



Rupert Hills
The Military Mutual
54 Fenchurch Street
London
EC3M 3JY

New Dawn Risk Group Limited
106 Leadenhall Street
London, EC3A 4AA
United Kingdom
Tel: +44 20 3668 2800
www.newdawnrisk.com

7th December 2021

Our reference: B1636U210060

Royal Engineers Association
Cyber Liability Insurance

Dear Rupert,

Please find attached the policy document relating to the recent placement of Cyber Liability Insurance for the Royal Engineers Association.

Please read this carefully and contact us as soon as possible with any questions you may have.

Many thanks for your support on this account; we look forward to working with you again soon.

Yours sincerely,

Tom Malcolm
Manager

Max Carter
Director



Policy Schedule

POLICY REFERENCE:	6666983
BINDING AUTHORITY REFERENCE:	B1179I268021000
THE POLICYHOLDER:	Royal Engineers Association
PRINCIPAL ADDRESS:	HQ Royal Engineers Chatham ME4 4UG
THE INSURER:	Underwritten by certain underwriters at Lloyd's'
BUSINESS:	Charity
BROKER:	New Dawn Risk Group Limited
TURNOVER:	£1,000,001 - £1,500,000
DATE OF PROPOSAL FORM:	03 November 2021
PERIOD OF INSURANCE:	FROM: 03 December 2021 TO: 02 December 2022 Both days inclusive Local Standard Time at the Policyholder's Principal Address stated above in this Schedule
LIMIT OF LIABILITY:	£1,000,000 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
RETENTION:	Retention each and every Cyber Event : £500 Save that:- In respect of cover under Clause 1.2 the Waiting Period is 8 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
PREMIUM:	£909.50
INSURANCE PREMIUM TAX:	£109.14
POLICY FEE:	£50.00
TOTAL:	£1,068.64
POLICY WORDING:	Optimum Cyber Plus v3.1
RETROACTIVE DATE:	03 December 2019
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
TERRITORY:	Worldwide
SEAT OF ARBITRATION:	England and Wales
INCIDENT RESPONSE PROVIDER (NOTIFICATION OF CLAIMS):	Crawford & Company – 0800 279 4214

INCLUDING THE FOLLOWING ADD ON COVERS ENDORSEMENTS:

	Limit:	Deductible:
Fund Transfer Fraud	£50,000	£500
Bricking	£50,000	£500

ENDORSEMENTS:

Please refer to the endorsement library contained within the policy wording for the full text of the endorsement were only the title is shown.

BRICKING INCIDENTS ENDORSEMENT

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.

CL370: INSTITUTE RADIOACTIVE CONTAMINATION, CHEMICAL, BIOLOGICAL, BIO-CHEMICAL AND ELECTROMAGNETIC WEAPONS EXCLUSION CLAUSE

FTF: FUNDS TRANSFER FRAUD/THEFT OF THIRD PARTY FUNDS ENDORSEMENT

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:	03 December 2020
Retention each and every Fund Transfer Fraud and/or Third Party Escrow Theft Event :	£500
Maximum aggregate sum the Insurer will pay in respect of any and all Funds Transfer Fraud(s) and / or Third Party Escrow Theft(s) under the Policy :	£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 COVERS

The following provisions are 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

Optimum Speciality Risks 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: Unit 2 Kildegaard Business Park, Easthorpe Road, Easthorpe, Colchester, Essex, CO5 9HE.
Registered in England and Wales No: 616849

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 means the commission by any **Third Party** of:

- i. via **Unauthorised Access** leading to any unauthorised electronic transfer of the **Insured's** funds from the **Insured's** computer system or network due to the fraudulent manipulation of electronic documentation which is stored on the **Insured's** computer system;
- ii. of theft of money or other financial assets from the **Insured's** corporate credit cards by electronic means; and / or
- iii. of any phishing, vishing or other social engineering attack against the **Insured** that results in the unauthorised transfer of the **Insured's** funds 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**.

