

Accessing your complimentary risk management package from OSR

OSR are dedicated to supporting your business with a multi layered cyber solution to protect you and ensure your staff are educated and prepared. These are just some of the benefits that you have **FREE** complimentary access to within your OSR Cyber Policy.



OSR: Breach Defence Portal

OSR have partnered with DynaRisk to provide an easy-to-use cyber security risk management portal designed to help SME businesses understand and manage their digital exposures by including Dark Web and Hacker Chatter Monitoring and Vulnerability Scanning with Education and Phishing Simulation learning modules.*

Key benefits:

- ✓ Detection of leaked data
- ✓ Educate & train your employees
- ✓ Prevent & respond to data breaches
- ✓ Continuously discover assets
- ✓ Easy-to-use dashboard

The point of contact provided by your broker will be emailed with link to enable activation of the portal for your business.



GDPR123 – Training and Consultancy Benefits

Increasingly, we are seeing cyber criminals focus more on hacking people than hacking networks so it is essential to ensure your staff are properly educated and prepared. Via GDPR 123, OSR will provide you with online employee awareness training on matters of GDPR compliance, Cyber Security and Data Protection. In addition to this, GDPR 123 will provide you with a complimentary one-hour consultation to discuss all things GDPR.

[Click here to register](#) or call **0203 457 4683** and select Option 2.

Please Note:

** To use this service, you must have a company-owned domain. The services will not be accessible for those using a free email services i.e @gmail.com*

Statement of Fact: OSR Cyber Plus

Date of Issue: 20/12/2024
Policy Number: CY-CP-00013017

Important Information

This Statement of Fact records the information provided to Optimum Specialty Risks and any assumptions that have been made about your business/organisation. It is important that the information is correct otherwise your claim maybe refused, or policy cancelled. This document must be read together with your schedule and the policy wording.

Duty of Disclosure

Please note that under English law, a business insured has a duty to disclose to the insurer every material circumstance which it knows or ought to know after reasonable search, in order that a fair presentation of the risk is made to the insurer. It is important to remember that you have a duty to make a fair presentation of the risk to the insurer at the start of the policy, when there are any mid-term changes and at the renewal of the policy.

A circumstance is material if it would influence an insurer's judgement in determining whether to take the risk and, if so on what terms. If you are in any doubt whether a circumstance is material we recommend that it should be disclosed.

Failure to disclose a material circumstance may entitle the insurer to impose different terms on the cover or proportionately reduce the amount of any claim payable, in some circumstances the insurer will be entitled to avoid the policy from inception and in this event any claims under the policy would not be paid.

Insured Details

Policyholder: Saltash Town Council
Subsidiary Companies: -
Principle Address: Saltash Town Council
12 Lower Fore Street
SALTASH
PL12 6JX
Trade: Councils / Municipalities / Public Institutions
Business Description: Local Government
Website: <https://www.saltash.gov.uk>
Date Established: 01/01/2000

Revenue

Country	Revenue Generated
UK:	£1,388,217
EU:	£0
USA/Canada:	£0

Australia/New Zealand: **£0**

Rest of World: **£0**

Does the Insured have any financial nexus, financial agreements or contractual associations to Russia, Ukraine or Belarus? **No**

1. What percentage of your revenue is delivered from on-line sales? **0.00**

If in excess of 25% please answer 2, 3 & 4 below

2. Do you (or your cloud provider) provide high availability for your transactional website and applications?

If yes, please provide brief details

3. Do you deploy a Web Application Firewall?

4. If yes, does the Web Application Firewall sit in front of the database, or network gateway if more than one database is being protected

If yes, please provide brief details

5. Total number of employees **26**

Section Additional Informaton

Records

Please give the total number of personal data records for which you are legally liable:

Name	Number of Records
Payment Card Industry (credit and debit cards):	0
Driving licence, Tax or Social Security numbers:	29
Other Personal Data:	45
Healthcare:	0
Financial (not credit or debit cards):	29

Do you adhere to the current legislation governing the handling of Personal Data in those territories in which you trade? **Yes**

Section Additional Information

Network Security

Do you allow remote access to your corporate network? **Yes**

If yes, is this protected by a minimum of 2 factor authentication? **Yes**

Do you run commercial grade antivirus and firewall protection across your entire network, including servers and all end points? **Yes**

How often are virus signatures updated? **Automatically**

If other, please specify:

Do you run a Security Information and Event Management Application? **No**

If so, is this monitored by a Security Operations Centre on a 24/7 basis?

Please provide details of all other network security applications running on your network and endpoints:

Have you disabled Remote Desktop Protocol on all of your endpoints, including servers where it use is not required? **No**

If not, is access restricted only through VPN, network level authentication and Multifactor authentication (MFA)? **Yes**

Do you encrypt all sensitive data whilst:

In transit **Yes**

Stored on servers? **Yes**

Stored on portable media? **Yes**

How often do you undertake an external security audit? **Annually**

If other, please specify:

Who has (position) overall responsibility for network security

How often do you apply critical patches? **Automatically**

If other, please specify:

Do you enforce a policy of auditing and managing computer and user accounts? **Yes**

Do you enforce password changes at least every three months? **No**

Is access to sensitive data restricted according to the employee's user requirements? **Yes**

Do you automatically revoke all IT access for staff on leaving your employment? **Yes**

How often is your information security policy reviewed? **Annually**

If other, please specify:

Section Additional Information

PCI Compliance

Are you in Compliance with the Payment Card Industry Data Security Standards? **Yes**

What level of merchant is the insured?

If Level 1, please advise Date of last PCI audit? **27/06/2024**

Were there any major non-compliance issues? **No**

If so, have these been rectified?

Are you EMV (chip and pin) compliant? **Yes**

Are you running Microsoft XP PoS Ready or any other unsupported application? **No**

Section Additional Information

Business Continuity

Are you ISO22301 certified?	No
Do you have a written business continuity plan that is reviewed annually?	Yes
Does your business continuity plan assess the risk from cyber perils?	No
Network Dependency - after how long will your business be impacted by an interruption to, or loss of, your network?	24hr
How long will it take to fully restore your critical systems (Recovery Time Objective)?	24hr
Do you test the DRP/BCP annually?	Yes
Do you (or your cloud/outsource partner) configure your network to provide high availability or failover for your website and other critical applications and data?	No
Do you back up data that is necessary to run your business at least every 5 days?	Yes
Is your backed up data stored offline such that it is not accessible from your network?	Yes
How often is back up data tested for integrity?	Monthly

Section Additional Information

Email Security

Do you use any of the following to authenticate your email:

SPF (Sender Policy Framework)	Yes
DKIM (DomainKeys Identified Mail)	Yes
DMARC (Domain-based Message Authentication, Reporting and Conformance)	Yes
Do you use Office 365?	Yes
If so, have you deployed Advanced Threat Protection / Defender?	Yes
Do you scan incoming email for malicious attachments or links?	Yes
Do you provide training to assist employees in spotting phishing and other social engineering attacks?	Yes
If yes, how frequently?	

Section Additional Information

Funds Transfer Fraud

Does the Insured have a procedure whereby, all new (including changes to existing) payment details or contact details are confirmed by an alternative method to the original method used, before any payment is made?	Yes
Are transfer of funds over GBP 10,000 and any instructions for releasing assets, funds, or investments approved by at least two staff members?	Yes

Claim Experience

Have the Insured suffered any loss or has any claim been made against them or are they aware of any matter that is reasonably likely to give rise to any loss or claim in the last 36 months where they would

seek an indemnity from a cyber insurance policy?

