentiality of any data pertaining to an **employee** or **senior executive officer**;
d. a breach of any rights of confidentiality, including a breach of any provisions of a non-disclosure agreement or breach of a contractual warranty relating to the confidentiality of commercial information, PII, or PHI;
e. a breach of any part of **your** privacy policy; or
f. actual or suspected disclosure of or unauthorized access to **your** data or data for which **you** are responsible.

We will also pay **costs and expenses** on **your** behalf.

SECTION C: MANAGEMENT LIABILITY

We agree to pay on behalf of any board member, C-level executive, in-house lawyer and risk manager of the **company** (including **your** Chief Information Security Officer, Chief Information Officer, Chief Technology Officer or their functional equivalents), all sums they become legally obliged to pay as a result of any **claim** made against them arising directly out of a **cyber event** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on their behalf.

However, **we** will not make any payment under this Section for which the board member, C-level executive, in-house lawyer or risk manager is entitled to indemnity under any other insurance, except for any additional sum which is payable over and above the other insurance.

SECTION D: REGULATORY FINES, PENALTIES AND INVESTIGATION COSTS

We agree to pay on **your** behalf any fines and penalties resulting from a **regulatory investigation** arising as a direct result of a **cyber event** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on **your** behalf.

SECTION E: PCI FINES, PENALTIES AND ASSESSMENTS

We agree to pay on **your** behalf any fines, penalties and card brand assessments including fraud recoveries, operational reimbursements, non-cooperation costs and case management fees, which **you** become legally obliged to pay to **your** acquiring bank or payment processor as a direct result of a **payment card breach** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on **your** behalf.

SECTION F: CONTINGENT BODILY INJURY

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimant's costs and expenses) as a result of any **claim** arising out of **bodily injury** caused as a direct result of a **cyber event** affecting **your computer systems** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on **your** behalf.

However, **we** will not make any payment under this Section for which **you** are entitled to indemnity under any other insurance, except for any additional sum which is payable over and above the other insurance.

INSURING CLAUSE 6: CRIMINAL REWARD COVER

We agree to reimburse **you** for any reasonable sums necessarily incurred with **our** prior written agreement to pay any person or organization, other than:

a. any external or internal auditor of the **company**; or
b. any individual or organization who manages or supervises the individuals stated in a. above;

for information not otherwise available which directly results in the arrest and conviction of any person or organization who is committing or has committed any illegal act directly relating to a claim covered under **INSURING CLAUSES 1**, **2**, **3**, **4** or **5**.

INSURING CLAUSE 7: MEDIA LIABILITY

SECTION A: DEFAMATION

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' costs and expenses) as a result of any **claim** first made against **you** during the **period of the policy** or any applicable optional extended reporting period for any:

a. defamation, including but not limited to libel, slander, trade libel, product disparagement and injurious falsehood; or
b. emotional distress or outrage based on harm to the character or reputation of any person or entity;

arising out of any **media content** (including any **media content** that has been created, in whole or in part, by artificial intelligence programmes or where such programmes have been used to assist in the creation of **media content**).

We will also pay **costs and expenses** on **your** behalf.

SECTION B: INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' costs and expenses) as a result of any **claim** first made against **you** during the **period of the policy** or any applicable optional extended reporting period for any:

a. infringement of any intellectual property rights, including, but not limited to, copyright, trademark, trade dilution, trade dress, commercial rights, design rights, domain name rights, image rights, moral rights, service mark or service name, but not including patent;
b. act of passing-off, piracy or plagiarism or any misappropriation of content, concepts, format rights or ideas or breach of a contractual warranty relating to intellectual property rights;
c. breach of any intellectual property rights license acquired by **you**; or
d. failure to attribute authorship or provide credit;

arising out of any **media content** (including any **media content** that has been created, in whole or in part, by artificial intelligence programmes or where such programmes have been used to assist in the creation of **media content**).

We will also pay **costs and expenses** on **your** behalf.

INSURING CLAUSE 8: TECHNOLOGY ERRORS AND OMISSIONS

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' costs and expenses) as a result of any **claim** first made against **you** during the **period of the policy** or any applicable optional extended reporting period arising out of any act, error, omission or breach of contract in the provision of **your technology services**.

We will also pay **costs and expenses** on **your** behalf.

INSURING CLAUSE 9: COURT ATTENDANCE COSTS

We agree to reimburse **you** for any reasonable sums necessarily incurred by **you** with **our** prior written agreement (which will not be unreasonably withheld) to attend court or any tribunal, arbitration, adjudication, mediation or other hearing in connection with any claim for which **you** are entitled to indemnity under this Policy.

HOW MUCH WE WILL PAY

YOUR MAXIMUM LIMITS UNDER THIS POLICY

The maximum amount payable by **us** under this Policy for any one claim or series of related claims is the **policy limit** plus the **incident response limit**.

The maximum amount payable by **us** under any Insuring Clause for any one claim or series of related claims is the amount shown as the limit in the Declarations page for that Insuring Clause.

The maximum amount payable by **us** under any Section for any one claim or series of related claims is the amount shown as the limit in the Declarations page for that Section.

HOW YOUR LIMITS OPERATE

In respect of **INSURING CLAUSES 1**, **2**, **3**, **4** and **6**, the **policy limit** and the **incident response limit** are provided on an each and every claim basis. This means that the **policy limit** and the **incident response limit** are not subject to an aggregate limit and the full **policy limit** and **incident response limit** will be available to **you** for any unrelated claims for which **you** are entitled to cover under this Policy.

