

TABLE OF CONTENTS

	<u>Page</u>
I. INSURING AGREEMENTS.....	4
A. THIRD PARTY INSURING AGREEMENTS	4
A.1 INFORMATION PRIVACY LIABILITY	4
A.2 REGULATORY DEFENCE AND AWARDS	4
A.3 PCI DSS LIABILITY	4
A.4 MEDIA LIABILITY	4
A.5 NETWORK SECURITY LIABILITY	5
B. FIRST PARTY INSURING AGREEMENTS.....	5
B.1 INCIDENT RESPONSE	5
B.1.1 Legal Privacy Breach Costs.....	5
B.1.2 Incident Forensic Costs	5
B.1.3 Notification Costs.....	6
B.1.4 Call Centre Costs	6
B.1.5 Credit Monitoring Costs	6
B.1.6 Identity Monitoring	6
B.1.7 Public Relations Costs.....	7
B.2 CYBER EXTORTION LOSSES.....	7
B.3 DATA RECOVERY COSTS	7
B.4 BRICKING COSTS	8
B.5 BUSINESS INTERRUPTION	8
B.6 CONTINGENT BUSINESS INTERRUPTION.....	8
B.7 SYSTEM FAILURE BUSINESS INTERRUPTION	9
B.8 SYSTEM FAILURE CONTINGENT BUSINESS INTERRUPTION.....	9
B.9 REPUTATION PROTECTION.....	9
B.10 KEY PERSON COVER	10
C. FINANCIAL CRIME AND FRAUD INSURING AGREEMENTS.....	10
C.1 ELECTRONIC THEFT	10
C.2 THEFT OF FUNDS HELD IN ESCROW	10

C.3	TELECOMMUNICATIONS FRAUD	10
C.4	SOCIAL ENGINEERING	11
C.5	CLIENT SOCIAL ENGINEERING LOSS	11
C.6	FRAUDULENT USE OF INSURED ORGANIZATION'S ELECTRONIC IDENTITY	11
C.7	UTILITY AND MARKETING FRAUD	11
D.	ADDITIONAL INSURING AGREEMENTS	12
D.1	REPEAT EVENT MITIGATION	12
D.2	COURT ATTENDANCE COMPENSATION	12
II.	EXCLUSIONS	12
A.	EXCLUSIONS APPLICABLE TO A. THIRD PARTY INSURING AGREEMENTS	12
B.	EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS	15
III.	DEFINITIONS	19
IV.	GENERAL TERMS AND CONDITIONS	27

The Insurers

Effected with certain subscribing insurance companies (hereinafter called “the Insurers”) through Boxx Insurance Inc. as shown in the Declarations.

Insurer’s promise to the Insured

In consideration of the **Insured Organization’s** payment of the premium and in reliance upon the **Insured Organization’s** presentation of the risk, including the **Application**, and subject to the aggregate limit of indemnity, applicable sub-limits and **Retention**, together with the exclusions, conditions, and terms of this **Policy**, the **Insurer** agrees to insure the **Insured** in accordance with this **Policy**.

Philip Baker



Chief Underwriting Officer, Boxx Insurance Inc.

Conditions

THIS POLICY IS WRITTEN ON A CLAIMS-MADE AND REPORTED BASIS. EXCEPT AS OTHERWISE PROVIDED, THIS POLICY COVERS ONLY CLAIMS FIRST MADE AGAINST THE INSURED AND INCIDENTS OR LOSSES FIRST DISCOVERED BY THE INSURED DURING THE POLICY PERIOD, OR ANY APPLICABLE EXTENDED REPORTING PERIOD, AND NOTIFIED TO THE INSURER PURSUANT TO THE INSURED’S OBLIGATIONS.

Please read this **Policy**, together with any endorsements and the Declarations, very carefully. If anything is not correct, please notify the **Insurer** immediately.

In return for the premium the **Named Insured** has paid, the **Insurer** agrees to insure the **Insured** in accordance with the terms and conditions of the **Policy**.

The liability Insuring Agreements of this **Policy** provide claims-made coverage which applies only to **Claims** first made during the **Policy Period**, or any applicable Extended Reporting Period.

The titles of the various sections, paragraphs, and clauses of this **Policy** and any endorsements attached to this **Policy** are inserted solely for convenience or reference and are not to be deemed in any way to limit or affect the provisions to which they relate.

I. INSURING AGREEMENTS

COVERAGE UNDER THIS POLICY IS PROVIDED ONLY FOR THOSE INSURING AGREEMENTS FOR WHICH A LIMIT APPEARS IN THE DECLARATIONS. IF NO LIMIT IS SHOWN FOR AN INSURING AGREEMENT, SUCH INSURING AGREEMENT IS NOT PROVIDED BY THIS POLICY. THE AGGREGATE POLICY LIMIT SHOWN IN ITEM 3 OF THE DECLARATIONS IS THE MOST THE INSURER WILL PAY UNDER THIS POLICY REGARDLESS OF THE NUMBER OF INSURING AGREEMENTS PURCHASED.

A. THIRD PARTY INSURING AGREEMENTS

A.1 INFORMATION PRIVACY LIABILITY

If during the **Policy Period**, any party brings a **Claim** against the **Insured**, the **Insurer** will pay **Claim Expenses** for any actual or alleged:

- (a) breach, violation, or infringement of any right to privacy, consumer data protection law, or other legal protection for **Personal Data**;
- (b) breach of duty to maintain the security or confidentiality of **Personal Data**;
- (c) breach of any duty of confidence, including with respect to any commercial information; or
- (d) breach of any contractual duty to maintain the security or confidentiality of **Personal Data**, including:
 - i. under a payment card processing agreement with any bank or payment processor; or
 - ii. under the **Insured Organization's Privacy Policy** that was in force at the time the **Claim** was made against the **Insured**.

A.2 REGULATORY DEFENCE AND AWARDS

If during the **Policy Period**, any party brings a **Regulatory Claim** against the **Insured**, the **Insurer** will pay **Claim Expenses**, including **Regulatory Awards** and **Privacy Investigation Costs**, for any actual or alleged **Privacy Breach**.

A.3 PCI DSS LIABILITY

If during the **Policy Period**, any party brings a **Claim** against the **Insured** for any actual or alleged breach of **PCI DSS**, the **Insurer** will pay **Claim Expenses**.

A.4 MEDIA LIABILITY

If during the **Policy Period**, any party brings a **Claim** against the **Insured** for a **Media Incident**, the **Insurer** will pay **Claim Expenses**.

A.5 NETWORK SECURITY LIABILITY

If during the **Policy Period**, any party brings a **Claim** against the **Insured**, the **Insurer** will pay the **Insured Organization's Claim Expenses** for any actual or alleged:

- (a) transmission of a **Malicious Code** from the **Insured's Computer System**;
- (b) denial of service attack against a third party emanating from the **Insured's Computer System**;
- (c) unauthorized acquisition, access, use, or disclosure of **Personal Data** or **Corporate Information** that is held or transmitted by an **Insured** in any form; or
- (d) failure to prevent unauthorized electronic access to the **Insured's Computer System**.

B. FIRST PARTY INSURING AGREEMENTS**B.1 INCIDENT RESPONSE**

The limit for Insuring Agreements in B.1. INCIDENT RESPONSE is in addition to the aggregate limit of indemnity for this **Policy** shown in the Declarations.

B.1.1 Legal Privacy Breach Costs

If during the **Policy Period**, the **Insured** discovers or reasonably suspects any **Privacy Breach**, the **Insurer** agrees to pay on the **Insured's** behalf the reasonable and necessary costs incurred by the **Insured Organization** to:

- (a) Provide legal advice to the **Insured** in connection with the **Insured Organization's** investigation of a **Privacy Breach**;
- (b) assist with the preparation of legally required notifications to any regulator and **Data Subjects** affected by a **Privacy Breach** that is covered under this **Policy**; and
- (c) determine and pursue any indemnity owed by a third party to the **Insured Organization** under a written agreement.

B.1.2 Incident Forensic Costs

If during the **Policy Period**, the **Insured** discovers or reasonably suspects any **Privacy Breach**, **Security Failure**, **Illegal Threat**, or **Cyber Attack** against the **Insured Organization**, the **Insurer** agrees to pay on the **Insured Organization's** behalf the reasonable and necessary costs incurred by the **Insured** for:

- (a) computer forensic analysis conducted by third party forensic experts to:
 - confirm whether or not a **Privacy Breach**, **Security Failure**, **Illegal Threat**, or **Cyber Attack** against the **Insured** has occurred, or is occurring;
 - identify any **Data Subjects** affected by a **Privacy Breach** that is covered under this **Policy**; and

- stop or contain the **Privacy Breach, Security Failure, Illegal Threat, or Cyber Attack** against the **Insured Organization**; and

(b) legal fees necessary for the preservation of the attorney-client privilege afforded to forensic reports and findings due to a **Privacy Breach**.

B.1.3 Notification Costs

The **Insurer** agrees to pay on the **Insured Organization's** behalf the reasonable and necessary costs incurred by the **Insured Organization** to notify each **Data Subject** affected by a **Privacy Breach** that is covered under this **Policy**; and any regulatory body, of the **Privacy Breach** where the **Insured Organization** is required by any applicable law or regulation to do so, and for up to 24 months.

Any costs included within this Insuring Agreement related to a voluntary notification require the **Insurer's** prior written consent, such consent not to be unreasonably withheld.