All other terms and conditions of the **Policy** remain unchanged

LMA3100: SANCTION LIMITATION AND EXCLUSION CLAUSE

LSW1001: SEVERAL LIABILITY NOTICE INSURANCE

NMA464: WAR AND CIVIL WAR EXCLUSION CLAUSE

TELEPHONE HACKING NEW: TELEPHONE HACKING ENDORSEMENT

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

SCHEDULE

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

TELEPHONE HACKING COVER

Inception date applicable to any Telephone Hacking Event :	03 December 2020
Retention each and every Telephone Hacking Event :	£500
Maximum aggregate sum the Insurer will pay in respect of any and all Telephone Hacking Events :	£1,000,000

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 and conditions of the **Policy** remain unchanged.

Signed by and on behalf of Optimum Speciality Risks:



Freddy Knight
Optimum Speciality Risks
150 Minories,
London,
EC3N 1LS

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.

Lloyd's Cyber Insurance



Insurance Product Information Document

This insurance is underwritten by certain underwriters at Lloyd's, 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: Unit 2 Kildegard Business Park, Easthorpe, Road, Easthorpe, Colchester, Essex CO5 9HE. 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.

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 Act (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"> ✗ Any bodily injury or physical damage. Note that (i) data is not considered to be physical property; (ii) bricked devices as a result of a cyber event are excluded unless the Bricking cover is purchased as part of the 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. ✗ Any losses caused by bankruptcy, insolvency or liquidation of you or any 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. If the Fund Transfer Fraud endorsement has been purchased then transfer of funds to an unintended third party

- ✓ 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.

Optional extension to coverage via the Fund Transfer Fraud and Bricking and Telephone Hacking endorsements 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 non-functional, providing they do not exceed the costs to restore functionality for such devices.
- ✓ A loss arising from a claim made by a Telcom Provider which arises from any unauthorised access to your internal digital telephony infrastructure.

on receipt of new, amended or differing instructions where you have not authenticated would not be covered, so where you have not: (1) called the telephone number held on file for the third party; (2) received oral confirmation from the third party that the transfer request is valid



Are there any restrictions on cover?

- ! You are responsible for the excess amount 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?

- You must maintain a commercial grade (not Home Edition) firewall, either hardware or software based.
- You must run and maintain a commercial grade (not Home Edition) anti-virus solution.
- You must backup all critical data at least every 7 days.
- You must password or biometrically protect all portable media, including smartphones and memory sticks, otherwise losses originating from portable media will not be covered.
- If you process Payment Card Information, you must be fully PCI DSS compliant.
- At 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 loss or 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 the policy document and is usually (but not always) of 12 months duration.



How do I cancel the contract?

You may cancel this insurance 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.



Optimum Cyber Plus Policy Document

This insurance 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: Unit 2 Kildegard Business Park, Easthorpe, Road, Easthorpe, Colchester, Essex CO5 9HE. Registered in England No. 616849.

Optimum Cyber Plus v3.1

01

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**:

- 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 discovered 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 reported 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**.

02

General definitions

2.1 **Business Interruption Event** means:

- (i) a **Cyber Event** that causes any unplanned system outage, network interruption, or degradation of the **Insured's** network, or the network 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.

2.5 **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**.

- 2.6 **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.
- 2.7 **Cyber Event** means:
- (i) **Unauthorised Access**;
 - (ii) **Operator Error**;
 - (iii) a denial of service attack;
 - (iv) the introduction of any **Malware** into a network owned or operated by an **Insured**, including the network of any **Cloud Service Provider**,
- 2.8 **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.
- 2.9 **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.
- 2.10 **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**.
- 2.11 **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**.
- 2.12 **Insured** means the **Policyholder**, and any subsidiary 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.

2.13 **Insurer** means Talbot Syndicate #1183.



2.14 **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.

2.15 **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**.

2.16 **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 network or system;
- (iii) circumvent any network security product or service.

2.17 **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**.

2.18 **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.

