

Bewica Cyber Policy Wording

Provided that **You** have paid **Your Premium**, subject to the terms and conditions set out in this **Policy**, **We** will indemnify **You** in accordance with the **Operative Clauses** for **Triggering Events** that occur during the **Policy Period** and/or **Retroactive Period**.

This **Policy** is an insurance contract between **You** and **Us**. It comprises the **Policy Wording**, the **Schedule** and any **Endorsements** and these three documents should be read together. This **Policy** is a legal document and should be read carefully. Please raise any questions with the broker who sold this **Policy** to **You**.

Terms shown in **bold** font and with capital letters have a specific meaning in this Policy. Those meanings will be detailed in the **Policy Definitions** in Section 6 of this Policy Wording.

Contents

1. WHAT IS COVERED	2
2. WHAT IS NOT COVERED	3
3. HOW MUCH WE WILL PAY YOU	7
4. YOUR OBLIGATIONS	9
5. GENERAL CONDITIONS AND INFORMATION	10
6. POLICY DEFINITIONS	12

1.1 LOSSES SUFFERED BY YOU

We will indemnify You for:

- a) **Breach Expenses** arising from **Data Breach** or **Security Breach**;
- b) **Data Recovery Expenses** arising from a **Data Breach**, **Security Breach** or **Computer System Attack**;
- c) **Special Expenses** arising from a **Data Breach**, **Security Breach** or **Computer System Attack**;
- d) **Extortion Monies** arising from a **Cyber Extortion Threat**;
- e) **Cyber Theft** arising from a **Phishing Attack** or **Social Engineering Event**;
- f) **Business Interruption** arising from **Computer System Disruption**;
- g) **Regulatory Fines, Penalties and Costs** arising from a **Data Breach** or **Security Breach**; and
- h) **PCI Fines, Penalties and Assessments**, arising from a **PCI Breach**.

Any **Loss** must arise from the applicable **Triggering Event** occurring or being alleged to have occurred during the **Retroactive Period** or the **Policy Period** providing that **You** first become aware of the **Triggering Event** during the **Policy Period** or **Extended Reporting Period**.

1.2 CLAIMS AGAINST YOU

- a) **Network Security Liability**: We will pay **Damages** arising from a **Claim** relating to a **Security Breach**.
- b) **Privacy Liability**: We will pay **Damages** arising from a **Claim** relating to a **Data Breach**.
- c) **Media Liability**: We will pay **Damages** arising from a **Claim** relating to a **Media Event**.

Any **Damages** covered under this **Policy** must relate to a **Claim** first made against **You** during the **Policy Period** and notified to **Us** during the **Policy Period** or **Extended Reporting Period**.

1.3 TRIGGERING EVENTS

A **Triggering Event** shall be any one of the following:

- a) **Computer System Attack**, being any unauthorised electronic or computer attack designed to destroy, modify or impair the functionality of Your **Computer Systems**.
- b) **Computer System Disruption** being the actual measurable interruption, suspension or failure of a **Computer System** resulting directly from a **Computer System Attack** or **Computer System Breach**;
- c) **Cyber Extortion Threat** being a demand for **Extortion Monies** arising from a **Credible Threat**;
- d) **Data Breach**, being the loss, theft, destruction, corruption, encryption or unauthorised disclosure of or access to **Personal Data** transmitted by, stored or otherwise processed by **You**.
- e) **Security Breach**, being unauthorised access to or use of **Your Computer Systems** (and any confidential data contained on these systems or networks) or failure to protect against a **Computer System** being attacked or where **Your Computer System** transmits malicious code or malware to a third party.
- f) **Media Event**, being an **Infringement of Intellectual Property Rights** or **Defamation**.
- g) **PCI Breach**, being a breach of **PCI Data Security Standards**.
- h) **Phishing Attack** being an attempt by a third party to impersonate **Your** customers or suppliers using a website or electronic communication to obtain usernames, passwords, credit card details or any **Personal Information**.
- i) **Social Engineering Event** being a misrepresentation of fact or an intentional, malicious, wilful or fraudulent act undertaken by a third party directed at **You** or **Your Employees** using a website or electronic communication.

2.1 ACTS OR OMISSIONS OUTSIDE OF COVER

Any **Triggering Event** which:

- a) should have been notified (including any known or unknown matters) under any previous insurance **Policy** that **You** had covering cyber losses;
- b) occurs or is alleged to have occurred prior to the **Retroactive Date** and **Policy Period**; or
- c) **You** first become aware of prior to the **Policy Period**; or
- d) occurs or is alleged to have occurred after the **Policy Period**.