B.1.4 Call Centre Costs

The **Insurer** agrees to pay on the **Insured Organization's** behalf the reasonable and necessary costs incurred by the **Insured Organization** to retain a third party to provide the service of call centre to answer inquiries from **Data Subjects** following notification of the **Privacy Breach** to **Data Subjects**, including those affected in compliance with the requirements for the Personal Information Protection and Electronic Documents Act (PIPEDA) or the Health Information Technology for Economic and Clinical Health Act (HITECH) (U.S.), and for up to 24 months.

Any costs included within this Insuring Agreement related to a voluntary notification require the **Insurer's** prior written consent, such consent not to be unreasonably withheld.

B.1.5 Credit Monitoring Costs

The **Insurer** agrees to pay on the **Insured Organization's** behalf the reasonable and necessary costs incurred by the **Insured Organization** to provide credit monitoring services or other credit protection services to each **Data Subject** affected by a **Privacy Breach** that is covered under this **Policy**, and for up to 24 months.

Any costs included within this Insuring Agreement related to a voluntary notification require the **Insurer's** prior written consent, such consent not to be unreasonably withheld.

B.1.6 Identity Monitoring

The **Insurer** agrees to pay on the **Insured Organization's** behalf the reasonable and necessary costs incurred by the **Insured Organization** to monitor the dark web for the appearance of any information accessed during a **Privacy Breach**, but not

including any overhead costs, general business expenses, salaries, or wages incurred by the **Insured Organization** or any other person or entity entitled to coverage under this **Policy**, and for up to 24 months.

Any costs included within this Insuring Agreement related to a voluntary notification require the **Insurer's** prior written consent, such consent not to be unreasonably withheld.

B.1.7 Public Relations Costs

The **Insurer** agrees to pay on the **Insured Organization's** behalf **Public Relations Costs** incurred by the **Insured Organization** as a direct result of a **Privacy Breach** that is covered under this **Policy**.

Any costs included within this Insuring Agreement related to a voluntary notification require the **Insurer's** prior written consent, such consent not to be unreasonably withheld.

B.2 CYBER EXTORTION LOSSES

During the **Policy Period** and following an **Illegal Threat**, the **Insurer** agrees to pay on the **Insured Organization's** behalf the reasonable and necessary costs incurred by the **Insured** for:

- (a) a consultant appointed by the **Insurer**, or incurred by the **Insured Organization** for advising the **Insured** on the handling and negotiation of the ransom demand;
- (b) the payment of any third party's ransom demand for:
 - i. **Money**; or
 - ii. goods or services (at their market value at the time of their surrender) to the third party making the demand.

B.3 DATA RECOVERY COSTS

If during the **Policy Period**, the **Insured** discovers or reasonably suspects any **Privacy Breach**, **Security Failure**, **Illegal Threat**, **Cyber Attack**, or **System Failure** against the **Insured Organization**, the **Insurer** agrees to pay **Data Recovery Costs** on the **Insured Organization's** behalf.

Data Recovery Costs do not include:

- (a) costs incurred after it has been established that the **Insured's Data Asset** cannot be replaced, restored, or repaired, or access to it cannot be regained;
- (b) the economic value of the **Insured's Data Asset**, including the value of any trade secrets;
- (c) costs to restore, update, or replace the **Insured's Data Asset** to a level beyond that which existed prior to the event, unless the **Insured's Data Asset** can only be replaced, restored or repaired by purchasing a newer equivalent; or

- (d) costs to research or develop the **Insured's Data Asset** or to recreate, gather or assemble facts, concepts, or information needed to reproduce the **Insured's Data Asset**.

B.4 BRICKING COSTS

The **Insurer** agrees to pay the **Insured Organization** the reasonable and necessary costs incurred by the **Insured Organization** rectifying or replacing any part of the **Insured Organization's Computer System** that is rendered nonfunctional or useless for its intended purpose, without being physically damaged, as a direct result of a **Security Failure** or a **Cyber Attack**.

Bricking Costs shall only be incurred by the **Insured Organization** with the **Insurer's** prior written consent, such consent not to be unreasonably withheld.

B.5 BUSINESS INTERRUPTION

The **Insurer** agrees to pay the **Insured Organization's** loss of **Income, Increased Costs of Working**, and the costs to retain a third party forensic accounting firm to determine the **Loss** described in this Insuring Agreement that the **Insured Organization** incurs during the **Indemnity Period** and that results solely and directly from a partial or total interruption to the **Insured Organization's Business** or from a **Voluntary Shutdown** commencing during the **Policy Period** and lasting longer than the **Waiting Period**, as a direct result of a **Privacy Breach, Security Failure, Illegal Threat**, or **Cyber Attack** against the **Insured Organization**.

For the purposes of this Insuring Agreement, **Waiting Period** shall be the period shown in the Declarations with respect to Insuring Agreement B.5 BUSINESS INTERRUPTION.

B.6 CONTINGENT BUSINESS INTERRUPTION

The **Insurer** agrees to pay the **Insured Organization's** loss of **Income, Increased Costs of Working**, and the costs to retain a third party forensic accounting firm to determine the **Loss** described in this Insuring Agreement that the **Insured Organization** incurs during the **Indemnity Period** and that results solely and directly from a partial or total interruption to the **Insured's Business** commencing during the **Policy Period** and lasting longer than the **Waiting Period**, and which is directly caused by a **Security Failure** or a **Cyber Attack** on the **Outsourced Service Provider's Computer System**.

The **Insurer** agrees to pay the **Insured Organization** the reasonable and necessary **Data Recovery Costs**, which are caused directly by a **Security Failure** or a **Cyber Attack** on the **Outsourced Service Provider's Computer System**, to regain access to the **Outsourced Service Provider's Computer System**.

For the purposes of this Insuring Agreement:

- (a) **Waiting Period** shall be the period shown in the Declarations with respect to Insuring Agreement B.6 CONTINGENT BUSINESS INTERRUPTION; and
- (b) **Outsourced Service Provider** shall be treated as an **Insured Organization** for the purposes of the definition of **Security Failure**.

B.7 SYSTEM FAILURE BUSINESS INTERRUPTION

The **Insurer** agrees to pay the **Insured Organization's** loss of **Income, Increased Costs of Working, Data Recovery Costs**, and the costs to retain a third party forensic accounting firm to determine the **Loss** described in this Insuring Agreement that the **Insured Organization** incurs during the **Indemnity Period** and that results solely and directly from a partial or total interruption to the **Insured's Business** commencing during the **Policy Period** and lasting longer than the **Waiting Period**, and which is directly caused by a **System Failure** to the **Insured's Computer System**.

For the purposes of this Insuring Agreement, **Waiting Period** shall be the period shown in the Declarations with respect to Insuring Agreement B.7 SYSTEM FAILURE BUSINESS INTERRUPTION.

B.8 SYSTEM FAILURE CONTINGENT BUSINESS INTERRUPTION

The **Insurer** agrees to pay the **Insured Organization's** loss of **Income, Increased Costs of Working**, and the costs to retain a third party forensic accounting firm to determine the **Loss** described in this Insuring Agreement that the **Insured Organization** incurs during the **Indemnity Period** and that results solely and directly from a partial or total interruption to the **Insured's Business** commencing during the **Policy Period** and lasting longer than the **Waiting Period**, and which is directly caused by a **System Failure** to the **Outsourced Service Provider's Computer System**.

The **Insurer** agrees to pay the **Insured Organization** the reasonable and necessary **Data Recovery Costs**, which are caused directly by a **System Failure** to the **Outsourced Service Provider's Computer System**, to regain access to the **Outsourced Service Provider's Computer System**.

For the purposes of this Insuring Agreement, **Waiting Period** shall be the period shown in the Declarations with respect to Insuring Agreement B.8 SYSTEM FAILURE CONTINGENT BUSINESS INTERRUPTION.

B.9 REPUTATION PROTECTION

The **Insurer** agrees to pay:

- (a) **Public Relations Costs**;
- (b) Reputational Loss to the **Insured Organization's**; and

- (c) the costs to retain a third-party forensic accounting firm to determine the **Loss** described in this Insuring Agreement,

resulting solely and directly from an **Adverse Publication** first published during the **Policy Period** and lasting longer than the **Waiting Period**, as a direct result of an **Incident**.

For the purposes of this Insuring Agreement, **Waiting Period** shall be the period shown in the Declarations with respect to Insuring Agreement B.9 REPUTATION PROTECTION.

B.10 KEY PERSON COVER

The **Insurer** agrees to pay the reasonable and necessary costs incurred by the **Insured Organization** to engage a consultant to:

- (a) undertake the day-to-day work of a **Senior Executive** to the extent that such individual is unable to fulfill his or her usual responsibilities as a direct result of their time being diverted to the management of a covered **Incident**; or
- (b) manage the **Insured's** response to a covered **Incident**, to enable a **Senior Executive** to fulfill his or her usual responsibilities.

C. FINANCIAL CRIME AND FRAUD INSURING AGREEMENTS

The most that the **Insurer** will pay for all Insuring Agreements in this section combined is the amount shown in the Declarations as FINANCIAL CRIME AND FRAUD AGGREGATE LIMIT.

C.1 ELECTRONIC THEFT

If during the **Policy Period**, the **Insured** discovers a **Loss** directly from the taking or misappropriation of **Money**, **Securities**, or tangible property belonging to the **Insured Organization** as a consequence of a **Security Failure**, the **Insurer** will pay the **Insured's Cyber Crime Loss**.

C.2 THEFT OF FUNDS HELD IN ESCROW

If during the **Policy Period**, the **Insured** discovers a **Loss** directly from the criminal taking or misappropriation by a third party of **Money**, **Securities**, or tangible property belonging to another third party from a bank account held by the **Insured Organization** on that third party's behalf as a consequence of a **Security Failure**, the **Insurer** will pay the **Insured's Cyber Crime Loss**.