For example, if **you** have a **policy limit** of $1,000,000 and a claim erodes $800,000 of that **policy limit**, should **you** notify a subsequent unrelated and covered claim under this Policy, the full $1,000,000 **policy limit** will be available to **you** for the subsequent claim. The **incident response limit** operates in the same manner.

In respect of **INSURING CLAUSES 5**, **7**, **8** and **9**, the maximum amount payable under this Policy in total aggregate will be the **policy limit**.

YOUR MAXIMUM LIMIT FOR RELATED INCIDENTS

Where more than one claim arises from the same original cause or single source or event, all of those claims will be deemed to be one claim and only one **policy limit** and one **incident response limit** will apply in respect of that claim.

PAYMENT FOR PHYSICAL GOODS

If **we** make any payment under **INSURING CLAUSE 2** (**SECTION D** only), **we** will do so on a cost price basis. This means that any payment **we** make will be based on the original purchase price or cost of production of **your** tangible property and will not include **your** loss of profit.

PAYMENT FOR LOSS INCURRED BEFORE TIME FRANCHISE ELAPSED

In respect of **INSURING CLAUSE 4** (**SECTIONS C**, **D**, **E** and **F** only), where **you** are entitled to cover for any **income loss** or **extra expense**, any **income loss** or **extra expense** incurred before the **time franchise** elapsed will also be covered.

YOUR LIABILITY COVERAGES

In respect of **INSURING CLAUSES 5**, **7**, **8** and **9**, **we** may at any time pay to **you** in connection with any **claim** the amount of the **policy limit** (after deduction of any amounts already paid). Upon that payment being made, **we** will relinquish the conduct and control of the **claim** and be under no further liability in connection with that **claim** except for the payment of **costs and expenses**

incurred prior to the date of such payment (unless the **policy limit** is stated to be inclusive of **costs and expenses**).

If **costs and expenses** are stated in the Declarations page to be in addition to the **policy limit** plus the **incident response limit**, or if the operation of local laws requires **costs and expenses** to be paid in addition to the **policy limit** plus the **incident response limit**, and if a damages payment in excess of the **policy limit** plus the **incident response limit** has to be made to dispose of any **claim**, **our** liability for **costs and expenses** will be in the same proportion as the **policy limit** plus the **incident response limit** bears to the total amount of the damages payment.

YOUR DEDUCTIBLE

YOUR AGGREGATE DEDUCTIBLE

The **deductible** operates on a single aggregate basis and is the maximum amount **you** will be liable to pay for all claims under this Policy. This means that only one **deductible** is payable by **you**. Upon total erosion of the **deductible**, **you** will have no further liability to make any payment under this Policy. If any expenditure is incurred by **us** which falls within the amount of the **deductible**, then **you** will reimburse that amount to **us** upon **our** request.

For example, if **you** have a **deductible** of $5,000 and make a claim where costs exceed this amount, should **you** notify a subsequent claim under this Policy, no **deductible** will apply to that claim and **you** will have no further liability to make any payment under this Policy.

NIL DEDUCTIBLE SECTIONS

You will not be liable to pay for any portion of a claim covered under **INSURING CLAUSES 1** (**SECTIONS A** or **G** only), **4** (**SECTION I** only) or **9**.

YOUR TIME FRANCHISE

In respect of **INSURING CLAUSE 4** (**SECTIONS C**, **D**, **E** and **F** only), a single **time franchise** and **indemnity period** will apply to each claim. Where the same original cause or single source or event causes more than one period of computer systems downtime these will be considered one period of computer systems downtime whose total duration is equal to the cumulative duration of each individual period of computer systems downtime.

DEFINITIONS

1. **"Approved claims panel providers"** means

   the approved claims panel providers stated in the Declarations page.

2. **"Bodily injury"** means

   death, bodily injury, mental injury, illness or disease.

3. **"Botnetting"** means

   the unauthorized use of **your computer systems** by a **third party** for the purpose of launching a denial of service attack or hacking attack against another **third party**.

4. **"Business operations"** means

   the business operations stated in the Declarations page.

5. **"Claim"** means

   a. a written demand for compensation;
   b. a written request for a retraction or a correction;
   c. a threat or initiation of a lawsuit; or
   d. a disciplinary action or **regulatory investigation**.

   made against **you**.

6. **"Claims managers"** means

   the claims managers stated in the Declarations page.

7. **"Client"** means

   any **third party** with whom **you** have a contract in place for the supply of **your** business services or products in return for a fee, or where a fee would normally be expected to be paid.

8. **"Company"** means

   the company named as the Insured in the Declarations page or any **subsidiary**.

9. **"Computer systems"** means

   all electronic computers used directly by **you**, including operating systems, software, hardware and all communication and open system networks and any data or websites wheresoever hosted, off-line media libraries and data back-ups and mobile devices including but not limited to smartphones, iPhones, tablets or personal digital assistants.

   "**Computer systems**" also means supervisory control and data acquisition (SCADA) systems, industrial control systems and other similar operational technology.

10. **"Continuity date"** means

    the **inception date** or if **you** have maintained uninterrupted insurance of the same type with **us**, the date this insurance was first incepted with **us**.

11. **"Costs and expenses"** means

    a. **third party** legal and professional expenses (including disbursements) reasonably incurred in the defense of **claims** or circumstances which could reasonably be

expected to give rise to a **claim** or in quashing or challenging the scope of any injunction, subpoena or witness summons;

b. any post judgment interest; and
c. the cost of appeal, attachment and similar bonds including bail and penal bonds.