2.19 **Network Security Event** means:

- (i) the transmission of any **Malware** from the **Insured's** network, or from the network of any **Cloud Service Provider**;
- (ii) failure to secure the Insured's computer system or network that results in **Unauthorised Access**;

- (iii) failure to prevent a denial of service attack launched from the **Insured's** network or from the network of any **Cloud Service Provider**, provided always that such **Network Security Event** occurs on or after the **Retroactive Date** specified in the schedule.

2.20 **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**.

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

2.22 **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-imbbursement of fraudulent transactions, and the costs incurred in card re-issuance and the appointment of a PCI Forensic Investigator.

2.23 **Period of Insurance** means the period denoted as such in the Schedule.

2.24 **Policyholder** means the entity denoted as such in the Schedule.

2.25 **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**.

2.26 **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.**

- 2.27 **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**.
- 2.28 **Retention** means the amount 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
- 2.29 **Retroactive Date** means the date denoted as such in the Schedule.
- 2.30 **Unauthorised Access** means use of the **Insured's** computer system or network infrastructure by any person or persons not authorised to do so, including employees.
- 2.31 **Waiting Period** means the number of hours denoted as such 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 Losses.

03

Exclusions

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

- 3.1 for death, bodily injury or loss of or damage to tangible property including bricked devices unless purchased via endorsement, 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, or telecommunications external services not under the direct operational control of the **Insured**.
- 3.5 arising from any physical act of war, invasion, or warlike operations, civil war, riot, civil commotion, rebellion, revolution, insurrection or civil uprising.
- 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. This provision overrides all other terms of this policy.
- 3.8 arising from or representing the costs for the upgrading or betterment of any application, system or network 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 Fraud Transfer Fraud and Bricking endorsement has been purchased which provides additional coverage for reimbursement of financial loss resulting from:

- (i) Theft or unauthorized transfer of your (the **Insured's**) funds by electronic means from your (the **Insured's**) computer or network.
- (ii) Phishing or social engineering resulting in transfer of your funds to an unintended party.
- (iii) Third party funds held in your account being transferred to an unintended party.

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 Insuring 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.

04

General conditions

Limit of liability

- 4.1 The limit of liability denoted as such in the Schedule is the maximum amount the **Insurer** will pay, including **Defence Costs**, irrespective of the number of policy claims.
- 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 as detailed in item 8 of 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, Loss, or Business Interruption Event** 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** or **Business Interruption Event**, and shall provide all such information and documents as the **Insurer** shall require in its sole discretion.

Defence Costs And Legal Representation Expenses

- 4.6 Subject to the **Insured's** compliance with the provisions of paragraphs 4.3, 4.4 and 4.5 and to 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 disposition of a **Claim**. **Insured** agrees to refund all such **Defence Costs** should it be found that the **Claim** is not valid.

Change Of Control

- 4.7 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

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

Cancellation

- 4.9 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 under 4.1 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

- 4.10 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.

Mediation And Arbitration

- 4.11 All disputes arising out of or in connection with this agreement, which remain unresolved after 90 days will be referred by written notice from either party to the other to a mediator acceptable to both parties (or one nominated by CEDR if a mediator cannot be agreed within 7 days of the written notice). The mediation shall take place within 28 days of the written notice and in the seat of arbitration specified in the Schedule. If no agreement is reached at mediation the parties agree that either party may by written notice to the other refer the dispute to arbitration in London in English under the rules then in force of the London Court of International Arbitration before a sole arbitrator acceptable to both parties (or one nominated by the LCIA if an arbitrator cannot be agreed within 7 days of the written notice).

Duty Of Fair Presentation

4.12 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:

4.12.1 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

4.12.2 make the disclosure in clause 4.12.1 above in a reasonably clear and accessible way; and

4.12.3 ensure that every material representation of fact is substantially correct, and that every material representation of expectation or belief is made in good faith.

4.13 If the **Insured** fails to comply with clause 4.12, the **Insurer** has the following remedies:

4.13.1 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.

