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: Canopius Email Address: cyber.incident@canopius.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.