Subject to all **costs and expenses** being incurred with the **claims managers**' prior written agreement (which will not be unreasonably withheld).

12. **"Cryptojacking"** means

    the unauthorized use of **your computer systems** by a **third party** for the sole purpose of cryptocurrency mining activities.

13. **"Cyber event"** means

    any actual or suspected unauthorized system access, electronic attack or **privacy breach**, including an attack that utilizes artificial intelligence (AI), denial of service attack, cyber terrorism, hacking attack, Trojan horse, phishing attack, man-in-the-middle attack, application-layer attack, compromised key attack, malware infection (including spyware or ransomware), computer virus or actions of a rogue **employee**.

14. **"Cyber incident response line"** means

    the telephone number stated as the cyber incident response line in the Declarations page.

15. **"Cyber war"** means

    any unauthorized access to or electronic attack on computer systems, carried out by or on behalf of a **state**, that directly results in another **state** becoming an **impacted state**.

16. **"Deductible"** means

    the amount stated as the aggregate deductible in the Declarations page.

17. **"Employee"** means

    any employee of the **company**, any volunteer working for the **company** and any individual working for the **company** as an independent contractor.

    "**Employee**" does not mean any **senior executive officer**.

18. **"Expiry date"** means

    the expiry date stated in the Declarations page.

19. **"Extra expense"** means

    your reasonable sums necessarily incurred in addition to **your** normal operating expenses to mitigate an interruption to and continue **your business operations**, provided that the costs are less than **your** expected **income loss** sustained had these measures not been taken.

20. **"Impacted state"** means

    any **state** that suffers a major detrimental impact on its:

    a. ability to function; or
    b. defense and security capabilities;

    as a direct result of any unauthorized access to or electronic attack on computer systems, carried out by or on behalf of another **state**.

21. **"Inception date"** means

    the inception date stated in the Declarations page.

22. **"Incident response limit"** means

    the highest individual limit available where cover is applicable under **INSURING CLAUSE 1** as stated in the Declarations page.

23. **"Income loss"** means

    your income that, had the **cyber event**, **system failure** or **operator error** which gave rise to the claim not occurred, would have been generated directly from **your business operations** (less sales tax) during the **indemnity period** or **reputational harm period**, less:

    a. actual income (less sales tax) generated directly from **your business operations** during the **indemnity period** or **reputational harm period**; and
    b. any cost savings achieved as a direct result of the reduction in income.

24. **"Indemnity period"** means

    the period starting from the first occurrence of:

    a. the **computer systems** downtime; or
    b. the downtime of computer systems used directly by a **supply chain partner**;

    and lasting up to the period stated as the indemnity period in the Declarations page.

25. **"Loss"** means

    any direct financial loss sustained by the **company**.

26. **"Media content"** means

    any content created or disseminated by **you** or on **your** behalf, including but not limited to content disseminated through books, magazines, brochures, social media, billboards, websites, mobile applications, television and radio.

    "**Media content**" does not include any:

    a. tangible product design;
    b. industrial design;

c. architectural or building services;
d. any advertisement created by **you** for a **third party**;
e. business, company, product or trading name;
f. product packaging or labeling; or
g. software products.

27. **"Operator error"** means

    any unintentional human error in entering or amending electronic data within **your computer systems** or in the upgrade, maintenance or configuration of those **computer systems**, where the proximate cause is not physical damage to any tangible equipment or property.

    "**Operator error**" does not mean any error in the design or architecture of any **computer systems**.

28. **"Payment card breach"** means

    an actual or suspected unauthorized disclosure of payment card data stored or processed by **you** arising out of an electronic attack, accidental disclosure or the deliberate actions of a rogue **employee**.

    "**Payment card breach**" does not mean a situation where payment card data is deliberately shared with or sold to a **third party** with the knowledge and consent of a **senior executive officer**.

29. **"Period of the policy"** means

    the period between the **inception date** and the **expiry date** or until the Policy is canceled in accordance with **CONDITION 5**

30. **"Policy limit"** means

    the highest individual limit available where cover is applicable under any Insuring Clause or Section as stated in the Declarations page.

31. **"Premium"** means

    the amount stated as the premium in the Declarations page and any subsequent adjustments.

32. **"Privacy breach"** means

    an actual or suspected unauthorized disclosure of information (including information in electronic, paper or audio format) arising out of an electronic attack, accidental disclosure, theft or the deliberate actions of a rogue **employee** or **third party**.

    "**Privacy breach**" does not mean a situation where information is deliberately shared with or sold to a **third party** with the knowledge and consent of a **senior executive officer**.

33. **"Regulatory investigation"** means

    a formal hearing, official investigation, examination, inquiry, legal action or any other similar proceeding initiated by a governmental, regulatory, law enforcement, professional or statutory body against **you**.

34. **"Reputational harm period"** means

    the period starting from when the **cyber event** is first discovered and lasting for the period stated as the reputational harm period in the Declarations page.

35. **"Senior executive officer"** means

    board members, C-level executives, in-house lawyers and risk managers of the **company**.

36. **"State"** means

    sovereign state.

37. **"Subsidiary"** means

    any entity which the **company** has majority ownership of, meaning more than 50% ownership, on or before the **inception date**.

38. **"Supply chain partner"** means

    any:

    a. **third party** that provides **you** with hosted computing services including infrastructure, platform, file storage and application level services; or
    b. **third party** listed as a supply chain partner in an endorsement attaching to this policy which **we** have issued.