4.13.2 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:

4.13.2.1 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.

4.13.2.2 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.

4.13.2.3 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

- 4.14 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).
- 4.15 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.
- 4.16 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**.

Use Of Firewall, Anti-Virus, Back Up Of Data And Pci Compliance

- 4.17 The **Insured** warrants as follows:
- 4.17.1 The **Insured** will deploy and maintain commercial grade anti-virus and firewall across the **Insured's** network.
- 4.17.2 The **Insured**, or the **Insured's Cloud Service Provider**, will back-up critical data at least every 7 days. Where such data is copied to portable media, such portable media will be secured off-site.
- 4.17.3 The **Insurer's** liability for a **Loss**, suffered by the **Insured** under insuring clause 1.4 (**PCI Fines and Assessment Costs**), is conditional on the **Insured** being compliant with the relevant Payment Card Industry Data Security Standard in relation to all circumstances leading up to the **Loss**.

4.18 If the **Insured** breaches any warranty under clause 4.17, the **Insurer's** liability under this policy shall be suspended from the time of the breach until the time when the breach is remedied (if it is capable of being remedied). The **Insurer** will have no liability to the **Insured** for any loss which occurs, or which is attributable to something happening, during the period when the **Insurer's** liability is suspended. If the **Insured's** breach of warranty leads to prejudice to the **Insurer**, the **Insurer** may at its absolute discretion elect instead to indemnify the **Insured** to the extent the **Insurer** would have been liable to pay in the absence of such prejudice, notwithstanding any suspension of cover.

Subrogation

4.19 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**.

Use Of Password & Biometric Security On Portable Devices & Equipment

4.20 The **Insured** shall take all reasonable precautions to ensure that all portable media including, but not limited to Laptops, Smart phones, tables and memory sticks are password or biometrically protected at all times.

4.21 As soon as reasonably practicable, after discovery that password or biometric protection has been disabled on any portable media device, take necessary steps to reinstate the security to the device.

Endorsement Library

Telephone Hacking Endorsement

The following provisions are inserted:

NEW CLAUSE AT 1. INSURANCE COVER

“TELEPHONE HACKING COVER

Retroactive date applicable to any **Telephone Hacking Event**: As per main cover

Retention each and every **Telephone Hacking Event**: As per main cover

Maximum sum the **Insurer** will pay in respect of each and every **Telephone Hacking Event**: As per main limit of liability

Maximum aggregate sum the **Insurer** will pay in respect of any and all **Telephone Hacking Events**: As per main limit of liability

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

In consideration of the payment of or agreement to pay the premium by the **Policyholder** on behalf of the **Insured**, the **Insurer** will pay, in excess of the applicable **Retention**, and up to the maximum sums set out above, the **Insurer** will indemnify the **Insured** in respect of any **Loss** arising from a **Claim** against the **Insured** made by a **Telcom Provider** which (i) results from a **Telephone Hacking Event** and (ii) is validly notified to the **Insurer** during the **Period of Insurance** in compliance with policy terms.

NEW CLAUSES AT 2. GENERAL DEFINITIONS

“**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.”

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

“or **Telephone Hacking Event** (where that written demand, civil, criminal, judicial, administrative, regulatory or arbitral proceeding is made by a **Telcom Provider**).”

All other terms and conditions to remain unchanged.

Institute Radioactive Contamination, Chemical, Biological, Bio-Chemical And Electromagnetic Weapons Exclusion Clause

This clause shall be paramount and shall override anything contained in this insurance inconsistent therewith.