C.3 TELECOMMUNICATION FRAUD

If during the **Policy Period**, the **Insured** discovers a **Security Failure** that causes telecommunication charges incurred by the **Insured Organization** from its telecommunications provider, the **Insurer** will pay the **Insured's Cyber Crime Loss**.

C.4 SOCIAL ENGINEERING

If during the **Policy Period**, the **Insured** discovers the transfer by the **Insured** of the **Insured Organization's Money, Securities**, or tangible property in direct response to a **Social Engineering Attack**, the **Insurer** will pay the **Insured's Cyber Crime Loss**.

C.5 CLIENT SOCIAL ENGINEERING LOSS

If during the **Policy Period**, the **Insured** discovers a **Client** transferring **Money, Securities**, or tangible property, which the **Insured** was entitled to receive, to a third party in direct response to a **Social Engineering Attack** sent from the **Insured Organization's Computer System**, the **Insurer** will pay the **Insured Organization's Cyber Crime Loss**.

For the purposes of this coverage, the **Client** shall be treated as the **Insured Organization** for the purposes of the definition of **Social Engineering Attack**.

C.6 FRAUDULENT USE OF INSURED ORGANIZATION'S ELECTRONIC IDENTITY

If during the **Policy Period**, and as a direct result of a **Security Failure**, the **Insured Organization** discovers the fraudulent or dishonest use of the electronic identity of the **Insured Organization's Business** to:

- (a) obtain credit in the **Insured Organization's** name;
- (b) electronically sign any contract;
- (c) create or use of a website designed to copy or imitate that of the **Insured Organization's Business**; or
- (d) allow a third party to use the **Insured Organization's** digital or electronic identity;

the **Insurer** will pay the **Insured Organization's Cyber Crime Loss**.

C.7 UTILITY AND MARKETING FRAUD

If during the **Policy Period**, and as a direct result of a **Cyber Attack** against the **Insured's Computer System**, the **Insured** discovers any of the following:

- (a) the increased cost of power;
- (b) the increased cost of internet usage;
- (c) the costs to restore the **Insured's** search engine rating; or
- (d) the cost of any malicious pay-per-click clicks;

the **Insurer** will pay the reasonable and necessary associated costs suffered or incurred by the **Insured**; provided, however, that the **Insurer** will not pay for any normal overhead costs, general business expenses, salaries, or wages incurred by the **Insured**, or any other person or entity entitled to coverage under this **Policy**.

D. ADDITIONAL INSURING AGREEMENTS**D.1 REPEAT EVENT MITIGATION**

Following any payment under Insuring Agreements in Sections A., B., or C. above, the **Insurer** will pay the reasonable and necessary costs and expenses incurred by the **Insured Organization** to:

- (a) purchase a software license, of up to 12 months, to upgrade existing hardware or software forming part of the **Insured's Computer System**; and
- (b) obtain risk management advice,

which is necessary to prevent or minimize the chance of a reoccurrence of the same event that gave rise to the payment under this **Policy**.

D.2 COURT ATTENDANCE COMPENSATION

If any individual within the definition of the **Insured** attends court as a witness in connection with a **Claim** against the **Insured Organization** that is covered under this **Policy**, the **Insurer** will pay the **Insured** the amount stated in the Declarations as compensation for each day, or part of a day, that their attendance is required by the **Insurer**.

Cover for court attendance compensation is in addition to the aggregate limit of indemnity for this **Policy** shown in the Declarations.

II. EXCLUSIONS

This **Policy** does not apply to, and the **Insurer** will not make any payment for, any **Claim**, **Incident**, **Loss**, or any other liability under this **Policy** directly or indirectly caused by, arising out of, resulting from, based upon, or relating to:

A. EXCLUSIONS APPLICABLE TO A. THIRD PARTY INSURING AGREEMENTS**A.1 BREACH OF PROFESSIONAL SERVICES**

negligent advice or professional services provided by the **Insured** to a **Client** for a fee, other than where the **Claim** arises directly from a **Cyber Attack** or a **Privacy Breach**.

A.2 BREACH OF CONTRACT

any contractual liability, whether oral or written. However, this exclusion shall not apply to:

- (a) the **Insured Organization's** contractual obligation to maintain the security of **Personal Data** or **Corporate Information**, or to the extent the **Insured** would have been liable in the absence of a contract or agreement;
- (b) the **Insured Organization's** obligation to comply with **PCI DSS** under a merchant services agreement or similar contract;
- (c) the **Insured Organization's** unintentional violation of the **Insured Organization's Privacy Policy**; or
- (d) solely with respect to Insuring Agreement A.4 MEDIA LIABILITY, any covered **Claim** for misappropriation of ideas under implied contract.

A.3 CLAIMS BROUGHT BY A RELATED PARTY

any **Claim** brought by any person or entity within the definition of the **Insured** or any party with a financial, executive, or managerial interest in the **Insured Organization**, including any parent company or any party in which the **Insured Organization** has a financial, executive, or managerial interest.

However, this exclusion does not apply to a **claim** based on liability to an independent third party directly arising out of the **Insured Organization's Business**.

A.4 INTELLECTUAL PROPERTY

the actual or alleged infringement of third-party intellectual property rights with respect to the manufacture, import, design, package, or trade dress of goods or services sold by, or on behalf of, any individual or entity of the **Insured**.

A.5 MEDIA LIABILITY

solely with respect to Insuring Agreement A.4 MEDIA LIABILITY:

- (a) any **Claim** made by any person or entity that the **Insured** currently employs or engages, or was formerly employed or engaged, including but not limited to any individual within the definition of the **Insured**;
- (b) any **Claim** made by or on behalf of a music licensing entity or organization, including, but not limited to, ASCAP, SECAC, BMI, or the RIAA, on their behalf or for others;
- (c) any **Claim** based upon, arising out of, or attributable to licensing fees or royalties ordered, directed, or agreed to be paid by the **Insured** pursuant to a judgment, arbitration award, settlement agreement or similar order or agreement, for the continued or future use of any intellectual property right;
- (d) any **Claim** based upon, arising out of, or attributable to false or deceptive advertising or promotion, any unfair or deceptive trade practices with respect to the sale of any goods, products, or services, any inaccurate, inadequate or

incomplete description of the price of goods, products, or services, disclosure of fees, representations with the respect to authenticity of any product, or the failure of any goods, products or services to conform with the advertised quality or performance;

- (e) any **Claim** alleging, based upon, arising out of, or attributable to any gambling, contest, game of chance or skill, lottery, or promotional game, including tickets or coupons or over-redemption related thereto; or
- (f) any **Claim** based upon, arising out of, or attributable to any actual or alleged error, omission, or misstatement in any labelling, packaging, or instructional content, including but not limited to any failure to warn or instruct as to any goods, products, or services.

A.6 INSURED VS. INSURED

- (a) any **Claim** made by or on behalf of the **Insured Organization** against another member of the **Insured Organization**. However, this exclusion shall not apply to any **Claim**:
 - i. brought by an **Employee** as a result of a **Privacy Breach** or **Security Failure**; or
 - ii. brought by an **Additional Insured** against the **Insured Organization**.
- (b) any **Claim** brought by the **Insured** or any of the **Insured's Employees** or shareholders due to the personal liability incurred by a **Senior Executive** when acting in that capacity or managing **Insured Organization's Business**.

A.7 EMPLOYMENT PRACTICES

employment practices. However, this exclusion shall not apply to **Claims** related to the **Privacy Breach** of an **Employee's Personal Data** that the **Insured Organization** is responsible for safeguarding.

A.8 UNLAWFUL COLLECTION OF DATA

the actual or alleged failure to comply with any statute, law, decree, regulation, or rule with respect to the unlawful collection, use, handling, storage, retention, processing, or destruction of biometric data, biometric information and/or biometric identifiers.

A.9 DISCRIMINATION

any actual or alleged discrimination of any kind. However, this exclusion shall not apply to **Claims** related to the **Privacy Breach** of an **Employee's Personal Data** that the **Insured Organization** is responsible for safeguarding.

A.10 SECURITIES

any purchase, sale, or offer, or solicitation of an offer, to purchase or sell **Securities**, or the violation of any federal, state or local securities law, and any amendments thereto; however, this exclusion does not apply to a **Privacy Breach**.

A.11 PRIOR ACTS

any **Incident**, act, error, or omission that took place prior to the Retroactive Date as stated in the Declarations.

B. EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS**B.1 INFRASTRUCTURE FAILURE**

any failure or interruption of service provided by an internet service provider, telecommunications provider, utilities supplier, or other infrastructure provider. However, this exclusion does not apply where the **Insured Organization** provides such services to a third party for a fee as part of the **Insured Organization's Business**.

B.2 INTELLECTUAL PROPERTY

any actual or alleged infringement, use or misappropriation of any intellectual property, including but not limited to patent, trade secret, copyright, trademark, trade dress, service mark, service name, title or slogan, or any publicity rights violations, cybersquatting violations, moral rights violations, or any act of passing-off.

However, this exclusion does not apply to:

- (a) any otherwise covered **Claim**:
 - i. directly arising from a **Privacy Breach** by a third party;
 - ii. directly arising from a **Security Failure**; or
 - iii. falling under Insuring Agreement A.4 MEDIA LIABILITY; or
- (b) any otherwise covered Loss falling under Insuring Agreement C.6. FRAUDULENT USE OF INSURED ORGANIZATION'S ELECTRONIC IDENTITY.