39. **"System failure"** means

    any sudden, unexpected and continuous downtime of **your computer systems** which renders them incapable of supporting their normal business function and is caused by an application bug, an internal network failure or hardware failure.

    However, in respect of **INSURING CLAUSE 4** (**SECTION F** only), **system failure** also means any sudden, unexpected and continuous downtime of computer systems used directly by a **supply chain partner** which renders them incapable of supporting their normal business function and is caused by an application bug, an internal network failure or hardware failure.

    "**System failure**" does not mean a **cyber event**.

40. **"Technology services"** means

    the supply by **you** of technology services to **your client**, including but not limited to hardware, software, data processing, internet services, data and application hosting, computer systems analysis, consulting, training, programming, installation, integration, support and network management.

41. **"Third party"** means

    any person who is not an **employee** or any legal entity that is not the **company**.

42. **"Time franchise"** means

    the number of hours stated as the time franchise in the Declarations page.

43. **"War"** means

    any physical:

    a. war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), civil war, rebellion, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power; or
    b. action taken in controlling, preventing, suppressing or in any way relating to a. above.

44. **"We/our/us"** means

    the underwriters stated in the Declarations page.

45. **"You/your"** means

    the **company**, **employees** and **senior executive officers** solely acting in the normal course of the **company's business operations**.

EXCLUSIONS

We will not make any payment under this Policy:

1. Antitrust

   in respect of **INSURING CLAUSES 7** and **8**, for or arising out of any actual or alleged antitrust violation, restraint of trade, unfair competition, false, deceptive or unfair trade practices, violation of consumer protection laws or false or deceptive advertising.

2. Associated companies

   a. in respect of any **claim** made by any company, firm or partnership in which the **company** has greater than a 10% executive or financial interest, unless the **claim** emanates from an independent **third party**;
   b. in respect of any **claim** made by any company, firm, partnership or individual which has greater than a 10% executive or financial interest in the **company**, unless the **claim** emanates from an independent **third party**;
   c. arising out of or resulting from any of **your** activities as a trustee, partner, officer, director or employee of any employee trust, charitable organization, corporation, company or business other than that of the **company**; or
   d. in respect of any **claim** made by or on behalf of the **company** against a **third party**.

3. **Betterment**

   which results in **you** being in a better financial position or **you** benefitting from upgraded versions of **your computer systems** as a direct result of the event which gave rise to the claim under this policy.

   However, in the event of a hacking attack, malware infection or computer virus, when rebuilding **your computer systems we** will pay the additional costs and expenses incurred to install a more secure and efficient version of the affected **computer system**, provided that the maximum amount **we** will pay is 25% more than the cost that would have been incurred to repair or replace the original model or license. Under no circumstances will **we** pay the cost of acquiring or installing **computer systems** which did not form a part of **your computer systems** immediately prior to the incident which gave rise to the claim.

   This Exclusion will not apply to **INSURING CLAUSES 1** (**SECTION G** only) and **4** (**SECTION B** only).

4. **Bodily injury and property damage**

   arising directly or indirectly out of **bodily injury** or tangible property damage.

   However, this Exclusion will not apply to:

   a. **INSURING CLAUSES 5** (**SECTIONS A**, **B** and **C** only) and **7**, in respect of any **claim** as a direct result of mental injury or emotional distress; and
   b. **INSURING CLAUSE 5** (**SECTION F** only), in respect of any **claim** as a direct result of **bodily injury**.

5. **Chargebacks**

   for any credit card company or bank, wholly or partially, reversing or preventing a payment transaction, unless specifically covered under **INSURING CLAUSE 5** (**SECTION E** only) for which **you** have purchased coverage.

6. **Core infrastructure failure**

   arising directly or indirectly out of any:

   a. failure, material degradation or termination of any core element of the internet, telecommunications or GPS infrastructure that results in a regional, countrywide or global outage of the internet or telecommunications network, including a failure of the core DNS root servers, satellite network or the IP addressing system or an individual state or non-state actor disabling all or part of the internet;
   b. failure in the power supply, including where the failure is caused by any surge or spike in voltage, electrical current or transferred energy; or
   c. failure, disruption or reduction in the supply of utilities, including telecommunications, gas and water infrastructure or services.

7. Known claims and circumstances

   arising out of any actual or suspected **cyber event**, **claim**, **loss**, **operator error**, **system failure** or circumstance which might give rise to a claim under this Policy which a **senior executive officer** was aware of, or ought reasonably to have been aware of, prior to the **continuity date**, including any claim or circumstance notified to any other insurer.

8. Liquidated damages, service credits and penalty clauses

   for liquidated damages or service credits, or arising out of penalty clauses unless **you** would have been liable in the absence of any contract stipulating the liquidated damages or service credits or penalty clauses.

9. Management liability

   for any sums that **your senior executive officers** become legally obliged to pay, including **costs and expenses**, as a result of any **claim** made against them arising out of a **cyber event**.

   However, this Exclusion will not apply to **INSURING CLAUSE 5** (**SECTION C** only).

10. Misleading advertising

    arising directly or indirectly from any advertisement, promotion or product description that is actually or alleged to be false or misleading.

11. Nuclear

    arising directly or indirectly from or contributed to by:

    a. ionizing radiations or contamination by radioactivity from any nuclear fuel or from any nuclear waste from the combustion of nuclear fuel; or
    b. the radioactive, toxic, explosive or other hazardous properties of any explosive nuclear assembly or nuclear component.

12. Patent infringement

    arising directly or indirectly out of the actual or alleged infringement of any patent or inducing the infringement of any patent.