1. In no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from:
 - 1.1 ionising radiations from or contamination by radioactivity from any nuclear fuel or from any nuclear waste or from the combustion of nuclear fuel.
 - 1.2 the radioactive toxic explosive or other hazardous or contaminating properties of any nuclear installation, reactor or other nuclear assembly or nuclear component thereof.
 - 1.3 any weapon or device employing atomic or nuclear fission and/or fusion or other like reaction or radioactive force or matter.
 - 1.4 the radioactive, toxic, explosive or other hazardous or contamination properties of any radioactive matter. The exclusion in this sub-clause does not extend to radioactive isotopes, other than nuclear fuel, when such isotopes are being prepared, carried, stored, or used for commercial, agricultural, medical, scientific or other similar peaceful purposes.
 - 1.5 any chemical, biological, bio-chemical, or electromagnetic weapon.

CL370

10/11/2003

Sanction Limitation And Exclusion Clause

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, 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

War And Civil War Exclusion Clause

Notwithstanding anything to the contrary contained herein this Certificate does not cover Loss or Damage directly or indirectly occasioned by, happening through or in 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.

NMA464

01/01/38

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

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

Complaints

If you wish to make a complaint, please contact:

for claims matters: 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

for all other matters: The Complaints Department

Independent Broking Solutions Limited
150 Minories – Suite 610
London
EC3N 1LS

Email: info@isgrp.co.uk

Tel: + 44 (0)20 347 5670

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:

Complaints
Lloyd's
One Lime Street
London EC3M 7HA

Tel: +44 (0)20 7327 5693

Fax: +44 (0)20 7327 5225

E-mail: complaints@lloyds.com

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



T: +44 (0) 20 3675 0910
E: support@optimumsr.co.uk
W: www.optimumsr.co.uk
150 Minories, London, EC3N 1LS



Statement of Fact for Your Optimum Cyber Plus Policy

IMPORTANT INFORMATION

This Statement of Fact records the information provided to Optimum Specialty Risks and any assumptions that have been made about your business. It is important that the information is correct otherwise your claim may be 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

THE POLICYHOLDER: Royal Engineers Association

PRINCIPAL ADDRESS:
HQ Royal Engineers
Chatham
ME4 4UG

INSURED DECLARATION

DATE OF PROPOSAL: 03 November 2021

POLICY REFERENCE: 6666983

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 or have any prosecutions pending or been given an official police caution, in respect of any criminal offence other than motoring offences 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
Are all changes to vendor/client/customer contact and/or bank account details agreed in writing, confirmed and validated over the telephone with the client/customer?	Yes
Does the Insured deploy commercial grade antivirus and firewalls across your network?	Yes
Does the insured take all reasonable precautions to password protect (or use biometrics) their operating systems and all portable media including, but not limited to smartphones, tablets and memory sticks?	Yes
Does the Insured (or you outsource provider) back up critical data at least every 7 days?	Yes
Does the Insured process or store any credit or debit card information?	Yes
Is the Insured PCI Compliant?	Yes

Has the Insured suffered any unplanned network outage in the last 12 months that exceeded 4 hours &/or any claims/incidents in the past 5 years that may have resulted in a claim if a policy had been in force?	No
In response to the recent DearCry Ransomware attack, has the insured has completed and 100% successfully installed the security patch released from Microsoft in March 2021 addressing the issues with Exchange Server 2013 / 2016 / 2019?	Yes

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.

How to utilise your Risk Management Support



Avast CloudCare

Avast Cloudcare included with your Optimum Cyber Plus Policy

OSR have partnered with Avast to help protect your staff from viruses, cyber-attacks and loss of data. Avast is one of the largest security companies in the world using next-gen technologies to fight cyber-attacks in real time.

Avast CloudCare solution includes award-winning anti-virus, firewall, endpoint protection and data backups for your organisation. As an OSR policyholder, you are eligible for up to 30 device licences of Avast CloudCare free of charge. You will also be given 300GB of Cloud storage.

Please click below to access the installation guide. This will assist you in installing the software correctly.