No

Details:

Disclosure

Can you confirm that the proposer(s), or any partner, or any director, or any officer, have:

- a) never been declared bankrupt or disqualified from being a company director
- b) no outstanding County Court Judgement(s) or Sheriff Court Decree(s)
- c) never been officers of a company that has been declared insolvent, or had a receiver or liquidator appointed, or entered into arrangements with creditors in accordance with the Insolvency Act 1986
- d) never been convicted of or charged with a criminal offence, other than a conviction spent under the Rehabilitation of Offenders Act 1974
- e) never had any insurance proposal declined, renewal refused, had any special or increased terms applied or had insurance cancelled or avoided by Underwriters

Yes

Details:

Additional Information

Changes Required

Please tell your insurance adviser immediately if any details in this document are incorrect &/or require changing. We may need to change the terms and condition of your quotation/policy &/or premium.

Policy Schedule

Date of Issue:	20/12/2024
Policy Number:	CY-CP-00013017
Binding Authority Reference:	B0572MR24OS01
Policyholder:	Saltash Town Council
Subsidiary Companies:	-
Principal Address:	Saltash Town Council 12 Lower Fore Street SALTASH PL12 6JX
Trade:	Councils / Municipalities / Public Institutions
Broker:	Clear Insurance Management Ltd (Leicester)
The Insurer:	Underwritten by certain underwriters at Lloyd's (see Insurer Endorsement)
Period of Insurance:	From: 21/12/2024 To: 20/12/2025 Both days inclusive Local Standard Time at the Policyholder's Principal Address stated above in this Schedule.
Limit of Liability:	GBP 500,000 This is the maximum amount in the aggregate that the policy will pay including Defence Costs , irrespective of the number of Claims, Losses, Business Interruption Losses or Cyber Events giving rise to an indemnity under this policy Sub-Limit of Indemnity: GBP 50,000 Funds Transfer Fraud / Theft of Third Party Funds Sub-Limit of Indemnity: GBP 100,000 Telephone Hacking Sub-Limit of Indemnity: GBP 50,000 Bricking Incidents
Retention:	Retention each and every Cyber Event: GBP 500 Save that: In respect of cover under Clause 1.2 the Waiting Period is 24 hours per Business Interruption Event . The Retention above will apply to each and every Business Interruption Event once the Waiting Period has been satisfied. In respect of cover under Clause 1.3 the Retention is NIL
Retroactive Date:	Unlimited
Premium:	GBP 1,174.00
IPT:	GBP 140.88
Policy Fee:	GBP 60.00
Total:	GBP 1,374.88
Policy Wording:	OSR Cyber Plus v.2022.1

Endorsements Applicable: FTF0003 - Funds Transfer Fraud / Theft of Third Party Funds Endorsement
 TEH0001 - Telephone Hacking Endorsement
 BRI0001 - Bricking Incidents Endorsement
 TRE0002 - Territory Restriction Endorsement
 MAN0002 - Mandatory Endorsements
 INS0001 - Insurers Endorsement

Law and Jurisdiction: This agreement is governed by the law of England and Wales and is subject to the jurisdiction of the courts of England and Wales

Territorial Limit: Worldwide

Seat of Arbitration: England & Wales

Incident Response Provider (Claims Notification): Notifications to be made to: Canopus
 Email Address: cyber.incident@canopus.com
 Emergency Telephone Number: 0333 305 8045

Signed by and on behalf of Optimum Speciality Risks:



Authorised Signatory

Optimum Speciality Risk acts as agent of the Insurer in performing its duties under the Binding Authority, including binding cover and collecting premiums.

Optimum Speciality Risk is a trading name of Independent Broking Solutions Limited and is authorised and regulated by the Financial Conduct Authority (FCA) under company number 312026 Registered Office & Mailing Address: Unit 2 Kildegaard Business Park, Easthorpe Road, Easthorpe, Colchester, Essex, CO5 9HE. Registered in England and Wales No: 616849.

Lloyd's is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Registered Office: One Lime Street, London, EC3M 7HA.

FTF0003 - Funds Transfer Fraud / Theft of Third Party Funds Endorsement

Attaching to and forming part of Policy Number: CY-CP-00013017

The above policy (in this endorsement, the **Policy**) is amended as follows. Words in bold have the meanings defined in the above **Policy**, as amended by this endorsement.

SCHEDULE

The following provisions are inserted to the **Policy** Schedule:

FUNDS TRANSFER FRAUD / THEFT OF THIRD PARTY FUNDS COVER

Inception Date of coverage applicable to Funds Transfer Fraud Event cover and Third Party Funds Theft Event cover granted under this endorsement:	21/12/2023
Retention each and every Fund Transfer Fraud and/or Third Party Funds Theft Event :	GBP 500
Maximum aggregate sum the Insurer will pay in respect of any and all Funds Transfer Fraud(s) and / or Third Party Funds Theft Event(s) under the Policy :	GBP 50,000

The aggregate sum set out above shall be part of and not in addition to the **Limit of Liability** set out in the **Policy** Schedule.

1. INSURANCE COVER

NEW COVER

The following provision is inserted into the **Policy**:

In consideration of the payment of or agreement to pay the premium by the **Policyholder** on behalf of the **Insured**, the **Insurer** will pay, or where specified, reimburse the **Insured**, in excess of the applicable **Retention**, up to the maximum aggregate sum above, for:

1.5 any loss of funds or assets of the **Insured**, which: (i) occurs on or after the above **Inception Date**; (ii) is notified to the **Insurer** during the **Period of Insurance** in compliance with the **Policy** terms; and (iii) is the sole and direct result of a **Funds Transfer Fraud Event**.

1.6 any **Loss** arising from any **Claim** against the **Insured** by any **Third Party** which (i) occurs on or after the above **Inception Date**, (ii) is notified to the **Insurer** during the **Period of Insurance** in compliance with the **Policy** terms; and (iii) is the sole and direct result of a **Third Party Funds Theft Event**.

2. GENERAL DEFINITIONS

The definition of **Claim** at clause 2.3 is deleted and replaced by the following definition:

Claim means any written demand, civil, criminal, judicial, administrative, regulatory or arbitral proceeding against the **Insured** seeking compensation or other legal remedy or penalty as a result of a **Data Liability Event**, **Media Liability Event**, **Network Security Event**.

Funds Transfer Fraud Event or **Third Party Funds Theft Event**.

NEW DEFINITIONS

The following definitions are inserted into the **Policy**:

Funds Transfer Fraud Event means the commission by any **Third Party**:

- i. via **Unauthorised Access** leading to any unauthorised electronic transfer of the **Insured's** funds or other financial assets from the **Insured's** computer system or network due to fraudulent manipulation of electronic documentation which is stored on the **Insured's** computer system;
- ii. of theft of funds or other financial assets from the **Insured's** bank account by electronic means, if the bank is unable to restore the **Insured** to the exact same financial position, they were in prior to the **Funds Transfer Fraud Event** taking place
- iii. of theft of money or other financial assets from the **Insured's** corporate credit cards by electronic means; and / or
- iv. of any phishing, vishing or other social engineering attack against the **Insured** that results in the unauthorised transfer of **Insured's** funds or other financial assets to a **Third Party**

Third Party means any legal entity or natural person who is not an **Insured**.

Third Party Funds Theft Event means the theft of money or other financial assets belonging to a **Third Party** for which the **Insured** is legally liable as a result of **Unauthorised Access** into the **Insured's** computer system.