13. Product IP infringement

    arising directly or indirectly from the actual or alleged theft or misappropriation of any trade secret by an **employee** from a former employer of theirs or infringement of any intellectual property right by any product manufactured, designed, formulated, licensed, distributed, or sold by **you** or the misappropriation of any trade secret by **you** or a **third party**.

14. Professional liability

    arising directly out of any negligent advice or professional services provided to a **client** for a fee except when arising directly from a **cyber event**.

    However, this Exclusion will not apply to **INSURING CLAUSE 8**.

15. **Property and hardware costs**

    for any tangible property repair or replacement including the cost of repairing any hardware or replacing any tangible property or equipment that forms part of **your computer systems**.

    However, this Exclusion will not apply to **INSURING CLAUSE 4** (**SECTION B** only).

16. **Terrorism**

    arising directly or indirectly out of:

    a. any act or threat of force or violence by an individual or group, whether acting alone or on behalf of or in connection with any organization or government, committed for political, religious, ideological or similar purposes including the intention to influence any government or to put the public, or any section of the public, in fear; or
    b. any action taken in controlling, preventing, suppressing or in any way relating to a. above.

    However, this Exclusion does not apply to a **cyber event** affecting **your computer systems** or a **supply chain partner**'s computer systems.

17. **Theft of funds held in escrow**

    for theft of money or other financial assets belonging to a **third party** from a bank account held by **you** on their behalf.

    However, this Exclusion will not apply to **INSURING CLAUSE 2** (**SECTION G** only).

18. **Uninsurable fines**

    for fines, penalties, civil or criminal sanctions or multiple, punitive or exemplary damages, unless insurable by law.

19. **Unlawful surveillance**

    in respect of any actual or alleged eavesdropping, wiretapping, or unauthorized audio or video recording committed by **you** or by a **third party** on **your** behalf with the knowledge and consent of **your senior executive officers**.

20. **Unsolicited communications**

    arising directly or indirectly from any actual or alleged violation of:

    a. the CAN-SPAM Act of 2003 or any subsequent amendments to that Act;
    b. the Telephone Consumer Protection Act (TCPA) of 1991 or any subsequent amendments to that Act; or
    c. any other law, regulation or statute relating to unsolicited communication, distribution, sending or transmitting of any communication via telephone or any other electronic or telecommunications device.

However, this Exclusion will not apply to **INSURING CLAUSE 5** (**SECTION A** only).

21. **War and cyber war**

    arising directly or indirectly out of:

    a. **war**; or
    b. **cyber war**.

    However, part b. above will not apply to:

    a. **INSURING CLAUSE 1** (**SECTION A** only); and
    b. that part of any claim relating to any computer systems which are physically located outside of an **impacted state**.

22. **Willful or dishonest acts of senior executive officers**

    arising directly or indirectly out of any willful, criminal, malicious or dishonest act, error or omission by a **senior executive officer** as determined by final adjudication, arbitral tribunal or written admission.

CONDITIONS

1. **What you must do if an incident takes place**

   If any **senior executive officer** becomes aware of any incident which may reasonably be expected to give rise to a claim under this Policy, **you** must:

   a. other than in accordance with **CONDITION 2**, notify the **claims manager** as soon as is reasonably practicable and follow their directions. However, this notification must be made no later than the end of any applicable extended reporting period. A telephone call to **our cyber incident response line** or confirmed notification via **our** cyber incident response app will constitute notification to the **claims manager**;
   b. in respect of **INSURING CLAUSES 2** and **3**, report the incident to the appropriate law enforcement authorities;
   c. provide **us** in a timely manner with any other information and assistance that **we** may request; and
   d. in respect of **INSURING CLAUSE 3**, not incur any costs or promise any payment, including any ransom payment, without **our** prior written agreement (which will not be unreasonably withheld); and
   e. in respect of **INSURING CLAUSES 5**, **7** and **8**, not admit liability for or settle or make or promise any payment or incur any **costs and expenses** without **our** prior written agreement (which will not be unreasonably withheld).

Due to the nature of the coverage offered by this Policy, any unreasonable delay by **you** in co-operating with or notifying the **claims manager** could lead to the size of the claim increasing or to **our** rights of recovery being restricted. **We** will not be liable for that portion of any claim that is due to any unreasonable delay in **you** co-operating with or notifying the **claims manager** of any incident in accordance with this clause. However, if **you** are prevented from co-operating with or notifying **us** by a legal or regulatory obligation then **your** rights under this Policy will not be affected.

If **you** discover a **cyber event you** may only incur costs, other than costs incurred to respond to an extortion demand (including any ransom payment), without **our** prior written consent within the first 72 hours following the discovery and any **third party** costs incurred must be with a company forming part of the **approved claims panel providers**. All other costs may only be incurred with the prior written consent of the **claims manager** (which will not be unreasonably withheld).

We require **you** to provide full details of the incident, including but not limited to:

a. the time, place and nature of the incident;
b. the manner in which **you** first became aware of this incident;
c. the reasons why **you** believe that the incident could give rise to a claim under this Policy;
d. the identity of any potential claimant; and
e. an indication as to the size of the claim that could result from this incident.

In respect of in respect of **INSURING CLAUSES 7** and **8**, if **you** notify an incident that **we** agree is reasonably expected to give rise to a **claim**, **we** will accept any **claim** that arises out of the incident as being notified under this Policy.