2.2 ASSOCIATED COMPANY

Claims arising from an entity:

- a) in which **You** own an interest exceeding 15% (fifteen per cent);
- b) in which **You** are a director or a partner, or an entity which operates, manages or controls **You**; or c) as an ownership interest exceeding 15% (fifteen per cent) in **You**.

This exclusion does not apply to **Your** data protection obligations to **Your Employees** under applicable laws within the United Kingdom or under European Union Directives or other international data protection laws.

2.3 BETTERMENT

Expenses relating to or arising from restoring, upgrading or replacing any **Digital Assets** and/or upgrading, designing, reconfiguring or maintaining any **Computer System** or software program to a level beyond that which existed prior to the event listed in Section 1.

This **Policy** only provides cover for restoration and does not cover a replacement of any hardware.

2.4 BODILY INJURY AND PROPERTY DAMAGE

Costs relating to or arising or alleged to be related to or arising from **Bodily Injury** or **Property Damage**. However, this exclusion shall not apply to emotional distress or mental anguish caused by a **Data Breach** or **Security Breach**.

2.5 CONTRACTUAL LIABILITY

Claims relating to or arising or alleged to be related to or arising from any contractual liability, guarantee or obligation, including without limitation, any liability or obligation assumed under contract or by way of guarantee, or alleging or arising out of or resulting from any breach of contract or agreement, in either oral or written form; provided, however, this exclusion shall not apply if **You** would be legally liable in the absence of such contract or agreement and to the extent this relates to **Your** contractual indemnification of a customer or client for a **Security Breach**, **Data Breach** or breach of **Privacy Regulations**.

2.6 PATENT AND TRADE SECRET

Losses related to or arising or alleged to be related to or arising from breach of patent or trade secret. This exclusion includes the infringement, misappropriation or disclosure of any patent or trade secret.

2.7 EXPENSE(S) INCURRED AFTER A FINAL JUDGEMENT

Expenses incurred after there is a final judgment or arbitrator's decision finding that **You** were not entitled to coverage under any **Operative Clause** outlined in Section 1, or in any situation where **You** admit that **You** were not entitled to coverage. In such circumstances, **You** shall reimburse to **Us** any **Defence Costs** paid to **You** or on **Your** behalf by **Us**.

2.8 DIRECTORS' AND OFFICERS' LIABILITY

Claims relating to or arising or alleged to be related to or arising from any actual or alleged violation of the Financial Services and Markets Act 2000 (UK) or the Financial Services Act 2012 (UK) or Companies Act 2006 (UK) (including any subsequent amendments or any rules or regulations promulgated thereunder), or any other similar law (including common law), regulation, or statute whether enacted within the UK or as part of the broader requirement or obligation under European Union Securities regulation or such legislation, statute or other law as applicable but issued or enforced by a foreign jurisdiction; or any shareholder demands or shareholder derivative lawsuit complaining of a breach of duties by any of **Your** directors or officers, or seeking access to books, records or other information.

2.9 EMPLOYMENT RELATED LIABILITY

Claims relating to or arising or alleged to be related to or arising from any liability to any **Employee**, former **Employee** or prospective **Employee** in respect of any harassment, unfair or wrongful dismissal, wrongful disciplinary action, defamation, humiliation, discrimination, deprivation of career opportunity, refusal to employ or promote, or repudiate or breach of any employment contract under the Employment Rights Act 1996 (UK), or any liability arising or alleged to have arisen from any employee benefit plan or pension plan, including but not limited to the Pensions Act 1995 (UK) or other legislation, regulation or laws governed or enforced by the Occupational Pensions Advisory Service or any other similar entities, bodies or enforcement authorities.

This exclusion does not apply to **Your** data protection obligations to **Your Employees** under applicable UK, European Union or other international data protection laws.

2.10 FAILURE OF ANY GOODS OR SERVICES

Claims relating to or arising or alleged to be related to or arising from the failure of any goods or services to conform with any represented quality or performance, liquidated damages, any breach of express warranty or guarantee, any failure to provide goods or products, or perform services within a specified time period, by a deadline or according to specified milestones.

2.11 FAIR CREDIT REPORTING

Claims relating to or arising or alleged to be related to or arising from any actual or alleged violation of the Consumer Credit Act 1974 (UK) or any amendment of or addition to such laws or any other United Kingdom or foreign act, statute, regulation, rule or common law or European Union directive.

2.12 FEES AND EXPENSES FOR THE PERFORMANCE OF A PCI DSS ASSESSMENT

PCI Fines do not include the fees and expenses for a Qualified Security Assessor to perform any PCI DSS Assessment or similar audit.

2.13 FORCE MAJEURE

Claims relating to or arising or alleged to be related to or arising from fire, smoke, explosion, lightning, wind, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, act of God or any other similar physical event howsoever caused or from any consequential losses arising or alleged to have arisen therefrom.