3. EXCLUSIONS

Exclusion 3.13 of the **Policy** is deleted and replaced with the following exclusion:

The **Insurer** shall not be liable to make any payment or provide any benefit or service in respect of any **Claim** or **Loss**:

- arising out of the electronic transfer of any funds, monies or goods belonging to the **Insured**, or for which the **Insured** is legally responsible, except for a **Fund Transfer Fraud Event** or **Third Party Funds Theft Event**.

NEW EXCLUSIONS

The following exclusions are inserted into the **Policy**:

The **Insurer** shall not be liable to make any payment or provide any benefit or service in respect of any **Claim** or **Loss**:

- for any **Loss** or other financial losses in any way directly or indirectly connected with cryptocurrencies are excluded from the cover provided under the "FUNDS TRANSFER FRAUD / THEFT OF THIRD FUNDS PARTY" endorsement in respect of any **Funds Transfer Fraud Event** or **Third Party Funds Theft Event**.
- for any **Loss** or other financial losses caused by any **Funds Transfer Fraud Event** or **Third Party Funds Theft Event** where such event is perpetrated by, or with the knowledge or collusion of, any director, partner or employee of the **Insured**.
- caused by a **Funds Transfer Fraud Event** where the **Insured** does not have a written verification procedure in place.

All other terms, conditions and exclusions remain unchanged.

TEH0001 - Telephone Hacking Endorsement

Attaching to and forming part of Policy Number: CY-CP-00013017

The above policy (in this endorsement, the **Policy**) is amended as follows. Words in bold have the meanings defined in the above **Policy**, as amended by this endorsement.

SCHEDULE

The following provisions are inserted to the Policy Schedule:

TELEPHONE HACKING COVER

Inception date applicable to any Telephone Hacking Event :	21/12/2023
Retention each and every Telephone Hacking Event :	GBP 500
Maximum aggregate sum the Insurer will pay in respect of any and all Telephone Hacking Events :	GBP 100,000

The aggregate sum set out above shall be part of and not in addition to the **Limit of Liability** set out in the **Policy** Schedule.

1. INSURANCE COVER

NEW COVER

The following provision is inserted into the **Policy**:

In consideration of the payment of or agreement to pay the premium by the **Policyholder** on behalf of the **Insured**, the **Insurer** will pay, or where specified, reimburse the **Insured**, in excess of the applicable **Retention**, up to the maximum aggregate sum above, for:

1.7 any **Loss** arising from a **Claim** against the **Insured** made by a **Telcom Provider** which (i) occurs on or after the above **Inception Date**, (ii) is notified to the **Insurer** during the **Period of Insurance** in compliance with the **Policy** terms; (iii) and is the sole and direct result of a **Telephone Hacking Event**.

2. GENERAL DEFINITIONS

The definition of **Claim** at clause 2.3 is amended by including the following at the end of the definition:

Claim means any written demand, civil, criminal, judicial, administrative, regulatory or arbitral proceeding against the **Insured** seeking compensation or other legal remedy or penalty as a result of a **Data Liability Event**, **Media Liability Event**, **Network Security Event** or **Telephone Hacking Event** (where that written demand, civil, criminal, judicial, administrative, regulatory or arbitral proceeding is made by a **Telcom Provider**).

NEW DEFINITIONS

The following definitions are inserted into the **Policy**:

Telcom Provider means any telephone or communications service provider with whom the **Insured** has a written contract for the provision of telephony or communication services.

Telephone Hacking Event means any **Unauthorised Access** to the **Insured's** internal digital telephony infrastructure.

All other terms, conditions and exclusions remain unchanged.

BRI0001 - Bricking Incidents Endorsement

Attaching to and forming part of Policy Number: CY-CP-00013017

The policy is amended as follows. Words in bold have the meanings defined in the above policy.

1. The following provisions are inserted:

New Clause AT 1. INSURANCE COVER

"In consideration of the payment or agreement to pay the premium by the **Policyholder** on behalf of the **Insured**, the **Insurer** will pay, in excess of the applicable **Retention, Hardware Replacement Costs** incurred by the Insured following a **Bricking Incident** notified to the **Insurer** during the **Period of Insurance** in compliance with policy terms."

NEW CLAUSES AT 2. GENERAL DEFINITIONS

"**Bricking Incident** means a **Cyber Event** that renders a **Computer Device** non-functional for its intended purpose.

Computer Device means desktop and laptop computers, associated input and output devices, mobile devices, data storage, networking hardware and backup facilities which are owned by the **Insured**.

Hardware Replacement Costs means those costs incurred to replace any **Computer Device** affected by a **Bricking Incident** with identical or the nearest available functionally equivalent equipment to the extent those costs are (a) reasonable and (b) do not exceed the costs that would have been incurred had the **Insured** taken all reasonable steps to (i) minimise those costs and (ii) restore such **Computer Device(s)** to the level of functionality that existed immediately prior to the relevant **Cyber Event**."

2. Exclusions 3.1 and 3.8 are deleted and replaced with the following:

"3.1 for death, bodily injury or loss of or damage to tangible property; however this exclusion shall not apply to (i) mental anguish, emotional distress or mental injury as a result of a **Data Liability Event** or **Network Security Event** or (ii) any **Hardware Replacement Costs** that would otherwise be covered. For the avoidance of doubt, data held in electronic format is deemed not to be tangible property."

"3.8 any costs comprising, arising from or in connection with the upgrade or betterment of any **Computer Device**, application, system or network of the Insured."

3. All other terms and conditions to remain unchanged

4. The sub-limit set out above shall be part of and not in addition to the **Limit of Liability** set out in the Schedule.

All other terms, conditions and exclusions remain unchanged.

TRE0002 - Territory Restriction Endorsement

Attaching to and forming part of Policy Number: CY-CP-00013017

It is hereby understood and agreed that this **Policy** is amended as follows:

Notwithstanding anything to the contrary in this **Policy**, or any appendix or endorsement added to this **Policy**, there shall be no coverage afforded by this **Policy** for any:

- i. entity organized or incorporated pursuant to local law of the **Specified Area**, or headquartered in a **Specified Area**;
- ii. natural person during the time such natural person is located in a **Specified Area**;
- iii. part of a **Claim**, action, suit or proceeding made, brought or maintained in a **Specified Area**; or
- iv. loss of, theft of, damage to, loss of use of, encryption of, interruption to the operations or availability of, or destruction of any part of any property (tangible or intangible) located in a **Specified Area**, including, but not limited to, any **Computer System**, data, digital assets, money or securities located in a **Specified Area**.

For purposes of this endorsement, "**Specified Area**" means:

- a. The Republic of Cuba; or
- b. The Islamic Republic of Iran; or
- c. The Islamic Republic of Afghanistan; or
- d. The Republic of Belarus; or
- e. The Republic of the Union of Myanmar; or
- f. The Democratic People's Republic of Korea; or
- g. The Russian Federation (as recognized by the United Nations) or their territories, including territorial waters, or protectorates where they have legal control (legal control shall mean where recognized by the United Nations); or
- h. The Syrian Arab Republic; or
- i. Ukraine; or
- j. The Bolivarian Republic of Venezuela.

Where there is any conflict between the terms of this endorsement and the terms of the **Policy**, the terms of this endorsement shall apply, subject at all times to the application of any Sanctions clause.

If any provision of this endorsement is or at any time becomes to any extent invalid, illegal or unenforceable under any enactment or rule of law, such provision will, to that extent, be deemed not to form part of this endorsement but the validity, legality and enforceability of the remainder of this endorsement will not be affected.