2. **What you must do in the event of a circumstance which could give rise to a claim**

In respect of **INSURING CLAUSES 7** and **8**, should a **senior executive officer** become aware of:

a. a situation during the **period of the policy** that could give rise to a **claim**; or
b. an allegation or complaint made or intimated against **you** during the **period of the policy**;

then **you** have the option of whether to report this circumstance to **us** or not. However, if **you** choose not to report this circumstance **we** will not be liable for that portion of any **claim** that is greater than it would have been had **you** reported this circumstance.

If **you** choose to report this circumstance **you** must do so no later than the end of any applicable extended reporting period for it to be considered under this Policy and **we** will require **you** to provide full details of the circumstance, including but not limited to:

a. the time, place and nature of the circumstance;

b. the manner in which **you** first became aware of this circumstance;
c. the reasons why **you** believe that this circumstance could give rise to a **claim**;
d. the identity of the potential claimant; and
e. an indication as to the size of the **claim** that could result from this circumstance.

Any subsequent **claim** arising directly from this circumstance will be deemed to have been made at the time this circumstance was notified to **us** and **we** will regard this **claim** as having been notified under this Policy.

3. Additional insureds

We will indemnify any **third party** as an additional insured under this Policy, but only in respect of sums which they become legally obliged to pay (including liability for claimants' costs and expenses) as a result of a **claim** arising solely out of an act, error or omission committed by **you**, provided that:

a. **you** contracted in writing to indemnify the **third party** for the **claim** prior to it first being made against them; and
b. had the **claim** been made against **you**, then **you** would be entitled to indemnity under this Policy.

Before **we** indemnify any additional insured they must:

a. prove to **us** that the **claim** arose solely out of an act, error or omission committed by **you**; and
b. fully comply with **CONDITION 1** as if they were **you**.

Where a **third party** is treated as an additional insured as a result of this Condition, any **claim** made by that **third party** against **you** will be treated by **us** as if they were a **third party** and not as an insured.

4. Agreement to pay claims (duty to defend)

We have the right and duty to take control of and conduct in **your** name the investigation, settlement or defense of any **claim**. **We** will not have any duty to pay **costs and expenses** for any part of a **claim** that is not covered by this Policy.

You may ask the **claims manager** to consider appointing **your** own lawyer to defend the **claim** on **your** behalf and the **claims manager** may grant **your** request if they consider **your** lawyer is suitably qualified by experience, taking into account the subject matter of the **claim**, and the cost to provide a defense.

We will endeavor to settle any **claim** through negotiation, mediation or some other form of alternative dispute resolution and will pay on **your** behalf the amount **we** agree with the claimant. If **we** cannot settle using these means, **we** will pay the amount which **you** are found

liable to pay either in court or through arbitration proceedings, subject to the **policy limit** and **incident response limit**.

We will not settle any **claim** without **your** consent. If **you** refuse to provide **your** consent to a settlement recommended by **us** and elect to continue legal proceedings in connection with the **claim**, any further **costs and expenses** incurred will be paid by **you** and **us** on a proportional basis, with 80% payable by **us** and 20% payable by **you**. As a consequence of **your** refusal, **our** liability for the **claim**, excluding **costs and expenses**, will not be more than the amount for which the **claim** could have been settled.

5. Cancellation

   This Policy may be canceled with 30 days written notice by either **you** or **us**.

   If **you** give **us** notice of cancellation, the return **premium** will be in proportion to the number of days that the Policy is in effect. However, if **you** have made a claim under this Policy there will be no return **premium**.

   If **we** give **you** notice of cancellation, the return **premium** will be in proportion to the number of days that the Policy is in effect.

   We also reserve the right of cancellation in the event that any amount due to **us** by **you** remains unpaid more than 60 days beyond the **inception date**. If **we** exercise this right of cancellation it will take effect from 14 days after the date the written notice of cancellation is issued.

   The Policy Administration Fee will be deemed fully earned upon inception of the Policy.

6. Continuous cover

   If during the period of a previous renewal of this Policy **you** neglected, through error or oversight only, to report to **us** an incident that might give rise to a **claim**, then provided that **you** have maintained uninterrupted insurance of the same type with **us** since expiry of the previous renewal of this Policy, **we** will permit the incident to be reported to **us** under this Policy and **we** will indemnify **you** under this Policy in respect of any **claim** that arises out of the incident, provided:

   a. the indemnity will be subject to the applicable limit of liability of the previous renewal of this Policy under which the incident should have been reported to **us** or the applicable **policy limit** plus the **incident response limit**, whichever is the lower;
   b. **we** may reduce the indemnity entitlement by the monetary equivalent of any prejudice which has been suffered as a result of the delayed notification; and
   c. the indemnity will be subject to all other terms and conditions of this Policy.

   We require **you** to provide full details of the incident, including but not limited to:

a. the time, place and nature of the incident;
b. the manner in which **you** first became aware of this incident;
c. reasons why **you** believe that this incident could give rise to a **claim**;
d. the identity of the potential claimant; and
e. an indication as to the size of the **claim** that could result from this incident.

For the avoidance of doubt, this Condition only applies to incidents that might give rise to a **claim**.

7. **Dispute resolution**

All disputes or differences between **you** and **us** will be referred to mediation or arbitration and will take place in the country of registration of the company named as the insured in the Declarations page.

In respect of any arbitration proceeding **we** will follow the applicable rules of the arbitration association in the country where the company stated as the insured in the Declarations page is registered, the rules of which are deemed incorporated into this Policy by reference to this Condition. Unless the applicable arbitration association rules state otherwise, a single arbitrator will be appointed who will be mutually agreed between **you** and **us**. If **you** and **we** cannot agree on a suitable appointment then **we** will refer the appointment to the applicable arbitration association.