2.14 GAMBLING AND LOTTERIES

Claims relating to or arising or alleged to be related to or arising from any gambling, sweepstakes, lotteries, promotional contests or quizzes.

2.15 INACCURATE PRICING OF GOODS

Claims relating to or arising or alleged to be related to or arising from any inaccurate, inadequate or incomplete description of the price of **Your** goods, products or services, or cost guarantees, cost representations, contract price or estimates of probable costs or costs estimates being exceeded.

2.16 INSOLVENCY

Claims relating to or arising or alleged to be related to or arising from **Your** insolvency, financial impairment, or bankruptcy.

2.17 INTERNET ACCESS

In respect of any failure of, interruption to, or outage of internet access provided by an internet service provider hosting **Your** website including any failure of telephone lines, data transmission lines or any other infrastructure comprising or supporting the internet such as but not limited to equipment enabling wireless or satellite transmission except to the extent these lines or infrastructure are under **Your** direct operational control.

2.18 MECHANICAL OR ELECTRICAL FAILURE

Expenses or costs associated with a **Claim** relating to or arising or alleged to be related to or arising from any mechanical or electrical failure attributable to an error or omission on the part of a third party acting independently of **You** or to any electrical power interruption, blackout, short circuit, induction or voltage fluctuations outside **Your** operational control.

2.19 TWO FACTOR AUTHENTICATION

We shall not be liable to make any payment or provide any benefit or service directly or indirectly arising from, attributable to or based upon **Your** failure to apply and maintain Two Factor Authentication to any web-based access to email, accounting software or data sources.

2.20 UNENCRYPTED MOBILE AND PORTABLE DIGITAL STORAGE DEVICES

Claims relating to or arising out of any mobile or portable digital storage device containing data in an electronic format unless the data stored on such device or media is stored in an encrypted format. A mobile or portable storage device includes but is not limited to USB drives, CD roms, laptops and mobile phones.

2.21 SANCTIONS

Action, event, and omission or otherwise that would expose **Us** to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the United Nations, European Union, United Kingdom or United States of America.

2.22 LEGISLATIVE AND/ OR REGULATORY PROTECTION OF MINORS WHEN ONLINE

Expenses or liabilities **You** incur and relate to, or arise from, any failure to comply with the Digital Economy Act 2017 (UK), Malicious Communications Act 1998 (UK), or equivalent legislation within the UK, European Union or international laws written specifically to protect the rights of minors in the collection, storing, sharing and displaying of data, information or likenesses of minors or in the access of or use of **Your** website(s) by minors.

2.23 UNAUTHORISED COLLECTION OF DATA

Claims relating to or arising or alleged to be related to or arising from any failure to obtain appropriate consent in respect of the collection, storage or sharing of any data including Personal Data (including but not limited to internet search histories, cookies and online purchasing profiles).

2.24 UNFAIR TRADE PRACTICES

Claims relating to or arising or alleged to be related to or arising from any actual or alleged antitrust violation, restraint of trade, unfair competition or false, deceptive, or unfair trade practices.

2.25 UNJUST ENRICHMENT

Claims relating to or arising or alleged to be related to or arising from **Your** gaining of profit, remuneration or financial advantage to which **You** were not legally entitled except for amounts paid to **You** or on **Your** behalf by **Us** under the **Policy** incurred until such time as there is a final decision or determination by any court, arbitration panel or arbitrator, or governmental, regulatory or administrative body finding that **You** were not so entitled, or **You** admit that **You** were not so entitled. If this occurs, **You** are obliged to reimburse the amount paid to **You** or on **Your** behalf by **Us**.

2.26 UNSOLICITED COMMUNICATIONS

Claims relating to or arising or alleged to be related to or arising from the unsolicited distribution, transmission or posting of emails, texts, advertisements or other communications by **You** or with **Your** knowledge, permission or authorisation or constructive knowledge.

2.27 WAR

Loss or damage directly or indirectly occasioned by, happening through or as a consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalisation or requisition or destruction of or damage to property by or under the order of any government or public or local authority (unless otherwise specifically provided for in the **Policy** or **Schedule**).

2.28 WILFUL, INTENTIONAL, MALICIOUS, RECKLESS, DISHONEST, FRAUDULENT OR CRIMINAL ACT OR OMISSION

Wilful, intentional, malicious, reckless, dishonest, fraudulent or criminal act or omission (including the making of any defamatory statements by **You**, or any of **Your** directors or officers or senior managers.