All other terms, conditions and exclusions remain unchanged.

MAN0002 - Mandatory Endorsements

Attaching to and forming part of Policy Number: CY-CP-00013017

Sanction Limitation and Exclusion Clause Endorsement

No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)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 or United States of America.

LMA3100

15/09/10

Insurance Act 2015 - Fraudulent Claims Clause

1) If the Insured makes a fraudulent claim under this insurance contract, the Insurer:

- a) Is not liable to pay the claim; and
- b) May recover from the Insured any sums paid by the Insurer to the Insured in respect of the claim; and
- c) May by notice to the Insured treat the contract as having been terminated with effect from the time of the fraudulent act.

2) If the Insurer exercises its right under clause 1) c) above:

- a) The Insurer shall not be liable to the Insured in respect of a relevant event occurring after the time of the fraudulent act. A relevant event is whatever gives rise to the Insurer's liability under the insurance contract (such as the occurrence of a loss, the making of a claim, or the notification of a potential claim); and
- b) The Insurer need not return any of the premiums paid.

Fraudulent claims – group insurance

3) If this insurance contract provides cover for any person who is not a party to the contract ("a covered person"), and a fraudulent claim is made under the contract by or on behalf of a covered person, the Insurer may exercise the rights set out in clause 1) above as if there were an individual insurance contract between the Insurer and the covered person. However, the exercise of any of those rights shall not affect the cover provided under the contract for any other person.

Nothing in these clauses is intended to vary the position under the Insurance Act 2015.

LMA5256

16 March 2016

Several Liability Notice Insurance

The subscribing insurers' obligations under contracts of insurance to which they subscribe are several and not joint and are limited solely to the extent of their individual subscriptions. The subscribing insurers are not responsible for the subscription of any co-subscribing insurer who for any reason does not satisfy all or part of its obligations.

LSW1001

08/94

Communicable Disease Exclusion (For Use on Liability Policies)

1. Notwithstanding any provision to the contrary within this policy, this policy does not cover all actual or alleged loss, liability, damage, compensation, injury, sickness, disease, death, medical payment, defence cost, cost, expense or any other amount, directly or indirectly and regardless of any other cause contributing concurrently or in any sequence, originating from, caused by, arising out of, contributed to by, resulting from, or otherwise in connection with a Communicable Disease or the fear or threat (whether actual or perceived) of a Communicable Disease.
2. For the purposes of this endorsement, loss, liability, damage, compensation, injury, sickness, disease, death, medical payment, defence cost, cost, expense or any other amount, includes, but is not limited to, any cost to clean-up, detoxify, remove, monitor or test for a Communicable Disease.
3. As used herein, a Communicable Disease means any disease which can be transmitted by means of any substance or agent from any organism to another organism where:
 - 3.1. the substance or agent includes, but is not limited to, a virus, bacterium, parasite or other organism or any variation thereof, whether deemed living or not, and
 - 3.2. the method of transmission, whether direct or indirect, includes but is not limited to, airborne transmission, bodily fluid transmission, transmission from or to any surface or object, solid, liquid or gas or between organisms, and
 - 3.3. the disease, substance or agent can cause or threaten bodily injury, illness, emotional distress, damage to human health, human welfare or property damage.

LMA5396
17/04/2020

All other terms, conditions and exclusions remain unchanged.

INS0001 - Insurer Endorsement

Attaching to and forming part of Policy Number: CY-CP-00013017

The **Policy** is underwritten by certain underwriters at Lloyds's under Binding Authority Reference B0572MR24OS01. The underwriters are as follows:

CNP 4444:	80.000%
CHN 2015:	20.000%

All other terms, conditions and exclusions remain unchanged.

OSR Cyber Insurance



Insurance Product Information Document

This insurance is underwritten by Talbot Underwriting Ltd, and has been arranged and has been administered by Optimum Speciality Risk ("OSR"). OSR is a trading name of Independent Broking Solutions Limited which is authorised and regulated by the Financial Conduct Authority with number 312026. Registered address: 150 Minorities, London, EC3N 1LS. Registered in England No. 616849.

This document provides a summary of the cover, exclusions and restrictions. The full terms and conditions of this insurance can be found in the policy document which is available on request from your broker. Complete pre-contractual information on the product (terms and conditions of this insurance) is provided in other documents.

What is this type of insurance?

This policy will protect your business from cyber-attack and any liabilities that arise due to a breach of privacy legislation, including but not limited to the Data Protection Act and the General Data Protection Regulation (GDPR). Cover is also provided for Media Liability and Payment Card Industry Fines and Penalties. You have direct access to a 24/7/365 helpline in the event of an incident.

 What is insured?	 What is not insured?
<p>Following a Cyber Event (defined as unauthorised access, an operator error, a denial of service attack or the introduction of any malware, including ransomware) into or against your network or any cloud provider with whom you have a written contract:</p> <ul style="list-style-type: none"> ✓ Re-instatement of your data, ✓ Loss of your gross profit caused by the Cyber Event, ✓ A specialist IT forensic company to investigate the cause and scope of the Cyber Event. <p>Following your loss of third party data or a breach of any privacy legislation worldwide (a Data Liability Event) :</p> <ul style="list-style-type: none"> ✓ Defence Costs, we will appoint a specialist law firm to defend you, ✓ A specialist IT forensic company to investigate what data has been compromised, ✓ Costs to notify data subjects if this is required by legislation or considered necessary to protect your reputation, ✓ A Public Relations Company to protect and mitigate any damage to your reputation. <p>In addition, where this data relates to credit or debit card information:</p> <ul style="list-style-type: none"> ✓ Credit monitoring costs for affected individuals, ✓ Any fines and penalties that you are required to pay by the Payment Card Industry as well as Assessment Costs that includes fraudulent transactions for which you are liable. <ul style="list-style-type: none"> ✓ Your legal liability for the transmission of a virus to a third party, or your unknowingly taking part in a denial of service attack. ✓ Your legal liability for accidentally infringing any copyright or trademark, or any defamation, provided always that this liability is incurred in undertaking your usual business practices. ✓ A loss arising from a claim made by a Telecom Provider which arises from any unauthorised access to your internal digital telephony infrastructure. 	<ul style="list-style-type: none"> ✗ Any bodily injury or physical damage. Note that (i) data is not considered to be physical property; (ii) redundant devices as a result of a cyber event are excluded unless the additional Bricking cover is purchased as part of the optional Fund Transfer Fraud/Bricking endorsement). ✗ Any claims or losses about which you were aware but did not tell us before incepting the policy. ✗ Any losses attributable to or based upon any intentional, criminal or fraudulent acts committed or condoned by any Principal, Partner or Director of your business. ✗ Any gross profit loss where the interruption to your network is less than the Waiting Period shown in the schedule. ✗ Any losses caused by the failure of electricity or telecommunications. ✗ Any statutory fines, unless these are considered to be insurable at law. Note this does not apply to Payment Card Industry fines and penalties. ✗ Any losses caused by bankruptcy, insolvency or liquidation of you or your cloud service provider. ✗ Any losses caused by the loss of media without password or biometric protection (including smartphones, tablets and laptops). ✗ Any losses caused by a breach of any anti-Spam legislation anywhere in the world. ✗ Any funds or monies that are transferred to a third party. Unless the optional Fund Transfer Fraud endorsement has been purchased then transfer of funds to an unintended third party on receipt of new, amended or differing instructions.