B.3 PROPERTY DAMAGE

any theft, damage, destruction, or loss of use of any property. However, this does not apply to:

- (a) loss, damage, or destruction of data;
- (b) any **Privacy Breach** the **Insured** experiences that involves the loss or theft of **Personal Data** or **Corporate Information** that is maintained in tangible form and is readable without the use of any electronic device; or
- (c) otherwise covered **Bricking Costs** under Insuring Agreement B.4 BRICKING COSTS.

B.4 BODILY INJURY

any death, bodily injury, sickness, mental anguish, emotional distress, or disease suffered or alleged to be suffered by anyone.

However, this exclusion shall not apply to:

- (a) solely with respect to Insuring Agreement A.1 INFORMATION PRIVACY LIABILITY, emotional distress, mental anguish, humiliation, or loss of reputation resulting from a **Media Incident**; or
- (b) solely with respect to Insuring Agreement A.1 INFORMATION PRIVACY LIABILITY, emotional distress, mental anguish, or mental injury resulting from a **Privacy Breach**.

B.5 SYSTEM DEGRADATION OR PERFORMANCE

- (a) any degradation, deterioration, or reduction in the performance of the **Insured Organization's Computer System** caused gradually or as a result of the **Insured Organization's** ordinary use of its **Computer System**; or
- (b) loss of, reduction in or loss of use of internet bandwidth, unless caused by an identifiable malicious act that gives rise to a **Claim** or **Loss** otherwise covered under this **Policy**;

including where caused by increased use of the **Insured Organization's Computer System** or by steps taken by the **Insured** to upgrade the system. However, this exclusion does not apply to any covered **Loss** under Insuring Agreements B.7 SYSTEM FAILURE BUSINESS INTERRUPTION or B.8 SYSTEM FAILURE CONTINGENT BUSINESS INTERRUPTION.

B.6 SEIZURE AND CONFISCATION

any confiscation, requisition, expropriation, nationalization, appropriation, seizure, or destruction of property by or under the order of any government or public or local authority, or any order by such authority to take down, deactivate or block access to the **Insured Organization's Computer System**.

B.7 NUCLEAR RISKS

- (a) any sort of nuclear material, nuclear reaction, nuclear radiation, or radioactive contamination;
- (b) any products or services which include, involve, or relate in any way to anything in (a) above, or the storage, handling, or disposal of anything in (a) above; or
- (c) all operations carried out on any site or premises on which anything in (a) or (b) above is located.

B.8 POLLUTION RISKS

any actual, alleged, or threatened discharge, dispersal, release, or escape of a **pollutant**, including any direction or request to test for, monitor, clean up, remove, contain, treat, detoxify, or neutralize a **pollutant**. For the purpose of this exclusion, **pollutant** means any solid, liquid, gaseous, biological, radiological, or thermal irritant or contaminant, including smoke, vapor, asbestos, silica, dust, nanoparticles, fibers, soot, fumes, acids, alkalis, chemicals, germs, and waste, including but not limited to materials to be recycled, reconditioned, or reclaimed.

B.9 INSOLVENCY

the **Insured Organization's** insolvency or the insolvency of the **Insured Organization's** suppliers, sub-contractors, and outsourcers. However, the **Insured Organization's** insolvency will not relieve the **Insurer** of any of the **Insurer's** legal obligations under this **Policy**.

B.10 PRIOR KNOWLEDGE, PRIOR PROCEEDINGS, AND PRIOR NOTICE

- (a) anything likely to lead to a **Claim, Loss**, or other liability under this **Policy**, which any member of the **Control Group** knew or should have reasonably known about before the **Insurer** agreed to insure the **Insured**;
- (b) any demand, suit, or other pending proceeding, or order, decree, or judgment entered against the **Insured** on or prior to the **Pending or Prior Litigation Date**, or the same or substantially the same facts underlying or alleged therein; or
- (c) any circumstance which has been the subject of any written notice given and accepted under any policy of which this **Policy** is a renewal or replacement.

B.11 DISHONEST AND CRIMINAL ACTS

any fraudulent, dishonest, malicious, or criminal conduct intended to cause harm to another person or entity, or any knowing or willful violation of a law, whether committed by the **Insured** or committed by another whose conduct or violation of the law the **Insured** has ratified or actively condoned.

However, this exclusion will not apply to **Claim Expenses** incurred in defending any **Claim** alleging the foregoing until there is a final non-appealable judgment, adjudication, binding arbitration decision, or finding of fact against such **Insured** or an adverse admission under oath or plea of *nolo contendere* or no contest by such **Insured** that establishes such conduct or violation. In the event of such final and non-appealable judgment, adjudication, binding arbitration decision, or finding of fact against such **Insured**, or an adverse admission under oath, or plea of *nolo contendere* or no contest by such **Insured**, the **Insured**, where legally permissible, shall reimburse the **Insurer** for any **Claim Expenses** paid by the **Insurer** and all of the **Insurer's** duties with respect to that **Claim, Loss**, or other liability under this **Policy** shall cease.

For purposes of determining the applicability of this exclusion, the knowledge or conduct of a natural person **Insured** will not be imputed to any other natural person **Insured**, but the knowledge or conduct of any member of the **Control Group** will be imputed to the **Insured Organization**.

B.12 FRAUDULENT USE OF ELECTRONIC IDENTITY

the fraudulent or dishonest use of the electronic identity of the **Insured Organization's Business**. However, this exclusion does not apply to:

- (a) the extent of any covered **Loss** under C. FINANCIAL CRIME AND FRAUD INSURING AGREEMENTS; or
- (b) any **Claim** made under A. THIRD PARTY INSURING AGREEMENTS arising solely as a direct result of an unauthorized access to or unauthorized use of the **Insured's Computer System**.

B.13 UNSOLICITED COMMUNICATIONS

any 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) Canada's Anti-Spam Legislation, or any related or similar provincial or territorial statutes.

B.14 WIRETAPPING

any actual or alleged violation of any other law, regulation, or statute relating to unsolicited communication, distribution, wiretapping, surreptitious recording, failure to obtain consent to record, sending or transmitting of any communication via telephone or any other electronic or telecommunications device including, but not limited to, tracking technologies such as Google Analytics, Google DoubleClick, Meta (f/k/a Facebook), and Pixel.

B.15 NATURAL PERILS

fire, flood, storm, lightning, frost, explosion, or extremes of weather or temperature. However, this exclusion does not apply to any **Claim**, **Loss**, or any other liability arising directly from a **Privacy Breach** that the **Insured** suffers, which is itself caused by such natural peril.

B.16 FINES, PENALTIES, AND SANCTIONS

criminal, civil, or regulatory sanctions, fines, penalties, disgorgement of profits, punitive damages, exemplary damages, treble damages, or multiple damages which the **Insured** is legally obligated to pay, including, but not limited to, those imposed by

any national, federal, provincial, territorial, state, or local governmental body or any licensing organization, provided, however, that this exclusion shall not apply to the extent such damages are insurable under the laws of any applicable jurisdiction most favourable to the **Insured** and which has a substantial relationship to the **Insured**, **Insurer**, this **Policy**, or the **Claim** or **Incident** giving rise to such damages.

However, this exclusion does not apply to **PCI Charges** or **Regulatory Awards**.

B.17 ILL-GOTTEN GAINS

any profit, remuneration, or advantage to which the **Insured** is not legally entitled.

B.18 RECALL AND DISPOSAL

any **Loss**, cost, or expense incurred by the **Insured** or others for the withdrawal, recall, inspection, adjustment, removal, or disposal of any tangible property or intangible property.

B.19 USE OF ILLEGAL OR UNLICENSED PROGRAMS

knowing use of illegal or unlicensed **Programs** or software.

III. DEFINITIONS

When used in this **Policy**, the terms below, whether in the singular or plural, are defined as follows:

1. **Additional Insured:** Any entity that the **Insured Organization** has expressly agreed in writing to add as an **Additional Insured** under this **Policy** prior to the commission or occurrence of any act, error, or omission for which such entity would be provided coverage under this **Policy**, but only to the extent that the **Insured Organization** would have been liable and coverage would have been afforded under the terms and conditions of this **Policy** had such **Claim** been made against the **Insured Organization**. This **Policy** does not provide coverage for any act, error, or omission committed in whole or in part by any **Additional Insured**.
2. **Adverse Publication:** Any report or communication to the public through any media channel including, but not limited to, television, print media, radio, the internet, or electronic mail, of information that was previously unavailable to the public, specifically concerning an actual or alleged **Security Failure**, **Cyber Attack** against the **Insured**, **Privacy Breach**, or **Illegal Threat** that affects any of the **Insured's** customers or **Clients**.
3. **Application:** All applications, including any attachment thereto, and supplemental information, submitted by or on behalf of the **Named Insured** to the **Insurer** in connection with the request for or underwriting of this **Policy**, or any prior insurance policy issued by the **Insurer** of which this **Policy** is a renewal.

4. **Associated Entity:** Any entity that has been identified in the presentation of the risk, or **Application**, for this **Policy**, provided that:
 - a. the entity's revenues have been provided to the **Insurer** in the **Application**;
 - b. the entity has at least the same level of security standards as those of the **Named Insured** shown in the presentation of the risk; and
 - c. the entity is listed on the Scheduled Associated Entity Endorsement attached to this **Policy**.
5. **Bricking Costs:** The costs, different than **Data Recovery Costs**, of rectifying or replacing any part of the **Insured's Computer System** that is rendered nonfunctional or useless for its intended purpose, without being physically damaged, as a direct result of a **Security Failure** or a **Cyber Attack**.
6. **Business:** The commercial and/or professional activities or services undertaken by the **Insured** as stated in the **Application**.
7. **Claim:** Any:
 - a. written demand seeking monetary damages or non-monetary or injunctive relief;
 - b. civil proceeding, investigation, or suit commenced by service of a complaint, notice, request for information, or similar proceeding seeking monetary damages or non-monetary or injunctive relief;
 - c. demand for arbitration, mediation, or other alternative dispute resolution proceeding seeking monetary damages or non-monetary or injunctive relief;
 - d. written request to toll or waive a statute of limitations; or
 - e. institution of a **Regulatory Claim** against an **Insured**, solely with respect to Insuring Agreement A.2. REGULATORY DEFENCE AND AWARDS.