We will pay **Defence Costs** relating to any alleged defamatory statements incurred until such time as there is a final decision by any court, arbitration panel or arbitrator, or governmental, regulatory or administrative body finding that **You** deliberately made such defamatory statements, or **You** admit to having deliberately made such defamatory statements.

This exclusion will not apply when the wilful, intentional, malicious, reckless, dishonest, fraudulent or criminal act or omission was committed without the knowledge or consent of any of **Your** directors or officers or senior manager but not limited to **Your** Chief Information Officer, Risk Manager, General Counsel, Chief Operations Officer, Chief Executive Officer or their functional equivalents.

If **We** pay **You** an amount (including **Defence Costs**) and later there is a determination or decision from any court, arbitration panel or arbitrator, or governmental, regulatory or administrative body finding any such intentional, wilful, deliberate, criminal, dishonest, fraudulent or malicious act, error or omission by **You** or intentional violation of law by **You**, or **You** admit to such an act or omission then **You** must reimburse to **Us** any money paid to **You** or on **Your** behalf.

The **Schedule** will confirm

- a) Whether **You** have purchased cover under the relevant **Operative Clauses**; and
- b) The **Limit** and **Excess** applicable to each **Operative Clause**.

All payments made to **You** under this **Policy** shall reduce and may exhaust the **Limit(s)**, **Sub-limits** and **Aggregate Limit**. They will be subject to **Exclusions** and **Time Retentions**.

We will only pay that portion of any **Loss** or **Claim** which exceeds the **Excess**. **We** can reduce payment of any covered amount owed by **Us** to **You** by an amount toward the **Excess**. The value of the **Excess** does not reduce the applicable **Limit**.

Under no circumstances will **We** pay **You** more than the **Aggregate Limit**.

3.1 LIMIT AND SUB-LIMIT

The **Limit** applicable to each **Operative Clause** is the maximum amount **We** will pay under this **Policy** including expenses where applicable, regardless of the number of **Triggering Events, Claims** or **Losses**.

Any **Sub-limit** applicable to an **Operative Clause**, is the maximum amount **We** will pay under this **Policy** including expenses where applicable, regardless of the number of **Triggering Events, Claims** or **Losses** and is part of and not in addition to the **Operative Clause Limit**.

All payments made to **You** or on **Your** behalf by **Us** under this **Policy** shall reduce and may exhaust the **Limit(s)**, **Sub-limit(s)** and **Aggregate Limit**. They will be subject to **Exclusions** and **Time Retentions**.

3.2 AGGREGATE LIMIT

The maximum amount **We** will pay **You**, or on **Your** behalf, in the aggregate under this **Policy** shall be the **Aggregate Limit** stated in the **Schedule** regardless of the number of **Triggering Events, Claims** or **Losses**.

3.3 LOSS OF INCOME

We will calculate the amount **We** will pay **You** for **Your** loss of income by reference to the amount of lost profit due to **Computer System Disruption**. **We** will do this by applying the **Rate of Gross Profit** to the amount by which **Turnover** falls short of **Standard Turnover** during the **Indemnity Period**.

For the purposes of this clause:

- a) **Gross Profit** - shall mean Standard Turnover less Operating Expenses;
- b) **Indemnity Period** - shall mean the period of one hundred and twenty (120) days following a Computer System Disruption;
- c) **Operating Expenses** - shall mean standard expense incurred by **You** (including salaries, standing and other charges), in the operation of the **Business**;
- d) **Rate of Gross Profit** - shall mean the average rate of Gross Profit earned on Turnover during the three (3) financial years prior to the **Computer System Disruption**;
- e) **Standard Turnover** - shall mean total earnings derived from the operation of the **Business** during the previous thirty-six (36) months;
- f) **Turnover** - shall mean the amount of money paid or payable to **You** for goods sold and delivered and for services rendered during the course of the **Business**.

We may make such adjustments as may be necessary to provide for the trend of the **Business** and for variations in or special circumstances affecting the **Business** either before or after the **Computer System Disruption** or which would have affected the **Business** had the **Computer System Disruption** not occurred so that the adjusted figures shall represent as nearly as may be practicable the results which but for the **Computer System Disruption** would have been obtained during the relative period after the **Computer System Disruption**.

3.4 AGGREGATION AND ALLOCATION

In the event that a **Loss** or **Claim** is covered under more than one **Operative Clause** of this **Policy**, only one **Excess** shall apply. The highest of any applicable excesses under the relevant **Operative Clauses** which are breached will be the amount payable.

3.5 DUAL INSURANCE

We will not pay any claim if any loss, damage or liability covered under this insurance is also covered wholly or in part under any other insurance except in respect of any amount in excess of the amount which would have been covered under such other insurance had this insurance not been effected.