OSR Avast CloudCare
Installation Guide

To obtain your Avast CloudCare licences please click below and complete the short registration:

OSR Avast CloudCare
Sign up

Product overview:

- File Shield scans files and programs before allowing them to open or run.
- CyberCapture sends suspicious files to the Threat Lab for analysis.
- Firewall filters network traffic and stops untrusted connections.
- Behaviour Shield stops dangerous programs and applications on your device.
- Web Shield blocks dangerous websites before they open.
- Email Shield continuously checks for threats in incoming and outgoing emails.
- Anti-spam blocks unwanted spam and phishing emails.
- Smart Scan quickly checks for any performance or security issues.
- Sandbox is a safe environment to test dubious files and programs.
- Wi-Fi Inspector discovers vulnerabilities in your network.
- Real Site keeps you away from fake sites designed to steal your data.
- Rescue Disk creates an external backup antivirus to salvage compromised PCs.
- Data Shredder permanently deletes files you don't want recovered.
- Browser Clean up erases junk files slowing down your browser.
- Webcam Shield alerts you before your webcam is turned on to protect your privacy.
- Passwords protects your passwords and streamlines your online accounts.
- Secure line VPN makes open, vulnerable networks safe, anywhere in the world.
- Supported devices: Windows PCs, Windows 7 SP1 or higher (32-bit, 64-bit), Windows 8/8.1, except RT & Starter edition (32-bit, 64-bit), Windows 10, except Mobile & IoT core edition (32-bit, 64-bit)

Please contact a member of our team if you have any questions. We are here to help.



Protect Customer Data

It's crucial that customers know their data is secure. With Avast CloudCare, data is protected both in-transit and at rest using three-tier encryption. Avast Business Cloud Backup data centre's also have ISO9001 and ISO27001 certification giving customers peace of mind that their data won't be compromised.



Restore and Back up anytime

Set schedules to automatically back up data whenever a device is connected to the Internet. Should the worst happen, customer data can be restored on-demand ensuring the impact of any data loss is minimized.



Data Reporting

Generate real-time reports on stored data usage, individual device usage, backup plans, history and much more.



View and restore files anytime

If data is lost or becomes corrupt, backed up data can be viewed and restored directly from the Avast CloudCare portal.



SQL and Exchange back up

Backup and restore SQL 2008 and 2012 databases, Exchange 2003, 2007, 2010 and 2013 mailbox databases from the Avast Business Cloud Care portal.



Protect Servers

ShadowProtect® enables you to image and back up servers to protect against hardware failures, lost information or even issues that arise with a location move.



CloudCare Architecture

- 256-bit AES encryption at device level
- 128-bit SSL encryption in transit
- 256-bit AES encryption at data centres
- Private Cloud, fully redundant data centres
- Secure user password enforcement
- Compatible with existing firewalls
- Log in to CloudCare using your Apple iPhone™ & iPad™ with our CloudCare app

Thank you for purchasing your policy

Your Optimum Cyber Plus Policy entitles your organisation to complimentary Cyber & Data Awareness Training and GDPR Gap Analysis.

Analysis provided by OSR's partners GDPR123.

For terms and conditions please see www.gdpr123.com/osr


Optimum Speciality Risks

GDPR123

THIS VOUCHER ENTITLES YOUR ORGANISATION* TO

GDPR GAP ANALYSIS

One Hour Consultation with our experts

TO BOOK YOUR APPOINTMENT:

Call us on: **+44 (0)203 457 4683**. Select option 2.
Before calling please ensure you have your insurance policy to hand.


Optimum Speciality Risks

GDPR123

THIS VOUCHER ENTITLES YOUR ORGANISATION* TO

CYBER & DATA AWARENESS TRAINING

E-Learning Based Training and Reporting

TO BOOK YOUR APPOINTMENT:

Call us on: **+44 (0)203 457 4683**. Select option 2.
Before calling please ensure you have your insurance policy to hand.

Important Cyber AMI

Reduce exposure to 80% of common cyber threats through compliance with HM Government's Cyber Essentials scheme.

A 12-month subscription to Cyber AMI is provided to you free-of-charge as a benefit of your insurance policy.

This service will help you achieve compliance with the Cyber Essentials scheme, and certification if desired.