All **Claims** with a common nexus of fact, circumstance, situation, transaction, or cause, or a series of related facts, circumstances, situations, transactions, or causes will be considered to be a single **Claim**.

8. **Claim Expenses:** Any of the following:
 - a. any of the amounts an **Insured** becomes legally obligated to pay including:
 - i. compensatory damages, settlements, and judgments;
 - ii. prejudgment interest, post judgment interests, judgments or settlements;
 - iii. punitive, exemplary, or multiplied damages, but only to the extent such damages are insurable under the laws of any applicable jurisdiction most favourable to the **Insured** and which has a substantial relationship to the **Insured**, **Insurer**, this **Policy**, or the **Claim** or **Incident** giving rise to such damages; or
 - iv. **Money** to be deposited into a consumer compensation fund as a form of equitable relief to pay for consumer **Claim** arising from an adverse judgment or settlement.
 - b. any **Regulatory Award**;
 - c. **PCI Charges**;
 - d. costs covered under Insuring Agreement B.1 INCIDENT RESPONSE;
 - e. **Privacy Investigation Costs**; or
 - f. **Defence Costs**;

provided, however, that the **Insurer** will not pay costs for any part of a **Claim** or **Privacy Investigation** not covered by this **Policy**.

9. **Client:** Any third party with whom the **Insured Organization** has a contract in place for the supply of the **Insured Organization's** services or products in return for a fee, or where a fee would normally be expected to be paid.
10. **Computer System:** A connected system of computing hardware, software, firmware, and associated electronic components and mobile devices, including industrial control systems and SCADA (supervisory control and data acquisition) systems.
11. **Control Group:** The **Insured Organization's** Chief Executive Officer, General Counsel, Chief Financial Officer, Risk Manager, Insurance Manager, Chief Information Officer, Chief Information Security Officer, and Chief Security Officer (or individuals holding functionally equivalent positions, regardless of title).
12. **Corporate Information:** Any confidential or proprietary information of an entity, other than an **Insured Organization**, which:
 - a. an **Insured Organization** is contractually or legally required to hold or maintain in confidence; and
 - b. is not known or accessible by the general public.

Corporate Information does not include **Personal Data**.
13. **Cyber Attack:** Any digital attack designed to disrupt access to or the operation of a **Computer System**, including a denial of service attack or distributed denial of service attack.
14. **Cyber Crime Loss:** Any of the following **Losses**:
 - a. the value or amount of any taken or misappropriated **Money, Securities**, or tangible property or, in the case of a telecommunication fraud, the cost to the **Insured** of the fraudulent calls or Internet service; and
 - b. the reasonable and necessary costs incurred to extricate the **Insured's Business** from any contract or arrangement entered into through such fraudulent or dishonest use of the electronic identity of the **Insured's Business**.
15. **Cyber Terrorism:** Any act or series of acts, or the threat of such act or acts, of any person or group of persons, whether acting alone or on behalf of or in connection with any organization, through the use of **Computer Systems** to destruct, disrupt or subvert any **Computer System**, computer network, infrastructure, the Internet, an intranet, telecommunications and/or its content, with the intention to cause harm or committed for political, religious or ideological purposes, including but not limited to the influencing of any government and/or to put the public or a section of the public in fear.
16. **Data Asset:** Any information represented, transmitted, or stored electronically or digitally, including code, **Programs**, software, and firmware, on the **Insured's Computer System**.

17. **Data Recovery Costs:** The reasonable and necessary costs and expenses incurred to regain access to the **Insured's Data Assets**, or to replace, restore, or repair the **Insured's Data Assets** from back-ups, originals, or other sources.
18. **Data Subject:** Any natural person who is the subject of **Personal Data**.
19. **Defence Costs:** The reasonable and necessary lawyers' and experts' fees and legal costs incurred in investigating, settling, defending, appealing, or defending an appeal against a covered **Claim**.
20. **Employee:** Any individual (including a part time, temporary, leased, or volunteer worker) employed by the **Insured Organization**, but only while acting on behalf of the **Insured Organization** and in the scope of the **Insured Organization's Business**. **Employee** does not include any individual performing work for the **Insured Organization** as an independent contractor.
21. **Illegal Threat:** Any reasonable threat or connected series of threats from a third party to:
- a. introduce **Malicious Code** into the **Insured's Computer System**;
 - b. commence a **Cyber Attack** upon the **Insured's Computer System**;
 - c. disseminate, divulge, or improperly utilize any of the **Insured's Data Assets** taken as a result of the unauthorized use of or the unauthorized access of the **Insured's Computer System** or **Outsourced Service Provider's Computer System**; or
 - d. encrypt or otherwise make unavailable the **Insured's Data Assets**;
- unless a payment is received from the **Insured Organization** or on the **Insured Organization's** behalf in return for the elimination, mitigation, or removal of such threat.
22. **Incident: Adverse Publication, Privacy Breach, Security Failure, Illegal Threat, Cyber Attack, a Social Engineering Attack, or a System Failure.**
- All **Incidents** with a common nexus of fact, circumstance, situation, transaction, or cause, or a series of related facts, circumstances, situations, transactions, or causes will be considered as a single **Incident** and will be deemed to have occurred at the time the first **Incident** occurred.
23. **Income:**
- a. the total net income (net profit or loss before income taxes) of the **Insured Organization's Business**, less any savings resulting from the reduced costs and expenses; and
 - b. the continuing normal operating expenses incurred, including payroll.
24. **Increased Costs of Working:** The reasonable and necessary costs and expenses incurred by the **Insured** for the sole purpose of minimizing the reduction in **Income** during the **Indemnity Period**, but not exceeding the reduction in **Income**.

25. **Indemnity Period:** The period, in days, beginning on the date the interruption to the **Insured's Business** or **Voluntary Shutdown** commences and lasting for the period during which the **Insured's Income** is affected as a result of such interruption or **Voluntary Shutdown**, but for no longer than the number of days shown in the Declarations.
26. **Insured:**
- a. the **Insured Organization**;
 - b. any **Senior Executive** or **Employee**, but only when acting on the **Insured Organization's** behalf;
 - c. any independent contractor when performing work for the **Insured Organization** under the **Insured Organization's** direction and supervision, based on a written contract; or
 - d. an **Additional Insured**, but only with respect to **Claims** made against such **Additional Insured** solely for the acts, errors, or omissions of the **Insured Organization**.
27. **Insured's Computer System:** A **Computer System** leased, owned, or operated by an **Insured** or operated solely for the benefit of an **Insured** by a third party under written contract with an **Insured**. **Insured's Computer System** does not include any **Outsourced Service Provider's Computer System**.
28. **Insured Organization:** The **Named Insured**, any **Associated Entity**, and any **Subsidiary**.
29. **Insured Organization's Computer System:** A **Computer System** leased, owned, or operated by an **Insured Organization** or operated solely for the benefit of an **Insured Organization** by a third party under written contract with an **Insured Organization**. **Insured Organization's Computer System** does not include any **Outsourced Service Provider's Computer System**.
30. **Insurer:** The entities named in the Declarations.
31. **Loss:** Any financial harm caused to the **Insured Organization's Business**.
32. **Malicious Code: Programs** that are secretly introduced without the **Insured Organization's** permission or knowledge including, but not limited to, malware, worms, trojans, rootkits, spyware, dishonest adware, crimeware, and other malicious unwanted software.
33. **Media Incident:** Any actual or alleged:
- a. infringement of copyright, trademark, trade name, trade dress, title, slogan, service mark, or service name;
 - b. defamation, libel, or slander;
 - c. trade libel, product disparagement, or malicious falsehood; or
 - d. plagiarism, piracy, or misappropriation of ideas under an implied contract;
- which directly arises from the **Insured Organization's Business** in the course of gathering, communicating, reproducing, publishing, disseminating, displaying, releasing, transmitting, or disclosing **Insured Organization's** information.

34. **Money:** Cash, coin, bank and currency notes, bullion, funds, cheques, registered cheques, travelers' cheques, postal orders, bank drafts, or money orders. **Money** does not include any electronic, digital, online, virtual currency, or any cryptocurrency; provided, however, that solely with respect to Insuring Agreement B.2 CYBER EXTORTION LOSSES, **Money** includes: (a) electronic, digital, online, virtual currency, or any cryptocurrency; and (b) transaction fees paid by the **Insured Organization** in obtaining cryptocurrency.
35. **Named Insured:** The legal entity stated in Item 1. of the Declarations.
36. **Outsourced Service Provider:** An entity not owned, operated or control by the **Insured Organization**, but that the **Insured Organization** hires for a fee pursuant to a written contract to perform services related to the conduct of the **Insured Organization's Business**, including, but not limited to:
- a. maintaining, managing, or controlling the **Insured Organization's Computer System**;
 - b. hosting or facilitating the **Insured Organization's** Internet website, or
 - c. providing administrative functions, human relations, marketing, or other outsourced services to the **Insured Organization**.
37. **PCI Charges:** Any charges, fines, penalties, levies, costs, recertification costs, expenses, assessments, contractual damages, or imposition of liabilities of any nature arising as a direct result of the **Insured's** failure to comply with **PCI DSS** due to a **Privacy Breach**, including any sums in relation to card reissuance or fraudulent transactions.
38. **PCI DSS:** Payment Card Industry Data Security Standard or any equivalent or successor standard or regime.
39. **Pending or Prior Litigation Date:** The date stated as the pending and prior litigation date in the Declarations.
40. **Personal Data:** Any private, non-public information of any kind from which a person or group of people may be uniquely and reliably identified or contacted, including, but not limited to, an individual's name, telephone number, email address, social insurance number, social security number, medical or healthcare data or other protected health information, provincial identification number, or driver's license number. **Personal Data** shall also include all personal information as defined in any local, state, provincial, territorial, or federal identity theft or privacy protection laws. **Personal Data** does not include **Corporate Information**.
41. **Policy:** This insurance document and the Declarations, including any endorsements and the **Application**.
42. **Policy Period:** The time for which this **Policy** is in force as shown in the Declarations.
43. **Privacy Breach:** The unauthorized acquisition, access, use, or disclosure of, or the loss or theft of, **Personal Data** or **Corporate Information**.