4.1 CLAIM NOTIFICATION & BREACH RESPONSE

We will only pay for **Loss** or **Damages** if **You** comply with the following provisions.

You must provide notice to **Us** as soon as reasonably practicable after the occurrence of a **Triggering Event** which does or which may result in a **Loss** or **Claim**.

You must provide **Us** with notice by contacting the **Incident Manager** who will assist **You** in the handling of a **Triggering Event**. They can be contacted 24 hours-a-day, 7 days per week on the telephone number or via the monitored email address shown in the **Schedule**. The **Incident Manager** will arrange for **You** to be provided with the services of our Cyber Response Team.

We will cover the costs of the *Cyber Response Team* up to the **Aggregate Limit**. The costs of the *Cyber Response Team* will be subject to the **Excess**.

4.2 CLAIMS ASSISTANCE, COOPERATION AND CONDUCT

You must provide assistance to or cooperate with **Us** or representatives appointed on **Our** behalf. This includes cooperation and assistance in the investigation, production or preservation of documentation, information or other physical evidence about a **Triggering Event**.

You must provide such information, respond to all relevant correspondence, communication, demand, **Claim** for, adjudication notice, referral, statement of case, submission, notice of hearing, order or other correspondence from during the resolution process (including communication from a court, arbitrator, mediator, adjudicator) in a timely manner. **You** may also be required to provide a position statement, witness statement, expert report, legal or quasi legal paper or report.

You must comply with any request for the physical or electronic examination of the property or operations or **Computer Systems** in relation to which a **Loss** or **Claim** arises. This includes allowing **Us**, approved agents, legal counsel or professional advisors to inspect and audit hard and electronic copies of any relevant files and take copies of them for the **Claims** adjustment process.

If **You** notify a **Loss** believing the same to be false or fraudulent with respect to the amount claimed or otherwise this **Policy** shall become void and **You** shall forfeit all benefit under it.

You must not admit any liability to a customer or other third party nor make any offer or payment without **Our** prior written agreement. Failure to comply with this requirement may result in a reduction of the payment that **We** make under this section (in proportion to the detriment that **We** have suffered as a result of **Your** actions). **You** must not waive or prejudice **Our** rights in relation to subrogation and salvage.

4.3 CONFIDENTIALITY

Except for when **You** are required to do so by law, **You** must not disclose to any third party the extent of cover under this **Policy** or the **Exclusions** or conditions without **Our** prior written consent.

4.4 COOPERATION WITH LAW ENFORCEMENT AUTHORITIES

In the event that **You** receive a **Credible Threat**, **You** must make every reasonable effort to notify and thereafter cooperate with the relevant law enforcement authorities before paying or entering into a commitment to pay any **Extortion Monies**.

4.5 RECOVERY OF AMOUNTS PAID

You will repay **Us** any amounts paid to **You**, under this **Policy** if it can be proven there is no coverage under this **Policy**.

5.1 ASSIGNMENT

You interest under this **Policy** cannot be assigned in whole or in part without **Our** prior written consent.

5.2 INSOLVENCY

If **You** become bankrupt or subject to insolvency proceedings, this will not automatically terminate or relieve **Us** of obligations owed under this **Policy**.

5.3 CANCELLATION

You can cancel this **Policy** at any time during the **Policy Period** by providing written notice to **Us** specifying when such cancellation is to take effect (must be after **We** receive written notice). If notifying **Us** by post, receipt will be deemed to have occurred on the third day after mailing.

We can cancel this **Policy** on thirty (30) calendar days' notice (or fourteen (14) calendar days' notice in the event of non-payment of the **Premium**) at any time during the **Policy Period** by providing written notification to **You** at the address stated in the **Schedule**. Such cancellation will take effect on the thirtieth (30) day (or fourteenth (14) day in the event of non-payment of the **Premium**) after **Your** receipt of **Our** written notification. If notifying by post, receipt will be deemed to have taken place on the third (3rd) calendar day after mailing.

In the event of cancellation as above, provided that **You** have not notified any actual or potential **Loss** or **Claim**, **You** will be entitled to a pro-rata refund of **Premium**. No **Premium** will be refunded to **You** if any actual or potential **Loss** or **Claim** has been notified prior to cancellation.

5.4 INNOCENT INSURED PROVISION

If coverage under this **Policy** would be excluded, suspended, or lost because of non-compliance with any provision of this **Policy**, including that relating to the giving of notice of a **Claim** to **Us**, then such insurance as would otherwise be afforded will be paid with respect to those of **You** who did not personally commit or personally participate in committing or personally acquiescing in such failure to give notice, provided that **You** are entitled to the benefit of this **Policy** and provided notice as soon as practicable upon knowledge of the non-notification.