Cyber AMI provides plain-English self assessment and education for non-technical individuals. Using Cyber AMI could save you thousands of pounds over using a consultant.

What is Cyber Essentials?

Cyber Essentials is a risk management specification designed by HM Government. Compliance with the requirements will reduce your risk of common cyber threats by up to 80%. Certification to this specification is increasingly demanded. Furthermore the ICO recognise it as supportive in complying with the GDPR.

Why should I use this?

1. Threats are increasing daily. Businesses of all sizes in all industries are at significant risk. Businesses should implement better working practices as soon as possible.
2. Cyber security consultancy now typically costs £1,000 +VAT per day. You won't need a consultant to achieve Cyber Essentials compliance through Cyber AMI.
3. Through plain-English Cyber AMI will help your business implement better security practices, and you can progress at your own pace.

How to get started?

Register your free account here:

<https://www.cyber-ami.com>

Help and support

Email support@berea-group.com
or call 0116 287 3600

KryptoScan onboarding guide

OSR has partnered with KryptoKloud to offer all new Optimum Cyber Plus policyholders usage of KryptoScan, their new rapid infrastructure threat analysis tool. KryptoScan will provide organisations an instant understanding of the exposure level of externally facing IT applications and infrastructure.

Further to your enrollment as a policy holder with OSR, you are entitled to a vulnerability analysis report from the KryptoScan service. In order to arrange and organize your KryptoScan please follow our on-boarding guide below to begin the registration process.



KryptoKloud

KryptoScan sign up process

1. To obtain your free KryptoScan report please click below and complete the brief registration.

OSR KryptoScan Sign up

2. Enter Password OSR-SCAN-1925! where prompted. You will also need your policy number to hand.
3. Your policy number will be verified by KryptoKloud.
4. A member of the KryptoKloud team will contact you to arrange your scan.
5. All results will be provided within 1 business day to ensure rapid visualisation of your risk exposure.
6. KryptoKloud will provide you with 2 hours free consultancy to review any issues highlighted by the KryptoScan.

Key Benefits



Lowens Risks

Helps prevent data breaches from those with access to critical business assets and information.



GDPR Alignment

Implementing KryptoScan can help ensure you have the right measures in place for GDPR compliance.



Protects in Minutes

Setup of KryptoScan is quick and easy, ensuring no business down time.

Please contact a member of our team if you have any questions. We are here to help.











U210060 RE Association Cyber - Covering Letter

Final Audit Report

2021-12-07

Created:	2021-12-07
By:	Account Controllers (accountcontrollers@newdawnrisk.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAHueJsl1Jk7MKNCxwIFLR_5maWsPIEVhT

"U210060 RE Association Cyber - Covering Letter" History

-  Document created by Account Controllers (accountcontrollers@newdawnrisk.com)
2021-12-07 - 6:43:54 PM GMT- IP address: 89.197.180.146
-  Document emailed to Tom Malcolm (tom.malcolm@newdawnrisk.com) for signature
2021-12-07 - 6:45:49 PM GMT
-  Email viewed by Tom Malcolm (tom.malcolm@newdawnrisk.com)
2021-12-07 - 8:29:00 PM GMT- IP address: 121.91.81.113
-  Document e-signed by Tom Malcolm (tom.malcolm@newdawnrisk.com)
Signature Date: 2021-12-07 - 8:29:08 PM GMT - Time Source: server- IP address: 84.255.50.4
-  Document emailed to Max Carter (max.carter@newdawnrisk.com) for signature
2021-12-07 - 8:29:09 PM GMT
-  Document e-signed by Max Carter (max.carter@newdawnrisk.com)
Signature Date: 2021-12-07 - 8:52:39 PM GMT - Time Source: server- IP address: 85.255.233.109- Located near: (51.5148, -0.0965183)
-  Offline document events synchronized and recorded
2021-12-07 - 8:52:41 PM GMT - Time Source: server- IP address: 85.255.233.109
-  Agreement completed.
2021-12-07 - 8:52:41 PM GMT