44. **Privacy Investigation:** Any written request for information, official examination, formal inquiry, or formal investigation brought by or on behalf of a governmental or regulatory authority and based on the same circumstances as any **Privacy Breach** or **Claim** covered under Insuring Agreement A.1 INFORMATION PRIVACY LIABILITY (a), (b), or (d).
45. **Privacy Investigation Costs:** The reasonable and necessary legal costs incurred in investigating, settling, defending, or appealing a **Privacy Investigation** or other investigation in connection with any local, state, provincial, territorial, or federal identity theft or privacy protection laws.
46. **Privacy Policy:** the **Insured Organization's** public declaration of its policy for use, disclosure, collection, dissemination, sharing, and correction or supplementation of, and access to, **Personal Data**.
47. **Program:** A set of instructions written in a computer language that tells a computer how to process data or interact with ancillary equipment.
48. **Public Relations Costs:** The reasonable costs incurred:
- a. for a public relations or crisis management consultant to assist the **Insured Organization** in re-establishing the **Insured Organization's** reputation and responding to media reports, including the development and communication of a strategy to repair **Insured's Organization's** reputation;
 - b. to issue statements via email or the **Insured's** website and social media accounts, including managing and monitoring the **Insured's** social media sites; and
 - c. for any other reasonable and proportionate measures taken to protect or re-establish the **Insured Organization's** reputation.
- The **Insurer** shall only reimburse the **Insured Organization** for such costs: (i) where the **Insurer** has provided prior written consent, such consent not to be unreasonably withheld; and (ii) where costs incurred by the **Insured Organization** for services performed by itself are over and above **Insured Organization's** normal operating expenses.
49. **Regulatory Award:** Following a **Privacy Investigation**, any civil or regulatory sanctions, fines, penalties, disgorgement of profits, treble damages, or multiple damages, including but not limited to those imposed by any national, federal, state or local governmental body or any licensing organization, if insurable in the jurisdiction where such award was first ordered, but not including **PCI Charges**.
50. **Regulatory Claim:** Any **Claim** brought by, or on behalf of, a federal, state, provincial, territorial, or foreign governmental entity in such entity's regulatory or official capacity due to a **Privacy Breach**, including violations of regulations including, but not limited to, the Personal Information Protection and Electronic Documents Act (PIPEDA), Gramm-Leach Bliley Act of 1999, Health Insurance Portability and Accountability Act of 1996 (HIPAA), General Data Protection Regulation, and the California Consumer Privacy Act.

51. Reputational Loss:

- a. the termination of the **Insured Organization's Business** written contract(s) with one or more of the **Insured Organization's Clients**; or
- b. the reduction in the **Insured's Organization's** book value.

52. Retention: The amount the **Insured** must bear as the first part of each covered **Claim** or **Loss** as stated in the Declarations with respect to the Insuring Agreement to which each such stated **Retention** applies.**53. Securities:** Negotiable and non-negotiable financial instruments or contracts, in physical or electronic form, which represent **Money** or tangible property.**54. Security Failure:** Any failure by the **Insured Organization** or by others on the **Insured's** behalf (including but not limited to the **Insured's** subcontractors and outsourcers) in securing the **Insured's Computer System** against unauthorized electronic access or use.**55. Senior Executive:** Any person who was, is, or during the **Policy Period** becomes the **Insured Organization's** director, officer, trustee, in-house counsel, chief information security officer, risk manager, or chief privacy officer in actual control of the **Insured Organization's** operations.**56. Social Engineering Attack:** Any request directed to the **Insured Organization**, or someone acting on the **Insured Organization's** behalf, by a person improperly seeking to obtain possession, or the transfer to a third party, of **Money, Securities**, or tangible property that such person or third party is not entitled to, where such person improperly:

- a. impersonates or claims to be another person who would be lawfully entitled to possession of or access to, or to authorize transactions with respect to, such **Money, Securities**, or tangible property had they made such a request; or
- b. assumes the identity of another person who the **Insured** or someone acting on the **Insured's** behalf reasonably believes exists and would be lawfully entitled to possession of or access to such **Money, Securities**, or tangible property had they existed and made such request.

57. Subsidiary:

- a. Any entity in which the **Insured Organization** owns more than 50% of the book value of the assets or of the outstanding voting rights on the first day of the **Policy Period**; or
- b. Any entity that the **Insured Organization** creates or acquires during the **Policy Period**:
 - 1. where its consolidated revenues at the date of creation or acquisition are less than 20% of the **Insured Organization's** existing consolidated revenues;
 - 2. where the acquired entity's business activities are similar to **the Insured Organization's**; and
 - 3. which has not suffered any **Loss** or has been subject to any **Claim** with a value greater than the **Retention** that would have been covered under this **Policy**.

If the **Insured Organization's** new **Subsidiary** does not qualify for automatic coverage as provided above, the **Insurer** will insure it for 30 days after the acquisition or its creation while

the **Insurer** underwrites the new **Subsidiary**. The **Insurer** will only provide coverage beyond the 30-day period by the **Insurer's** written agreement.

58. **System Failure:** Any unintentional, unplanned, or unexpected measurable **Computer System** disruption or failure where the proximate cause is not: a **Security Failure**; **Privacy Breach**; loss of or damage to any physical equipment or property; or planned or scheduled outage or maintenance of a **Computer System**.
59. **Terrorism:** An act, or the threat of an act, by any person or group of persons, whether acting alone or on behalf of or in connection with any organization or government, that:
- a. is committed for political, religious, ideological, or similar purposes; and
 - b. is intended to influence any government or to put the public, or any section of the public, in fear; and
 1. involves violence against one or more persons; or
 2. involves damage to property; or
 3. endangers life other than that of the person committing the action; or
 4. creates a risk to health or safety of the public or a section of the public.

Terrorism does not include any of the elements described under **cyber terrorism**.

60. **Voluntary Shutdown:** The **Insured Organization's** intentional shutdown of all or part of the **Insured Organization's Computer System** to attempt to prevent or mitigate any interruption or degradation of the **Insured Organization's Computer System** resulting from an **Incident**.
61. **Waiting Period:** The period of time set forth in the Declarations for the corresponding coverage.

IV. GENERAL TERMS AND CONDITIONS

1. LIMITS AND RETENTION

1.1 AGGREGATE LIMIT AND SUBLIMITS

The Aggregate Limit of Liability shown in item 3 of the Declarations is the most the **Insurer** will pay under this **Policy** regardless of the number of Insuring Agreements purchased, or otherwise stated.

The amount the **Insurer** pays for a particular type of **Claim**, **Incident**, or **Loss** may be further limited in the Declarations.

1.2 PAYING OUT THE LIMIT OF INDEMNITY

At any stage of a **Claim**, **Loss**, or other liability under this **Policy**, the **Insurer** can pay the **Insured** the applicable limit of indemnity or what remains after any earlier payment from that limit. The **Insurer** will pay covered costs and expenses already

incurred at the date of the **Insurer's** payment. The **Insurer** will then have no further liability for that **Claim**, **Loss**, or liability, including any costs or expenses.

1.3 RETENTION AND WAITING PERIOD

The **Insured Organization** must:

- (a) pay the applicable **Retention** shown in the Declarations; and
- (b) bear any **Loss** or expense suffered during the **Waiting Period** with respect to each covered:
 - i. partial or total interruption to the **Insured's Business** or **Voluntary Shutdown**; or
 - ii. **Loss** under Insuring Agreements B.5 BUSINESS INTERRUPTION, B.6 CONTINGENT BUSINESS INTERRUPTION, B.7 SYSTEM FAILURE BUSINESS INTERRUPTION, B.8 SYSTEM FAILURE CONTINGENT BUSINESS INTERRUPTION, or B.9 REPUTATION PROTECTION.

The **Retention** shown in the Declarations is not required with respect to:

- (a) any **Loss** under Insuring Agreements B.5 BUSINESS INTERRUPTION, B.6 CONTINGENT BUSINESS INTERRUPTION, B.7 SYSTEM FAILURE BUSINESS INTERRUPTION, B.8 SYSTEM FAILURE CONTINGENT BUSINESS INTERRUPTION, or B.9 REPUTATION PROTECTION where the **Insured** has borne a **Waiting Period**; or
- (b) Insuring Agreement D.2 COURT ATTENDANCE COMPENSATION.

Any **Loss** or expense the **Insured Organization** incurs during the **Waiting Period** shall not be applied to satisfy any applicable **Retention** shown in the Declarations.

If more than one Insuring Agreement applies, only the single highest **Retention** will apply to any **Loss** or expense.