5.5 MERGERS AND ACQUISITION AND CHANGE OF CONTROL

If during the operation of this **Policy**, **You** or any **Subsidiary** of **You** acquires another entity (which increases **Your** assets, revenue or **Personal Data** processed by **You** by more than (10%) ten per cent), **You** will not be covered unless **You** receive prior written notice from **Us** (regarding the acquisition) and **You** agree to pay any resulting additional premium that **We** may calculate.

If during the **Policy**, **You** are acquired by another entity or merged with another entity, any cover under this **Policy** terminates on the date of the merger or acquisition. **We** can issue an **Endorsement** to extend cover and may charge an additional **Premium**.

5.6 MATERIAL CHANGES

You must advise **Us** as soon as practicable of any material changes to information of which **You** become aware. **We** reserve the right to amend the terms and conditions of this **Policy** and to charge an additional **Premium** resultantly.

5.7 LAW & JURISDICTION

This **Policy** is subject to the law stated in the **Schedule**. The **Courts** stated in the **Schedule** shall have exclusive jurisdiction to resolve any disputes involving this **Policy**.

5.8 COMPLAINTS

We aim to provide the highest quality of service. However, if **You** feel that the level of service **You** have received falls short of the standard that **You** expect, please let **Us** know immediately. If **You** have a complaint **You** have the right to raise **Your** complaint with Bewica or **Your** agent or **You** can write to:

The Compliance Manager
Am Trust at Lloyd's
1 Great Tower Street London
EC3M 5AA
Email: complaints@amtrustgroup.com
Telephone: +44 (0) 20 3003 6899

If **You** remain dissatisfied, **You** may refer **Your** complaint to Lloyd's who will investigate and provide a response. See: www.lloyds.com/complaints

Ultimately, if **You** remain dissatisfied **You** may in writing refer **Your** complaint to the Financial Ombudsman Service (FOS). See: www.financial-ombudsman.org.uk

This complaints procedure is without prejudice to **Your** right to initiate legal proceedings.

Aggregate Limit: Means the **Aggregate Limit** which is stated in the **Schedule**.

Bodily Injury: Means death or any physical injury or illness.

Breach Expenses: Means the reasonable and necessary monetary expenses incurred by **You** with **Our** prior approval, following a **Data Breach**. These include:

- a) **Forensic cost expenses** – being expenses associated with computer forensic analysis performed by outside experts to provide confirmation of or respond to a **Data Breach** and to identify the affected **Data Subjects**;
- b) **Legal expenses** - being expenses associated with legal advice provided to **You** and action taken respond to a **Data Breach** and comply with laws, regulations or obligations following a **Data Breach**;
- c) **Notification expenses** – being expenses to comply with regulatory notification requirements, the drafting cost and applicable postage cost of appropriate notification letters to both the regulator and those affected by the **Data Breach** and shall include voluntary notification if agreed upon by **Us** in writing prior to such notification;
- d) **Call centre expenses** – being expenses for the provision of a call centre service to respond to inquiries from affected **Data Subjects** following the dispatch of notification communications;
- e) **Credit monitoring expenses** – being expenses for up to twelve (12) months' credit monitoring services (or such longer period as may be required under relevant legislation or by a regulator) offered by **You** to the **Data Subjects** within twelve (12) months from the date on which **You** first learned of the actual **Data Breach**.

Breach Expenses do not include:

- a) Salaries, overhead expenses, or other internal charges or costs **You** incur for any time **You** or **Your Employees** spend cooperating with any investigations or responding to any customer complaints following a **Data Breach**;
- b) Any customer credits, hardware or software upgrades; or
- c) Expenses associated with the repair of **Your** reputation, including all related professional fees of independent advisors, legal advice concerning media strategy and any public relations services to mitigate the adverse reputational effects of a **Data Breach**;
- d) The fees and expenses for a Qualified Security Assessor to perform any PCI DSS Assessment or similar audit.

Business: The commercial activities undertaken by **You** including the offering of any products, services or activities carried on in the course of trade and commerce.

Business Interruption: Means **Loss of Income** to the **Business** and any **Increased Costs of Working** lasting longer than the **Time Retention**.

Claim: Means:

- a) A demand in writing to cease and desist, for compensation, **Damages** or injunctive relief;
- b) A notice in writing of an intention to commence legal, arbitration or adjudication proceedings;
- c) The commencement of legal, arbitration or adjudication proceedings, an invocation of a pre-action protocol; or
- d) An investigation or a proceeding by a regulator alleging any failure to maintain the security of **Personal Data** or to comply with the requirements of data protection legislation.