Each party will bear its own fees and costs in connection with any mediation or arbitration proceeding but the fees and expenses of the arbitrator will be shared equally between **you** and **us** unless the arbitration award provides otherwise.

Nothing in this Condition is intended to remove **your** rights under **CONDITION 21**. However, if a determination is made in any mediation or arbitration proceeding, **CONDITION 21** is intended only as an aid to enforce this determination.

8. **Extended reporting period**

An extended reporting period of 60 days following the **expiry date** will be automatically granted at no additional premium. This extended reporting period will cover, subject to all other terms, conditions and exclusions of this Policy:

a. in respect of **INSURING CLAUSES 7** and **8**, any **claim** first made against **you** during the **period of the policy** and reported to **us** during this extended reporting period;
b. in respect of **INSURING CLAUSES 1**, **2**, **3**, **4**, **5** and **6**, any **cyber event**, **loss**, **operator error** or **system failure** first discovered by **you** during the **period of the policy** and reported to **us** during this extended reporting period; and
c. any circumstance that a **senior executive officer** became aware of during the **period of the policy** and reports to **us** during this extended reporting period.

No claim will be accepted by **us** in this 60 day extended reporting period if **you** are entitled to indemnity under any other insurance, or would be entitled to indemnity under such insurance if its limit of liability was not exhausted.

9. **Optional extended reporting period**

   If **we** or **you** decline to renew or cancel this Policy then **you** will have the right to have issued an endorsement providing an optional extended reporting period for the duration stated in the Declarations page which will be effective from the cancellation or non-renewal date.

   This optional extended reporting period will cover, subject to all other terms, conditions and exclusions of this Policy:

   a. in respect of **INSURING CLAUSES 7** and **8**, any **claim** first made against **you** and reported to **us** during this optional extended reporting period, provided that the **claim** arises out of any act, error or omission committed prior to the date of cancellation or non-renewal; and
   b. in respect of **INSURING CLAUSES 1**, **2**, **3**, **4**, **5** and **6**, any **cyber event**, **loss**, **operator error** or **system failure** first discovered by **you** during this optional extended reporting period, provided that the **cyber event**, **loss**, **operator error** or **system failure** first occurred during the **period of the policy**.

   If **you** would like to purchase the optional extended reporting period **you** must notify **us** and pay **us** the optional extended reporting period premium stated in the Declarations page within 30 days of cancellation or non-renewal.

   The right to the optional extended reporting period will not be available to **you** where cancellation or non-renewal by **us** is due to non-payment of the **premium** or **your** failure to pay any amounts in excess of the applicable **policy limit** and **incident response limit** or within the amount of the applicable **deductible** as is required by this Policy in the payment of claims.

   At the renewal of this Policy, **our** quotation of different **premium**, **deductible**, limits of liability or changes in policy language will not constitute non-renewal by **us**.

10. **Fraudulent claims**

    If it is determined by final adjudication, arbitral tribunal or written admission by **you**, that **you** notified **us** of any claim knowing it to be false or fraudulent in any way, **we** will have no responsibility to pay that claim, **we** may recover from **you** any sums paid in respect of that claim and **we** reserve the right to terminate this Policy from the date of the fraudulent act. If **we** exercise this right **we** will not be liable to return any **premium** to **you**. However, this will not affect any claim under this Policy which has been previously notified to **us**.

11. Innocent non-disclosure

    We will not seek to avoid the Policy or reject any claim on the grounds of non-disclosure or misrepresentation except where the non-disclosure or misrepresentation was reckless or deliberate.

12. Insolvency

    Your insolvency will not relieve **us** of any of **our** legal obligations under this contract of insurance where this insolvency does not give rise to a claim under this Policy.

13. Mergers and acquisitions

    If **you** acquire an entity during the **period of the policy** whose annual revenue does not exceed 20% of the **company's** annual revenue, as stated in its most recent financial statements, cover is automatically extended under this Policy to include the acquired entity as a **subsidiary**.

    If **you** acquire an entity during the **period of the policy** whose annual revenue exceeds 20% of the **company's** annual revenue, as stated in its most recent financial statements, cover is automatically extended under this Policy to include the acquired entity as a **subsidiary** for a period of 45 days.

    We will consider providing cover for the acquired entity after the period of 45 days if:

    a. **you** give **us** full details of the entity within 45 days of its acquisition; and
    b. **you** accept any amendment to the terms and conditions of this Policy or agree to pay any additional **premium** required by **us**.

    In the event **you** do not comply with a. or b. above, cover will automatically terminate for the entity 45 days after the date of its acquisition.

    Cover for any acquired entity is only provided under this Policy for any act, error or omission committed on or after the date of its acquisition.

    No cover will be automatically provided under this Policy for any acquired entity:

    a. whose business activities are materially different from **your** business activities;
    b. that has been the subject of any lawsuit, disciplinary action or regulatory investigation in the 3 year period prior to its acquisition; or
    c. that has experienced a **cyber event** in the 3 year period prior to its acquisition, if the **cyber event** cost more than the highest **deductible** of this Policy.

    If during the **period of the policy you** consolidate, merge with or are acquired by another entity then all coverage under this Policy will terminate at the date of the consolidation, merger or acquisition unless **we** have issued an endorsement extending coverage, and **you** have agreed to any additional **premium** and terms of coverage required by **us**.

14. **Our rights of recovery**

    If **we** make any payment under this Policy and **you** have any right of recovery against a **third party** in respect of this payment, then **we** will maintain this right of recovery. **You** will do whatever is reasonably necessary to secure this right and will not do anything after the event which gave rise to the claim to prejudice this right.