1.4 RETENTION WAIVER

If the **Insured** notifies the **Insurer** within 24 hours of the **Insured's** first awareness of any actual or reasonably suspected **Incident**, the **Insurer** will waive a portion of the **Retention**, as shown in the Declarations, for any **Losses** suffered. The **Insurer** will only waive such portion of the **Retention** up to a total of the amount shown in the Declarations for all **Claims** and **Losses** combined. This limited waiver does not apply to any **Waiting Period** or to any Insuring Agreement within C. FINANCIAL CRIME AND FRAUD INSURING AGREEMENTS.

2. INSURED'S OBLIGATIONS

2.1 NOTICE TO INSURER & ADMISSIONS

If a **Claim** or **Incident** arises, the **Insurer** will not make any payment under this **Policy** unless the **Insured**:

- (a) notifies the **Insurer** as soon as practicable after a member of the **Control Group** first discovers an **Incident** or becomes aware of a **Claim**, and in no event later than 90 days after the **Policy Period** or during the Extended Reporting Period (if applicable); and
- (b) provides the **Insurer**, at the **Insured Organization's** expense, any information which the **Insurer** may reasonably require and further cooperates fully in the investigation of any **Claim** under this **Policy**.

The **Insured** shall not admit or assume any liability or obligation, nor make any offer, deal, or payment, unless the **Insured** has the **Insurer's** prior written consent, such consent not to be unreasonably withheld.

2.2 NOTICE OF CIRCUMSTANCE

If, during the **Policy Period**, a member of the **Control Group** first becomes aware of any fact, matter, or circumstance that may reasonably be expected to be the basis of a **Claim** against an **Insured** under this **Policy**, then any **Claim** that arises out of such circumstances shall be deemed to have been first made at the time such written notice was received by the **Insurer**, but only to the extent that such written notice includes the following details and is received by the **Insurer** during the **Policy Period**:

- (a) details on why the **Insured** believes a **Claim** may be forthcoming;
- (b) all pertinent facts, particulars, and dates, including the nature of such circumstances and the potential consequences and **Loss**; and
- (c) the identities of those persons allegedly involved or affected.

The **Insured** must not incur any costs or expenses in relation to any such circumstance without the **Insurer's** prior written consent, such consent not to be unreasonably withheld.

2.3 CLAIM PROCESS

- (a) The **Insurer** has the right, but not the obligation, to take control of and conduct in the **Insured's** name, the investigation, settlement, or defence of any **Claim**, **Privacy Investigation**, or **Loss**. If the **Insurer** thinks it necessary, the **Insurer** will appoint an adjuster, attorney, or any other appropriate person to handle the **Claim**, **Privacy Investigation**, investigation, or **Loss**.
- (b) If the **Insurer** recommends a settlement of any **Claim** acceptable to the claimant and the **Insured** refuses to consent to such settlement, then the **Insurer's** liability for such **Claim** shall not exceed:
 - i. the amount for which such **Claim** could have been settled by the **Insurer** plus **Defence Costs** up to the date the **Insured** refused to settle such **Claim**; and
 - ii. 70% of any **Loss** and **Defence Costs combined**, in excess of Subparagraph 2.3(b)i. above, incurred in such **Claim**.

The remaining **Loss** and **Defence Costs** shall be borne by, or on behalf of, the **Insured** at its own risk.

- (c) The **Insurer** will not pay any costs or expenses for any part of any **Claim, Loss**, or any other liability not covered by this **Policy**.
- (d) The **Insured** has the right to select defence counsel and incident response vendors from the **Insurer's** vendor panel list, which can be found at <http://www.bboxinsurance.com/vendor-panel/>.
- (e) If a dispute arises between the **Insured** and the **Insurer** in connection with this **Policy** that cannot be resolved through informal negotiation, the parties will attempt to resolve the dispute through mediation before a mutually agreeable mediator. The mediator's expenses and fees will be split equally between the **Insured** and the **Insurer**. If the **Insurer's** dispute has not been resolved upon conclusion of the mediation process, then either party may file suit in any court having jurisdiction over the parties and the subject matter of the dispute or disagreement.

2.4 LOSS MINIMIZATION

The **Insured Organization** must make every reasonable effort to minimize any **Loss** or liability and take appropriate emergency measures immediately if they are required to reduce or mitigate the severity of any **Claim** or **Incident**. The **Insured** must give the **Insurer** all assistance which the **Insurer** may reasonably require to pursue recovery of amounts the **Insurer** may become legally liable to pay under this **Policy** in the **Insured Organization's** name, but at the **Insurer's** expense.

2.5 POTENTIAL LOSSES AND CLAIMS

- (a) The **Insured** may notify the **Insurer** of facts, matters, or circumstances which the **Insured** first become aware of within the **Policy Period**, or Extended Reporting Period if applicable, and which the **Insured** believes are reasonably likely to give rise to a **Privacy Breach, Security Failure, Illegal Threat, Cyber Attack, System Failure, Claim, Privacy Investigation, Loss**, business interruption, contingent business interruption, **Voluntary Shutdown**, or any other liability under this **Policy**.
- (b) If the **Insurer** accepts the **Insured's** notification, the **Insurer** will regard any subsequent **Privacy Breach, Security Failure, Illegal Threat, Cyber Attack, System Failure, Claim, Privacy Investigation, Loss**, business interruption, contingent business interruption, or any other liability as notified to this **Policy**.

2.6 PROOF OF LOSS

- (a) With respect to requests for payment or reimbursement of **Losses, Claim Expenses** or any other costs or expenses covered incurred by the **Insured Organization** will be accompanied by a proof of such **Losses**, costs or expenses. Such proof of **Loss** must include, in detail, how the costs were calculated, what assumptions have been made and will include any applicable reports, books of accounts, bills, invoices and other vouchers or proofs of payment made by the **Insured** in relation to such **Losses** or **Claim Expenses**. Furthermore, the **Insured Organization** will cooperate with, and provide any additional information reasonably requested by, the **Insurer**.
- (b) Solely with respect to verification of Insuring Agreements B.5 BUSINESS INTERRUPTION, B.6 CONTINGENT BUSINESS INTERRUPTION, B.7 SYSTEM

FAILURE BUSINESS INTERRUPTION, B.8 SYSTEM FAILURE CONTINGENT BUSINESS INTERRUPTION, or B.9 REPUTATION PROTECTION (b), the **Insured Organization** agrees to allow the **Insurer** to examine and audit the **Insured Organization's** books and records that relate to this **Policy** at any time during the **Policy Period** and up to 12 months following the **Insurer's** receipt of any proof of **Loss** in accordance with this section.

- (c) Any requests for payment or reimbursement of **Losses** or **Claim Expenses** shall not include or be calculated based on any of the **Insured Organization's** overhead expenses, the **Insured's** liability for debt, taxes, lost costs or profits, salaries or wages ordinarily incurred in the performance of the **Insured Organization's Business**, or any future cost of doing business, including but not limited to the cost of any future license or royalty, or costs of improving the **Insured Organization's** security or performing audits.
- (d) Following a covered interruption or **Voluntary Shutdown**, or a covered **Loss** under Insuring Agreements B.5 BUSINESS INTERRUPTION, B.6 CONTINGENT BUSINESS INTERRUPTION, B.7 SYSTEM FAILURE BUSINESS INTERRUPTION, B.8 SYSTEM FAILURE CONTINGENT BUSINESS INTERRUPTION, or B.9 REPUTATION PROTECTION (b), the **Insurer** will determine the **Losses** taking full account and due consideration of an **Insured's** proof of loss, and by considering the difference between the **Insured Organization's** actual **Income** during the **Indemnity Period** and the **Income** it is estimated the **Insured** would have earned during that period or, if this is the **Insured Organization's** first year of business, the difference between the **Insured's Income** during the **Indemnity Period** and during the period immediately prior to the interruption, **Voluntary Shutdown** or **Loss**, less any savings resulting from the reduced costs and expenses the **Insured** paid out of the **Insured's Income** during the **Indemnity Period**. The **Insurer** will also pay for **Increased Costs of Working**.

2.7 REPRESENTATIONS

The **Named Insured** warrants that the content of the materials provided to the **Insurer** are true, accurate, and complete and are material to the **Insurer's** reliance upon same and acceptance of the risk to which the **Policy** applies. Any material misrepresentation, concealment, or misstatement by the **Named Insured** (or on the **Named Insured's** behalf), whether in the **Application** or in any supplemental materials submitted to the **Insurer**, will render the **Policy** null and void with respect to any natural person **Insured** who knew of such material misrepresentation, concealment, or misstatement, and with respect to the **Insured Organization** if any member of the **Control Group** knew of such material misrepresentation, concealment, or misstatement, and will relieve the **Insurer** from all obligations and liability under the **Policy** with respect to those **Insureds**.

2.8 CANCELLATION AND EXTENDED REPORTING PERIOD**(a) Automatic Extended Reporting Period**

If this **Policy** does not renew or is otherwise terminated (other than for non-payment of premium), then the **Named Insured** will have an Automatic Extended Reporting Period for a period of sixty (60 days) following such event in which to provide the **Insurer** with written notice of any **Claims** first made against any **Insured** during such sixty (60) day period, but only with respect to any act, error or omission committed prior to such **Policy** termination or the end of the **Policy Period**, whichever is applicable.