Computer System: Means:

Computer and telecommunication networks including computers and computer devices, data storage devices, back up facilities, operating systems, network systems, hardware, software, firmware, websites, email systems, intranet; owned by **You** or provided to **You** by a Third Party under written contract.

Computer System Attack: Means **Computer System Attack** which is stated under **Triggering Events** in Section 1.

Computer System Disruption: Means **Computer System Disruption** which is stated under **Triggering Events** in Section 1.

Computer System Breach: Means any unauthorized electronic attack, disruption, intrusion designed to destroy, impair, impact the functionality of a **Computer System**.

Credible Threat: Means a threat that is real and immediate, that is not conjectural or hypothetical to:

- a) Release, divulge, disseminate, destroy or use **Your Digital Assets** acquired by unauthorized access or unauthorized use of **Your Computer Systems**;
- b) Introduce malware, ransomware into **Your Computer System**;
- c) Corrupt, damage or destroy **Your Computer System**;
- d) Electronically communicate with **Your** customers and falsely **Claim** to be **You** or to be acting under **Your** direction in order to falsely obtain personal confidential information of **Your** customers (also known as “pharming,” “phishing,” or other types of false communications); or
- e) Restrict or hinder access to **Your Computer System**, including the threat of a criminal or malicious denial of service attack.

Cyber Extortion Threat: Means the **Cyber Extortion Threat** which is included under **Triggering Events** in **Section 1**.

Cyber Theft: Means the transfer, disbursement, payment, delivery, alteration, corruption or **Loss** of money, securities or assets belonging to **You** or from an account that is in the trust or control of **You**.

Damages: Means any financial award or settlement to a claimant, including pre-judgement interest and post-judgement interest. **Damages** do not include any criminal fines, criminal penalties or aggravated, punitive and exemplary damages unless insurable by applicable law. **Damages** are inclusive of **Defence Costs** and costs that **You** may be liable to pay to a Claimant.

Data Breach: Means **Data Breach** as per the meaning stated under **Triggering Events** in Section 1.

Data Recovery Expenses: Means the costs incurred by **You** with **Our** prior approval, in relation to determination and/or restoration of damaged or destroyed computer programs, software or electronic data and/ or the costs associated with ensuring the data are in the same or substantially the same position it was, prior to the **Data Breach, Security Breach** or **Computer System Attack**.

Data Recovery Expenses do not include:

- a) Salaries, overhead costs, or other internal charges or costs **You** incur for any time **You** spend following a **Data Breach**;
- b) Any customer credits, hardware or software upgrades; or
- c) Costs associated with the repair of **Your** reputation, including all related professional fees of

independent advisors, legal advice concerning media strategy and any public relations services to mitigate the adverse reputational effects of a **Data Breach**.

Data Subjects: Means an individual whose **Personal Data** has been or may have been compromised in the relevant **Data Breach**.

Defamation: Means damaging the reputation of another person or entity through intentional false communication that results in libel, slander, trade libel, product disparagement and malicious falsehood. This communication can be written, spoken, pictures, gestures or any other form which results in a disparagement of character, reputation, decreases respect, regard or confidence in which a person held or which a product or service came to acquire.

Defence Costs: Means all legal costs and expenses (excluding **Your** internal costs and expenses) incurred with **Our** prior approval in relation to the investigation, defence, mitigation or settlement of any **Claim**. **Defence Costs** will not be paid for any part of a **Claim** for which **You** do not have cover under this **Policy**.

Digital Assets: Means assets or content stored in an online account owned by **You** or controlled by **You**. **Digital Assets** do not include hardware.

Employees: Means an individual contracted to work for **You** under a contract of services in a permanent or part time or fixed term basis (excluding an independent contractor). It includes individuals undertaking work experience or internship (paid or unpaid).

Excess: Means the **Excess** which is stated in the **Schedule**.

Exclusions: Means the **Exclusions** listed in **Section 2**.

Extended Reporting Period: Means the **Extended Reporting Period** stated in the **Schedule**.

Extortion Monies: Means monies, property, online credit or other online currency (such as BitCoin) payable by **You** with **Our** prior written consent together with associated forensic costs and legal expenses.

Increased Costs of Working: Means costs incurred by **You** with **Our** prior written consent to avoid or mitigate the effects of a system outage or **Computer System** interruption, or any costs associated with the discovery or minimization of any interruption or degradation of the **Computer System**, costs associated with preserving evidence and/or substantiating **Your** loss(es).

Infringement of Intellectual Property Rights: Means the broadcast, publication or display or other digital means of disseminating media content which is protected by intellectual property laws applicable within the UK, EU or other international laws which can be enforced within the UK.

Incident Manager: Means the **Incident Manager** as outlined in the **Schedule**.

Limit: Means the **Limit** corresponding to each **Operative Clause** stipulated in the **Schedule**.