    We will not exercise any rights of recovery against any **employee** or **senior executive officer**, unless this is in respect of any fraudulent or dishonest acts or omissions as proven by final adjudication, arbitral tribunal or written admission by the **employee** or **senior executive officer**.

    Any recoveries will be applied as follows:

    a. towards any recovery expenses incurred by **us**;
    b. then to **us** up to the amount of **our** payment under this Policy, including **costs and expenses**;
    c. then to **you** as recovery of **your deductible**.

15. **Proceeds of crime recovery**

    Notwithstanding **CONDITION 14**, if **we** have reimbursed **you** for any claim under **INSURING CLAUSES 2** and **3** that subsequently relates to any proceeds of crime that have been forfeited to or seized by any law enforcement authority, or confiscated as part of any legal proceeding, **you** must:

    a. notify **us** as soon as practicable in the event **you** become aware of the forfeiture, seizure or confiscation;
    b. provide **us** with any assistance **we** may request in the recovery of these proceeds of crime, including **your** automatic consent for **us** to initiate, progress secure and finalize any investigation in the recovery; and
    c. reimburse to **us** upon **our** request that part of any payment **we** have made which falls within the amount of any proceeds of crime that **you** have recovered.

16. **Prior subsidiaries**

    Should an entity cease to be a **subsidiary** after the **inception date**, cover in respect of the entity will continue as if it was still a **subsidiary** during the **period of the policy**, but only in respect of an act, error, omission or event occurring prior to the date that it ceased to be a **subsidiary**.

17. **Process for paying business interruption losses**

    In respect of **INSURING CLAUSE 4**, in the event of a claim for any financial loss sustained by **you**, **you** must provide the **claims manager** with **your** calculation of the financial loss including.

    a. how the loss has been calculated and what assumptions have been made; and

b. relevant supporting documents including but not limited to account statements, sales projections, invoices, profit and loss statements, payroll records, **client** contracts and tax records.

If **we** do not agree with **your** calculation of the financial loss, **we** will appoint an expert which will be paid for by **us** to assist the **claims manager** with adjustment of **your** claim.

We may make interim payments to **you** prior to the final settlement of the claim, subject to **you** providing **us** with sufficient evidence to support the requirement of an interim payment and **we** agree the financial loss is covered at the time of the interim payment. Any interim payment will form part of the total amount payable by **us** under the Policy in relation to the claim and will be deducted from the total claim amount payable by **us** to **you**. If any overpayment is made by **us** as a result of any interim payment then **you** will reimburse that amount to **us** upon **our** request.

18. **Process for paying privacy breach notification costs**

Any **privacy breach** notification transmitted by **you** or on **your** behalf must be done with **our** prior written consent. **We** will ensure that notification is compliant with any legal or regulatory requirements and contractual obligations. No offer must be made for financial incentives, gifts, coupons, credits or services unless with **our** prior written consent which will only be provided if the offer is commensurate with the risk of harm.

We will not be liable for any portion of the costs **you** incur under **INSURING CLAUSE 1** (**SECTION E** only) that exceed the costs that **you** would have incurred had **you** gained **our** prior written consent. In the absence of **our** prior written consent **we** will only be liable to pay **you** the equivalent cost of a notification made using the most cost effective means permissible under the governing law.

19. **Sanctions suspension**

It is a condition under this Policy that the provision of cover, the payment of any claim and the provision of any benefit will be suspended, to the extent that the provision of the cover, payment of the claim or provision of the benefit would expose **us** to any sanction, prohibition or restriction under the United Nations resolutions or the trade or economic sanctions, laws or regulations of Australia, Canada, the European Union, United Kingdom or United States of America. The suspension will continue until such time **we** would no longer be exposed to the sanction, prohibition or restriction.

20. **Supply chain interruption events**

In respect of **INSURING CLAUSE 4** (**SECTION F** only), it is a condition precedent to liability under this Policy that **you** submit to **us** a written report from the **supply chain partner** confirming the root cause and length of the outage.

21. **Choice of law and service of suit**

In the event of a dispute between **you** and **us** regarding this Policy, the dispute will be governed by the laws of the State of the United States of America shown as the choice of law stated in the Declarations page. **We** agree, at **your** request, to submit to the jurisdiction of a court of competent jurisdiction within the United States of America.

Nothing in this Condition constitutes or should be understood to constitute a waiver of **our** rights to commence an action in any court of competent jurisdiction in the United States of America, to move an action to a United States District Court, or to seek a transfer of a case to another court as permitted by the laws of the United States of America or the laws of any State of the United States of America.

It is further agreed that service of process in such suit may be made upon the law firm stated in the Declarations page and that in any suit instituted against **us**, **we** will abide by the final decision of such court or of any appellate court in the event of an appeal. The law firm stated in the Declarations page is authorized and directed to accept service of process on **our** behalf in any such suit and, at **your** request, to give a written undertaking to **you** that they will enter a general appearance on **our** behalf in the event such suit is instituted.

Additionally, in accordance with the statute of any state, territory or district of the United States which makes such a provision, **we** hereby designate the Superintendent, Commissioner or Director of Insurance or other officer specified for that purpose in the statute, or his successor or successors in office, as **our** true and lawful attorney upon whom may be served any lawful process in any action, suit or proceeding instituted by **you** arising out of this Policy. The law firm stated in the Declarations page is hereby designated as the firm to whom the above mentioned officer is authorized to mail such process or a copy thereof.