Optional extension to coverage can be purchased, via the Fund Transfer Fraud and Bricking endorsements, which would also cover:

The reimbursement of financial loss resulting from:

- ✓ Theft or unauthorized transfer of your funds by electronic means.
- ✓ Phishing or social engineering resulting in transfer of your funds to an unintended party.
- ✓ Third party funds held in your account being transferred to an unintended party.
- ✓ Hardware replacement costs as a result of a Cyber Event which renders a computer device redundant ("bricked"), providing they do not exceed the costs to restore functionality for such devices.



Are there any restrictions on cover?

- ! You are responsible for the excess / retention amount (including the waiting period) as shown on your policy documents.
- ! Endorsements may apply to your policy. These will be shown in your policy documents.
- ! Fund Transfer Fraud and Bricking is excluded from the policy, unless purchased as additional coverages



Where am I covered?

- ✓ Your policy will respond to losses anywhere in the world and will also defend you (if necessary) anywhere that an action is taken against you, including the United States and its dependent territories.



What are my obligations?

- Prior to the beginning of the period of insurance or when making changes to your policy, you must give complete and accurate answers to any questions you are asked relating to the insurance.
- You must tell **Optimum Speciality Risks** as soon as practicable if you become aware of any inaccuracies or changes in the information you have provided to us, whether happening before or during the period of insurance.
- In the event of a suspected damage, loss or potential claim you must contact the helpline number given in your policy.
- You must not admit any liability or enter into any settlements without our prior written consent.
- You must co-operate with us, and any counsel that we may appoint.
- You should take all reasonable steps to prevent further loss or damage.
- Failure to meet your obligations could result in a claim being rejected, a reduction in the amount we pay or the cancellation of your policy



When and how do I pay?

- Your broker will advise you of the full details of when and the options by which you can pay.



When does the cover start and end?

- Your period of insurance is given in your policy document and is usually (but not always) of 12 months duration.



How do I cancel the contract?

You may cancel this policy after the fourteen (14) day cooling off period, provided you have not made a claim, you will be entitled to a refund of any premium paid, subject to a deduction for any time for which you have been covered and the administrative cost of providing the insurance.

You may cancel this policy at any time by contacting OSR on +44 (0) 203 675 0910 or at 150 Minories, London, EC3N 1LS or your broker, and such cancellation being effective 10 business days after such notice is received by OSR. In such case, OSR shall refund any unearned premium calculated at pro rata rate of the annual premium, except in the event of a Claim having been notified prior to the date of cancellation whereupon no refund shall be due, unless agreed otherwise by OSR.

This policy may not be cancelled by OSR except for non-payment of the premium, upon expiry of a period of notice of not less than 21 days.



OSR: Cyber Plus

This insurance has been arranged and has been administered by Optimum Speciality Risks ("OSR"). OSR is a trading name of Independent Broking Solutions Limited which is authorised and regulated by the Financial Conduct Authority with number 312026. Registered address: 150 Minorities, London, EC3N 1LS. Registered in England No. 616849.

Contents Page

1. Insurance Cover	3
2. Defined Words	4
3. Exclusions	9
4. General Conditions	9
5. Notice Concerning Personal Information	16
6. Complaints Notice	17

1. Insurance Cover

In consideration of the payment of or agreement to pay the premium by the **Policyholder** on behalf of the **Insured**, the **Insurer** will pay, or where specified, reimburse the **Insured**, in excess of the applicable **Retention**, up to the maximum aggregate limit of liability (both as stated in the Schedule), for:

- 1.1 **Loss of the Insured** in respect of any **Claim** first made against the **Insured** and reported to the **Insurer** during the **Period of Insurance**;
- 1.2 **Business Interruption Loss** resulting from a **Business Interruption Event** commencing on or after the **Retroactive Date** and first discovered and notified by the **Insured** to the **Insurer** during the **Period of Insurance**;
- 1.3 **Remediation Costs** incurred by the **Insured** following an actual or threatened **Business Interruption Event, Data Liability Event** or **Network Security Event** first discovered by the **Insured** and notified to the **Insurer** during the **Period of Insurance**;
- 1.4 **Loss of the Insured** in respect of **PCI Fines and Assessment Costs** caused by a **Data Liability Event** discovered by the **Insured** and reported to the **Insurer** during the **Period of Insurance**.

The cover available under this policy is subject to the operation of Exclusion 3.7 which overrides all other terms of this policy.

2. Defined Words

- 2.1 **Business Interruption Event** means:
- (i) a **Cyber Event** that causes any unplanned system outage, network interruption, or degradation of the **Insured's Computer System**, or the **Computer System** of any **Cloud Service Provider** or
 - (ii) a **Reputational Harm Event**.
- 2.2 **Business Interruption Loss** means the **Insured's** loss of gross profit, plus reasonable expenses necessary to maintain the operation, functionality or service of the **Insured's** business, as a direct result of a **Business Interruption Event**, but only:
- (i) in respect of a **Cyber Event**, after the expiration of the **Waiting Period**, and
 - (ii) until the date on which the **Insured's** business is restored to the same or equivalent trading conditions, functionality and service that existed prior to the loss, however not exceeding 180 days from the date on which the outage, interruption or degradation commenced, such 180 day period not to be limited by the expiration of the Period of Insurance;
- Business Interruption Loss** shall also include costs and expenses incurred to avoid or mitigate the effects of a system outage or network interruption, discover and minimize such interruption or degradation of the network, preserve evidence and/or substantiate the **Insured's** loss.
- 2.3 **Claim** means any written demand, civil, criminal, judicial, administrative, regulatory or arbitral proceeding against the **Insured** seeking compensation or other legal remedy or penalty as a result of a **Data Liability Event**, **Media Liability Event** or **Network Security Event**.
- 2.4 **Cloud Service Provider** means any third party with whom the **Insured** has a written contract for the provision of computing services, infrastructure platforms or business applications. **Cloud Service Provider** does not include any **Social Media Platform**.
- 2.5 **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.
- 2.6 **Credit Monitoring Costs** means reasonable fees, costs and expenses incurred with the prior written consent of the **Insurer** for the monitoring services of identity or credit theft including the purchase of identity theft insurance for a period of 12 months from the date of any **Data Liability Event**.
- 2.7 **Cyber Event** means:
- (i) **Unauthorised Access**;
 - (ii) **Operator Error**;
 - (iii) a denial of service attack;
 - (iv) the introduction of any **Malware** into a **Computer System** owned or operated by an **Insured**, including the **Computer System** of any **Cloud Service Provider**.