Loss: Means any **Breach Expenses, Data Recovery Expenses, Special Expenses, Extortion Monies, Cyber Theft, Business Interruption, Regulatory Fines Penalties and Costs and PCI Charges**.

Loss of Income: Means the **Loss of Income** suffered by **You** calculated in accordance with **Section 3**.

Media Event: Means a **Media Event** as outlined under the **Triggering Events** in **Section 1**.

Online Account: Means an account which is stored or accessed through the internet. An **Online Account** specifically includes email accounts but also includes other internet hosted accounts such as but not limited to accounts held for the purposes of hosting data on the internet.

Operative Clauses: Means the coverage provided under each of the items listed in Section 1.1 and Section 1.2 of this **Policy Wording**. These should be read in conjunction with the **Schedule** to determine whether cover is available to **You** under this **Policy** and the applicable limits of liability, **Sub-Limits**, **Excess** and **Time Retention**.

PCI Breach: Means a **PCI Breach** as stated under **Triggering Events** in **Section 1**.

PCI Assessments: Fines, penalties, assessments or payments imposed by the Payment Card Industry ('PCI') Security Standards Council for any breach of **PCI Data Security Standards** together with legal expenses incurred in connection with any preceding investigation.

PCI Data Security Standards: Standards, requirements and procedures issued from time to time by the Payment Card Industry Security Standards Council.

Period of Restoration: Means the period of time that commences upon the date when the interruption, degradation or failure of the **Computer System** began and ends on the later of:

- a) No more than thirty (30) consecutive days after the date the **Computer System** was restored or could have been repaired; or
- b) restored with reasonable speed to the same condition, functionality and level of service that existed prior to the **Loss**; or
- c) One hundred and twenty (120) consecutive days after the date upon which the interruption, degradation or failure of the **Computer System** began.

Personal Data: Means data which is controlled or processed by **You** that relates to a **Data Subject** by which a **Data Subject** can be identified or from which it may be possible to obtain other data or other information by using the data identifying the individual.

Personal Information: Means the information that forms **Personal Data**.

Phishing Attack: Means a **Phishing Attack** as outlined under **Triggering Events** in **Section 1**.

Policy: Means this **Policy Wording**, the **Schedule** and any **Endorsements**.

Policy Period: Means the period for which the **Policy** operates as stipulated in the **Schedule**.

Privacy Regulations: Means statutes, regulation and legislative instruments within the UK or alternatively based upon an European Union Directive or international legal obligation associated with protecting the confidentiality, control, use of and access to personally identifiable information including financial and medical information as that information exists now and in the future.

Property Damage: Means physical injury to, impairment, destruction or corruption of any tangible property including loss of such property. **Property Damage** does not apply to data.

Regulatory Fines, Penalties and Costs: Means fines, penalties, assessments or any other financial imposition or penalty which **You** are obliged to pay based upon an order or requirement or demand from a regulator or subject to privacy regulations within UK legislation, a European Union directive or international legal obligation associated with the protecting of confidentiality, control and use of or access to **Personal Data** together with legal expenses incurred in connection with any preceding investigation.

Retroactive Date: Means the **Retroactive Date** stipulated in the **Schedule**.

Retroactive Period: Means the period beginning with the **Retroactive Date** up to but not including the **Policy Period**.

Security Breach: Means a **Security Breach** which is stated under **Triggering Events** in **Section 1**.

Schedule: Means the **Policy Schedule** confirming the coverage available to You under this **Policy**.

Social Engineering Event: Means a **Social Engineering Event** which is outlined under **Triggering Events** in **Section 1**.

Special Expenses: Means reasonable and necessary costs **You** incur with **Our** prior consent to prevent, preserve, minimize, or mitigate any further damage to **Your Computer System**, including specialists, outside consultants or forensic experts **You** engage to preserve critical evidence of any criminal or malicious wrongdoing and/or purchase replacement licenses for programs because the copy protection system and/or access control software was damaged or destroyed by a **Loss**.

Sub Limits: Means the **Sub Limits** stipulated in the **Schedule**, as applicable.

Subsidiary: Means any company in respect of which the legal entity named as the **Insured** in the **Schedule** to this **Policy**

- a) holds more than half of the issued share capital;
- b) controls more than half of the voting power; or
- c) otherwise controls the composition of the board of directors.

Time Retention: Means the **Time Retention** stipulated in the **Schedule**.

Triggering Event: Means one of the events listed under the heading **Triggering Events** in **Section 1**.

We/Us/ Our: Means the **Underwriters** subscribing to this **Policy** as shown in the **Schedule**.

You/ Your: Means the insured party stipulated in the **Schedule**.