(b) Optional Extended Reporting Period

- i. If this **Policy** does not renew or is otherwise terminated (other than for non-payment of premium), then the **Named Insured** has the right to purchase an Optional Extended Reporting Period within sixty (60 days) after such **Policy** termination or the end of the **Policy Period**, whichever is applicable.
- ii. Such Optional Extended Reporting Period applies only to a **Claim** first made against any **Insured** during the Optional Extended Reporting Period, but only with respect to any act, error or omission committed prior to such **Policy** termination or the end of the **Policy Period**, whichever is applicable.
- iii. The **Named Insured** will have the right to purchase an Optional Extended Reporting Period, subject to all terms, conditions, and limitations of this **Policy**, for a period of:
 1. one (1) year for an additional premium of 100% of the total annual premium;
 2. two (2) years for an additional premium of 150% of the total annual premium; or
 3. three (3) years for an additional premium of 200% of the total annual premium.
- iv. This Optional Extended Reporting Period is only available if the **Insurer** receives within 60 days following any **Policy** termination or the end of the **Policy Period**, whichever is applicable:
 1. written notice from the **Named Insured** of the election to purchase the Optional Extended Reporting Period; and
 2. payment of premium for the applicable Optional Extended Reporting Period.
- v. The Optional Extended Reporting Period shall be non-cancellable and the entire additional premium is considered fully earned at the beginning of the Optional Extended Reporting Period.

- vi. The election of this Optional Extended Reporting Period shall not increase the aggregate limit of indemnity provided by this **Policy** or any sub-limits.

(c) Cancellation and Non-Renewal

- i. The **Named Insured** may cancel or elect not to renew this **Policy** by giving a written notice at the address shown in the Declarations.
- ii. The **Insurer** will refund to the **Named Insured** the unearned pro-rata proportion of the premium for the remaining portion of the **Policy Period** after the effective date of cancellation for which the **Insured** has already paid.
- iii. The **Insurer** will not cancel this **Policy** except for failure to pay premium when due, in which event, the **Insurer** will provide the **Insured** with written notice of cancellation at the address stated in the Declarations. The **Insurer's** notice will be mailed to the **Insured** at least 20 days prior to the effective cancellation date with a copy sent to the **Insured's** agent of record.

2.9 CHANGE OF OWNERSHIP

If during this **Policy**, the **Insured Organization** is purchased, acquired, or merged into another entity such that the **Insured Organization** no longer holds or controls the voting rights of the **Insured Organization**, the **Policy** will continue in full force and effect until the expiration date of the current **Policy Period** with respect to **Claims** made or **Incidents** discovered before such acquisition or merger.

3. OTHER PROVISIONS

3.1 MULTIPLE INSURED

- (a) The most the **Insurer** will pay is the relevant amount shown in the Declarations.
- (b) If more than one **Insured** is named in the Declarations, the total amount the **Insurer** will pay will not exceed the amount the **Insurer** would be liable to pay to any one of the **Insured**.
- (c) The **Insured** agrees that the **Named Insured**, or if there is more than one **Insured** named in the Declarations the first of them, is authorized to receive all notices and agrees any amendments to the **Policy**.

3.2 CHOICE OF LAW

It is understood and agreed that in the event of a dispute concerning the payment of any amount claimed by the **Insured** to be due hereunder, the **Insurer**, at **Insured's** request, will submit to the jurisdiction of a court of competent jurisdiction within Canada. The foregoing shall not constitute a waiver of the right by the **Insurer** to remove, remand, or transfer such suit to any other court of competent jurisdiction in accordance with the applicable statutes of the province of Canada pertinent hereto.

3.3 NO CHANGES OR ASSIGNMENT

No change in, modification of, or assignment of interest under this **Policy** shall be effective except when made by endorsement signed by the **Insurer**.

3.4 SUBROGATION

If any payment is made under this **Policy** and there is the ability to recover against any third party, it is agreed that the **Insured** tenders all rights of recovery to the **Insurer**. The **Insured** further agrees to assist the **Insurer** in exercising the **Insurer's** subrogation rights, including executing all required documents and doing everything reasonably necessary, to secure and preserve such rights and to enable the **Insurer** effectively to bring an action or suit in the name of the **Insured**. Any recovery from the **Insurer's** subrogation efforts will first be paid to the **Insurer** for any incurred subrogation expenses, then to the payment the **Insurer** made that gave rise to the **Insurer's** subrogation rights, then to reimburse the **Insured** for the **Retention** paid, with any remainder to the **Insured**. This obligation does not apply to the extent that the right to subrogate is waived by the **Insured Organization** under a written contract with a third party prior to any **Incident** discovered giving rise to any coverage provided.

3.5 SEVERABILITY OF INSUREDS

The **Insurer** will not impute any conduct or knowledge of any of those included in the definition of the **Insured** to any individual **Insured** under this **Policy**. However, the **Insurer** will impute the conduct or knowledge of any member of the **Control Group** to the **Insured Organization**.

3.6 OTHER INSURANCE

Any payment due under this **Policy** with respect to B. FIRST PARTY INSURING AGREEMENTS shall be applied as primary insurance. Any other payment due under this **Policy** shall be specifically excess of, and will not contribute to or with, any other valid and collectible insurance available to the **Insured**, unless such other insurance is written as excess insurance over the limit of liability of this **Policy**.

3.7 ALLOCATION OF COSTS

If a **Claim** is only partially covered by the **Insurer**, either because of uncovered matters or because it includes uncovered parties, the **Insurer** will use the **Insurer's** best efforts to agree to a fair and proper allocation based upon the relative legal exposure to such covered and uncovered parties and/or matters. The allocation will ultimately be the **Insurer's** decision.

3.8 SANCTIONS

The **Insurer** will not be liable to pay any **Claim** or provide any benefit under this **Policy** that would expose the **Insurer** to any sanction, prohibition, or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom, Switzerland, Canada, or the United States of America.

In the event of the above, the **Insurer** will treat this **Policy** as if it had never existed.

3.9 TERRITORY

The coverage provided under this **Policy** applies worldwide.

3.10 ENTIRE AGREEMENT

The **Insured** agrees that this **Policy** constitutes the entire agreement between the **Insured** and the **Insurer** relating to this insurance.

Endorsement: WAR, CYBER WAR & CYBER OPERATION ENDORSEMENT**Policy No:****Insured:****Effective:** dd-mmm-yyyy

Notwithstanding any other provision in the **Policy**, it is hereby agreed to by the **Insured** and the **Insurer** that the **Policy** is hereby amended, as follows:

The following is added to **II. EXCLUSIONS**

War and cyber operation Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind (together "loss" for the purpose of this exclusion only) directly or indirectly occasioned by, happening through or in consequence of:

- (a) **War** or a **Cyber Operation** that is carried out in the course of **War**; and/or
- (b) retaliatory **Cyber Operations** between any **Specified States** leading to two or more **Specified States** becoming **Impacted states**; and/or
- (c) a **Cyber Operation** that has a major detrimental impact on:
 - i. the functioning of a **state** due to the direct or indirect effect of the **Cyber Operation** on the availability, integrity or delivery of an **Essential Service** in that **State**; and/or
 - ii. the security or defence of a **State**.

Paragraph c) shall not apply to the direct or indirect effect of a **Cyber Operation** on a **Bystanding Cyber Asset**.

The **Insurer** shall have the burden of proving that this exclusion applies.

Attribution of a **Cyber Operation** to a **State**

- a) The primary but not exclusive factor in determining attribution of a **Cyber Operation** shall be whether the government of the **state** (including its intelligence and security services) in which the **Computer System** affected by the **Cyber Operation** is physically located attributes the **Cyber Operation** to another **state** or those acting on its behalf.
- b) Pending attribution by the government of the **state** (including its intelligence and security services) in which the **Computer System** affected by the **Cyber Operation** is physically located,

the **Insurer** may rely upon an inference which is objectively reasonable as to attribution of the **Cyber Operation** to another **State** or those acting on its behalf. It is agreed that during this period no loss shall be paid.

- c) In the event that the government of the **State** (including its intelligence and security services) in which the **Computer System** affected by the **Cyber Operation** is physically located either:
- i. takes an unreasonable length of time to, or
 - ii. does not, or
 - iii. declares it is unable to

attribute the **Cyber Operation** to another **State** or those acting on its behalf, it shall be for the **Insurer** to prove attribution by reference to such other evidence as is available.

Definitions applicable only to this exclusion:

1. **Bystanding Cyber Asset** means a **Computer System** used by the insured or its third party service providers that is not physically located in an **Impacted State** but is affected by a **Cyber Operation**.
2. **Computer System** means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.
3. **Cyber Operation** means the use of a **Computer System** by or on behalf of a **State** to disrupt, deny, degrade, manipulate or destroy information in a **Computer System** of or in another **State**.
4. **Essential Service**, for the purposes of this exclusion, means a service that is essential for the maintenance of vital functions of a **State** including without limitation: financial institutions and associated financial market infrastructure, health services or utility services.
5. **Impacted State** means any **State** where a **Cyber Operation** has had a major detrimental impact on:
 - i. the functioning of that **State** due to the direct or indirect effect of the **Cyber Operation** on the availability, integrity or delivery of an **Essential Service** in that **State**; and/or
 - ii. the security or defence of that **State**.

6. **Specified States** means China, France, Germany, Japan, Russia, UK or USA.
7. **State** means sovereign state.
8. **War** means:
- i. the use of physical force by a **State** against another **State** or as part of a civil war, rebellion, revolution, insurrection, and/or
 - ii. military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority,

whether war be declared or not.

This endorsement should be read in conjunction with the Definitions listed above as items in bold are defined within the **Policy**.

All other terms and conditions of this **Policy** remain unchanged.

This endorsement forms a part of the **Policy** to which attached, effective on the inception date of the **Policy** unless otherwise stated herein.

Signed for and on behalf of Lloyd's:



Philip Baker

Dated: dd-mmm-yyyy