- 2.8 **Cyber Extortion Costs** means the reimbursement of reasonable fees, costs and expenses incurred by the **Insured**, or paid on the **Insured's** behalf, with the prior written consent of the **Insurer**, such consent not to be unreasonably withheld, to terminate or mitigate any credible threat of a **Business Interruption Event**, **Data Liability Event** or **Network Security Event** resulting from an actual or attempted extortion by a third party.
- 2.9 **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**.
- 2.10 **Data Liability Event** means:
- (i) the loss or suspected loss of any third-party non-public data or information for which the **Insured** is legally responsible;
 - (ii) the breach of any privacy legislation worldwide by the **Insured** or someone for whom the **Insured** is legally responsible
- provided always that such **Data Liability Event** occurs on or after the **Retroactive Date** specified in the Schedule.
- 2.11 **Data Restoration Costs** means reasonable fees, costs and expenses for the restoration and/or replacement of data and/or programs that have been lost, erased corrupted or encrypted by a **Cyber Event** or **Data Liability Event** and costs to prevent or minimise any further damage and preserve material evidence of civil, criminal or malicious wrongdoings. These costs include the cost of purchasing replacement licenses for programs where necessary.
- 2.12 **Defence Costs** means reasonable fees, costs and expenses (including but not limited to lawyers' fees and experts' fees) incurred by the **Insured** relating to the defence, settlement or appeal of a **Claim**.
- 2.13 **Forensic Costs** means reasonable fees, costs and expenses of the **Insured** to investigate the cause, scope and extent of any **Data Liability Event**, **Business Interruption Event** or **Network Security Event**.
- 2.14 **Insured** means the **Policyholder**, as set out in the Schedule, and any subsidiary domiciled in the same territory and owned by the **Policyholder** that is intended and agreed to be insured by the **Insurer** at inception and/or acquired subsequent to inception provided notice is given to the **Insurer** of such acquisition and the **Insurer** has not objected within 30 days of such notice.
- 2.15 **Insurer** means Underwriters at Lloyd's, as set out in the Schedule
- 2.16 **Legal Representation Expenses** means reasonable and necessary fees, costs and expenses incurred to obtain legal advice or representation to protect the **Insured's** interests in connection with a **Data Liability Event** or **Network Security Event**.

Legal Representation Expenses shall include the costs associated with the investigation, adjustment and defence of regulatory proceedings.

2.17 **Loss** means judgments, settlements, awards, and costs, including, without limitation, damages, consumer redress funds, fines, penalties and punitive and exemplary damages in respect of a **Claim** covered under this policy to the extent permitted by law. **Loss** shall also include **Defence Costs** and **Legal Representation Expenses**.

2.18 **Malware** means any code designed to:

- (i) erase, deny access to or corrupt data, including but not limited to ransomware;
- (ii) damage or disrupt any **Computer System**;
- (iii) circumvent any network security product or service.

2.19 **Media Liability Event** means any digital content or printed media created and displayed by the Insured directly leading to

- (i) an infringement of any copyright, title, slogan, trademark, trade name, or domain name;
- (ii) plagiarism, piracy, or the misappropriation or theft of ideas
- (iii) defamation, including the disparagement of any product or service
- (iv) any breach of confidentiality or invasion or interference with any right of privacy

provided always that such **Media Liability Event** occurs in the course of the **Insured's** usual business practices and that such **Media Liability Event** occurs on or after the **Retroactive Date** specified in the Schedule. For the avoidance of doubt the manufacture, supply, retail or distribution of any tangible goods or products shall not be considered a **Media Liability Event**.

2.20 **Merchant Services Agreement** means a contractual agreement between the **Insured** and any other organisation which allows the Insured to accept payment by credit or debit card.

2.21 **Network Security Event** means:

- (i) the transmission of any **Malware** from the **Insured's Computer System**, or from the **Computer System** of any **Cloud Service Provider**;
- (ii) failure to secure the **Insured's Computer System** that results in **Unauthorised Access**;
- (iii) failure to prevent a denial of service attack launched from the **Insured's Computer System** or from the **Computer System** of any **Cloud Service Provider**,

provided always that such **Network Security Event** occurs on or after the **Retroactive Date** and notified to the **Insurer** by the **Insured** during the **Period of Insurance** specified in the Schedule.

2.22 **Notification Costs** means reasonable fees, costs and expenses in respect of notifying any natural person or legal entity whose data or information has been or may have been lost, or the cost of notifying any data protection authority or equivalent, as a result of a **Data Liability Event**.

2.23 **Operator Error** means the accidental erasure, destruction or modification of the **Insured's** data or programs by an employee or a **Cloud Service Provider**.

2.24 **PCI Fines and Assessment Costs** means all amounts that the Insured is legally required to pay under a **Merchant Services Agreement** following a **Data Liability Event** that leads to a

breach of the Payment Card Industry Data Security Standard, including but not limited to fines, case management fees, non-compliance fees, re-imbusement of fraudulent transactions, and the costs incurred in card re-issuance and the appointment of a PCI Forensic Investigator.

- 2.25 **Period of Insurance** means the period stated as such in the Schedule.
- 2.26 **Policyholder** means the entity stated as such in the Schedule.
- 2.27 **Public Relations Costs** means reasonable fees, costs and expenses incurred with the prior written consent of the **Insurer**, such consent not to be unreasonably withheld, for obtaining advice and support to protect, or mitigate any damage to, the **Insured's** reputation following a **Reputational Harm Event**.
- 2.28 **Remediation Costs** means any:
- (i) **Credit Monitoring Costs;**
 - (ii) **Cyber Extortion Costs;**
 - (iii) **Data Restoration Costs;**
 - (iv) **Forensic Costs;**
 - (v) **Legal Representation Expenses;**
 - (vi) **Notification Costs;** and
 - (vii) **Public Relations Costs.**
- 2.29 **Reputational Harm Event** means adverse media, including social media, caused solely by a **Cyber Event** or a **Data Liability Event** that directly leads to a **Business Interruption Loss**.
- 2.30 **Retention** means the amount stated in the Schedule that the **Insured** must pay as the first part of each and every claim for indemnity under this policy after application of all other terms and conditions of this policy
- 2.31 **Retroactive Date** means the date stated as such in the Schedule.
- 2.32 **Social Media Platform** means any internet based system for the creation, exchange or sharing of any user generated content for information, advertising or any other purpose. **Social Media Platforms** include, but are not limited to: Facebook, LinkedIn, Instagram, Twitter and YouTube.
- 2.33 **State** means sovereign state.
- 2.34 **Unauthorised Access** means use of the **Insured's Computer System** by any person or persons not authorised to do so, including employees.
- 2.35 **Waiting Period** means the number of hours stated in the Schedule which must elapse following a **Business Interruption Event** before a **Business Interruption Loss** is agreed to have occurred. The **Waiting Period** will apply to each **Business Interruption Event**. For the avoidance of doubt, once the **Waiting Period** is satisfied only the monetary Retention will apply to **Business Interruption Loss(es)**.
- 2.36 **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 nationalisation or requisition or destruction of damage to property by or under the order of any government or public or local authority,

whether **War** be declared or not.

3. Exclusions

The **Insurer** shall not be liable to make any payment or provide any benefit or service in respect of any **Claim, Loss**, damage, liability, cost or expense of any kind:

- 3.1 for death, bodily injury or loss of or damage to tangible property, however this exclusion shall not apply to mental anguish or mental injury as a result of a **Data Liability Event** or **Network Security Event**. For the avoidance of doubt data held in electronic format is not tangible property.
- 3.2 arising from, attributable to, or based upon any fact or circumstance known to the **Insured** prior to the inception of the **Period of Insurance**.
- 3.3 arising from, attributable to or based upon any intentional, criminal or fraudulent acts committed or condoned by any Principal, Partner or Director of the **Insured**.
- 3.4 arising from any failure, outage, or disruption of power, utility services, satellites, internet service provider (including any provider of internet connectivity), or telecommunications external services not under the direct operational control of the **Insured**.
- 3.5 arising from directly or indirectly occasioned by, happening through or in consequence of **War** or a **Cyber Operation**. The **Insurer** shall have the burden of proving this exclusion applies.

Attribution of a **Cyber Operation** to a **State** shall be determined as follows:

- 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** of 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.

- 3.6 arising from any bankruptcy, liquidation or insolvency of the **Insured** or any other person, including any **Cloud Service Provider**.

- 3.7 to the extent that such cover, payment, service, benefit and/or any business or activity of the **Insured** from which the **Claim** or **Loss** arises would violate any applicable trade or economic sanctions or any law or any regulation worldwide.
- 3.8 arising from or representing the costs for the upgrading or betterment of any application or **Computer System** of the **Insured**.
- 3.9
- a) brought against a director or officer of the **Insured**, in their capacity as such
 - b) arising from any obligation owed by the **Insured** as an employer or potential employer to any employee, including claims for wrongful dismissal or under any contract of employment or under any retainer with any consultant or under any training contract or work experience placement;
 - c) whether by any employee or not, alleging sexual, racial or other harassment or molestation, or sexual, racial, ethnic, disability, sexual orientation, religious and/or age discrimination or victimisation, or discrimination or victimisation of any other kind.
- 3.10
- a) directly or indirectly, arising out of, or resulting from, asbestos or any actual or alleged asbestos related loss injury or damage involving the use, presence, existence, detection, removal, elimination or avoidance of asbestos or exposure to asbestos;
 - b) arising from, based upon, attributable to or as a consequence of, whether direct or indirect, or in any way involving:
 - (i) ionising radiation or contamination by radioactivity or from any nuclear fuel or from any nuclear waste;
 - (ii) the radioactive, toxic, explosive or other hazardous properties of any nuclear assembly or component thereof.
 - c) arising out of, based upon, attributable to, as a consequence or in any way involving, pollution or directly or indirectly the actual, alleged or threatened discharge, dispersal, release or escape of pollutants;
 - d) arising from, based upon, attributable to or as a consequence of any electromagnetic field, electromagnetic radiation or electromagnetism, which terms are defined as follows:
 - (i) electromagnetic field means any field of force that is made up of associated electric and magnetic components;
 - (ii) electromagnetic radiation means any succession of electromagnetic waves;
 - (iii) electromagnetism means magnetism that is developed by a current of electricity.
- 3.11 arising from any fire, lightning, explosion, aircraft, impact or any other natural peril.

- 3.12 arising out of any violation of anti-Spam or telemarketing legislation worldwide.
- 3.13 arising out of the electronic transfer of any funds, monies or goods belonging to the **Insured**, or for which the **Insured** is legally liable, unless the funds transfer fraud coverage is purchased by way of endorsement.
- 3.14 arising from any contractual liability assumed by the **Insured**, unless such liability would have attached in the absence of such contract. This exclusion shall not apply to Insurance Cover 1.4.
- 3.15 arising out of the misappropriation or infringement of patent or trade secret.
- 3.16 arising out of the actual or alleged failure to render any professional services.

4. General Conditions

Limit of Indemnity

- 4.1 The limit of liability shown in the Schedule is the maximum amount the **Insurer** will pay, including **Defence Costs**, irrespective of the number of claims submitted under the policy by the **Insured**.
- 4.2 The **Insurer** may, in its sole discretion, elect to discharge its liability to the **Insured** fully and finally in respect of any **Claim(s)** covered under this policy by either (a) paying the applicable limit of indemnity (less any sums previously paid) to the **Insured** or (b) paying a sum less than the limit of indemnity when the **Claim(s)** can be settled for such a lesser sum.
- 4.3 If a **Claim** is settled by a payment to a third party and such payment is not 100% insured under this policy, the **Insurer** will be liable for no more than a proportionate share of the **Defence Costs** based on the insured proportion of such payment (and, for the avoidance of doubt, the **Insurer's** liability is always subject to the limit of liability, inclusive of **Defence Costs**, per clause 4.1 above).

Related Claims

- 4.4 Any **Claims** or **Losses** under all applicable sections of this policy, directly or indirectly arising out of or in any way connected with the same originating cause or event, will be deemed to be a single claim, reported at the date of the first such claim. Any **Claims** or **Losses** under all applicable sections of this policy, triggering more than one coverage section, will be deemed to be a single claim.

Claims Handling and Notification

- 4.5 It is a condition precedent to the **Insurer's** liability that the **Insured** complies with each of the provisions of this clause 4.5. If the **Insured** fails to do so, the **Insurer** may (a) reject any claim for an indemnity under this policy; or, at its absolute discretion (b) elect to indemnify the **Insured** to the extent the **Insurer** would have been liable to pay in the absence of any prejudice in the handling or settlement of any **Claim** or notifiable circumstance under this policy which arises from the **Insured's** breach of condition precedent:
 - 4.5.1. The **Insured** shall notify any **Claim**, **Loss**, or **Business Interruption Event** to the agreed incident response provider specified in the Schedule, as soon as reasonably practicable, but in no case later than 7 (seven) days after the **Insured** has become aware of such incident. The **Insured** shall provide such information and documentation relating to the **Claim**, or **Loss** as the **Insurer** may require in its sole discretion.
 - 4.5.2 The **Insured** may give notice to the **Insurer** during the Period of Insurance of circumstances which may reasonably be expected to give rise to a **Claim**, specifying the reasons for anticipating such a **Claim**. If such notice is given, any **Claim** subsequently made against the **Insured** alleging, arising out of or in any way connected with such circumstances shall be deemed to have been made at the time such notice of circumstances was given by the **Insured** to the **Insurer**. The **Insured** shall provide such information and documentation relating to the notification as the **Insurer** may require in its sole discretion.

- 4.5.3 No **Insured** shall (expressly or impliedly) admit nor assume any liability, make a compromise, enter into any settlement agreement, waive any rights nor consent to any judgment in respect of any **Claim, Loss** or notifiable circumstances without the prior written consent of the **Insurer**, such consent not to be unreasonably withheld or delayed.
- 4.5.4 The **Insured** shall co-operate with the **Insurer**, including but not limited to any counsel, advisor or specialist incident response provider that the Insurer shall appoint to investigate any **Claim** and shall provide all such information and documents as the **Insurer** shall require in its sole discretion.

Incident Response Panel

- 4.6 The **Insurer** has the right to appoint any counsel, advisor, specialist incident response provider or other provider to investigate or assist the **Insured** with any **Claim, Cyber Event, Data Liability Event, Media Liability Event** or **Network Security Event**. The **Insured** shall co-operate with the **Insurer** and any counsel, advisor, specialist incident response provider or other provider to investigate or assist the **Insured**. The **Insured** must not under any circumstances appoint its own counsel, advisor, specialist incident response provider or other provider to investigate or assist the **Insured** with any **Claim, Cyber Event, Data Liability Event, Media Liability Event** or **Network Security Event**.

Defence Costs and Legal Representation Expenses

- 4.7 Subject to the **Insured's** compliance with the provisions of paragraph 4.5 the **Limit of Liability** and **Retention** set out in the Schedule to this policy, the **Insurer** agrees to advance **Defence Costs** on an on-going basis and prior to the final position of a **Claim**. **Insured** agrees to refund all such **Defence Costs** should it be found that the **Claim** is not valid.

Change of Control

- 4.8 If during the **Period of Insurance** any person, group or entity acquires control of more than 50% of the issued share capital of the **Policyholder** or of the composition of the board of the **Policyholder**, the cover provided by this policy shall be restricted so as to apply only to **Claims** in respect of **Business Interruption Events, Data Liability Events** or **Network Security Events** occurring prior to the effective date of such sale, consolidation, merger or acquisition of control, unless the Insurer has agreed to extend coverage under the policy and the **Policyholder** has agreed to the terms of any such extension of coverage.

Assignment

- 4.9 This policy and any rights under it cannot be assigned without the prior written consent of the **Insurer**.

Cancellation

- 4.10 The **Policyholder** may cancel this policy at any time by giving written notice to the **Insurer** and such cancellation being effective 10 business days after such notice is received by the **Insurer**. In such case, the **Insurer** shall refund any unearned premium calculated at pro rata rate of the annual premium, except in the event of a **Claim** as defined in this policy having been notified prior to the date of cancellation whereupon no refund shall be due, unless agreed otherwise by the **Insurer**.

This policy may not be cancelled by the **Insurer** except for non-payment of the premium, upon expiry of a period of notice of not less than 21 days.

Applicable Law

- 4.11 This agreement and any dispute or claim between the **Insured** and the **Insurer** arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws set out in the Schedule. If any term of this agreement is to any extent invalid, illegal, or incapable of being enforced, such term shall be excluded to the extent of such invalidity, illegality, or unenforceability and all other terms of this agreement shall remain in full force and effect.

Arbitration

- 4.12 All disputes arising out of or in connection with this agreement, or in respect of any legal relationship associated with or derived from this agreement, shall be resolved by arbitration. The seat of the arbitration will be as specified in the Schedule.

Duty of Fair Presentation

- 4.13 Before this insurance contract (or any variation thereto) is entered into, the **Insured** must make a fair presentation of the risk to the **Insurer** in any application, proposal form or other information submitted to the **Insurer**. This means the **Insured** must:
- 4.13.1 disclose to the **Insurer** (i) every material circumstance which the **Insured** knows or ought to know or (ii) sufficient information to put a prudent insurer on notice that it needs to make further enquiries in order to reveal material circumstances. A matter is material if it would influence the judgement of a prudent insurer as to whether to accept the risk, or the terms of the insurance (including premium); and
 - 4.13.2 make the disclosure in clause 4.13.1 above in a reasonably clear and accessible way; and
 - 4.13.3 ensure that every material representation of fact is substantially correct, and that every material representation of expectation or belief is made in good faith.
- 4.14 If the **Insured** fails to comply with clause 4.13, the **Insurer** has the following remedies:
- 4.14.1 If the **Insured's** breach of the duty of fair presentation is deliberate or reckless, then (i) the **Insurer** may avoid the policy, and refuse to pay all claims; and (ii) the **Insurer** need not return any of the premiums paid.
 - 4.14.2 If the **Insured's** breach of the duty of fair presentation is not deliberate or reckless, then the **Insurer's** remedy will depend on what the **Insurer** would have done if the **Insured** had complied with the duty of fair presentation:
 - 4.14.2.1 If the **Insurer** would not have entered into the contract at all, the **Insurer** may avoid the contract and refuse all claims, but must return the premiums paid.
 - 4.14.2.2 If the **Insurer** would have entered into the contract, but on different terms (other than terms relating to the premium), the contract is to be treated as if it had

been entered into on those different terms from the outset, if the Insurer so requires.

4.14.2.3 If the **Insurer** would have entered into the contract, but would have charged a higher premium, the Insurer may reduce proportionately the amount to be paid on a claim (and, if applicable, the amount already paid on prior claims).

Indemnity and Settlement

- 4.15 The **Insurer** has the right but not the duty to assume control, defence and settlement of any **Claim** or investigation. At any stage of a **Claim** the **Insurer** may choose to pay the **Limit of Liability** or any amount that remains following any earlier payment(s).
- 4.16 The **Insurer** shall have the right to make an investigation it deems necessary including, without limitation, any investigation with respect to the Application and statements made in connection with the procurement of the policy and with respect to coverage.
- 4.17 With respect to any **Claim**, if the Insured refuses to consent to a settlement the **Insurer** recommends and the claimant will accept, the **Insured** may continue the defence and investigation of that **Claim**. However, the further costs and expenses incurred will be paid by the **Insured** and the **Insurer** on a proportional basis, with 25% payable by the **Insurer** and 75% payable by the **Insured**.

Subrogation

- 4.18 If the **Insurer** makes any payment under this Policy and there is available to the **Insurer** any of the **Insured's** rights of recovery against any third party, then the **Insurer** shall maintain all such rights of recovery. The **Insured** shall execute and deliver instruments and papers and do whatever else is necessary to secure such rights. This includes, but is not limited to, placing any third party on notice of any rights the **Insured** or the **Insurer** may have against it. The **Insured** shall do nothing to prejudice such rights. Any recoveries shall be first applied to subrogation expenses, second to any amounts paid or reimbursed by the **Insurer** under the Policy, and third to the Retention set out in Schedule. Any additional amounts shall be paid to the **Insured**.

5. Notice Concerning Personal Information

Personal Information

Your insurance cover includes cover for individuals who are either insureds or beneficiaries under the policy (individual insureds). We (the Lloyd's underwriter(s) identified in the contract of insurance), being Talbot Underwriting Limited, and other insurance market participants collect and use relevant information about individual insureds to provide you with your insurance cover and to meet our legal obligations.

This information includes individual insured's details such as their name, address and contact details and any other information that we collect about them in connection with your insurance cover. This information may include more sensitive details such as information about their health and criminal convictions.

We will process individual insureds' details, as well as any other personal information you provide to us in respect of your insurance cover, in accordance with our privacy notice(s) and applicable data protection laws.

Information notices

To enable us to use individual insureds' details in accordance with applicable data protection laws, we need you to provide those individuals with certain information about how we will use their details in connection with your insurance cover.

You agree to provide to each individual insured our short form information notice, which we have provided to you in connection with your insurance cover, on or before the date that the individual becomes an individual insured under your insurance cover or, if earlier, the date that you first provide information about the individual to us.

Minimisation and notification

We are committed to using only the personal information we need to provide you with your insurance cover. To help us achieve this, you should only provide to us information about individual insureds that we ask for from time to time.

You must promptly notify us if an individual insured, contacts you about how we use their personal details in relation to your insurance cover so that we can deal with their queries.

LMA9154

Further information about Lloyd's personal information protection policy may be obtained from your broker or by contacting Lloyd's on +44 (0)207 327 5933

6. Complaints Notice

Complaints

If you wish to make a complaint, please contact:

Complaints
Talbot Underwriting Ltd
60 Threadneedle Street
London
EC2R 8HP

Email: complaints@talbotuw.com
Tel: +44 (0)20 7550 3500
Fax: +44 (0)20 7550 3555

In the event that you remain dissatisfied, it may be possible in certain circumstances for you to refer the matter to the Complaints team at Lloyd's.

The address of the Complaints team at Lloyd's is:

Fidentia House
Walter Burke Way
Chatham Maritime
Chatham
Kent
ME4 4RN

Email: complaints@lloyds.com
Tel: +44 (0)20 7327 5693
Website: www.lloyds.com/complaints

Details of Lloyd's complaints procedures are set out in a leaflet "Your Complaint - How We Can Help" available at www.lloyds.com/complaints and are also available from the above address.

If you remain dissatisfied after Lloyd's has considered your complaint, you may have the right to refer your complaint to the Financial Ombudsman Service (FOS).

The contact details for the FOS are: The Financial Ombudsman Service, Exchange Tower, London E14 9SR. Telephone 0800 023 4567 (calls to this number are free from "fixed lines" in the UK) or 0300 123 9123 (calls to this number are charged at the same rate as 01 and 02 numbers on mobile phone tariffs in the UK). Email complaint.info@financial-ombudsman.org.uk.

The FOS is an independent service in the UK for settling disputes between consumers and businesses providing financial services. You can find more information on the FOS at www.financial-ombudsman.org.uk.

LMA9124

