

Product Name: CyberSafe  
Carrier name: Munich Re Syndicate Limited  
Class of business: Cyber  
Date: Q3 2023

## 1 Manufacturer Information

Munich Re Syndicate Limited and Munich Re Specialty Insurance (UK) Limited are the joint manufacturers for this product as set out in our binding authority agreement and the manufacturer activities are allocated as follows:

Activity	Party Responsible
Product Approval Process	Munich Re Syndicate Limited and Munich Re Specialty Insurance (UK) Limited
Target Market	Munich Re Specialty Insurance (UK) Limited
Product Testing	Munich Re Specialty Insurance (UK) Limited
Product Monitoring & Review	Munich Re Syndicate Limited and Munich Re Specialty Insurance (UK) Limited
Distribution Channels	Munich Re Syndicate Limited and Munich Re Specialty Insurance (UK) Limited
IPIID Development	The activity of IPIID development is not required for UK Commercial Risks

This document is intended to provide a summary of the product, intended target market, product distribution strategy, and the product approval process. It also sets out the outcome of the annual product review and fair value assessment. This document is intended to be used by distributors and not provided to the end customer.

### 1.1 Product Information

- **Product Description:** CyberSafe is designed to protect against the loss, theft or destruction of the insureds digital assets, systems and electronic funds and offer protection from cyber risk which could be damaging to the insureds business and reputation.
- **Demands & needs:** CyberSafe provides first party cover for cyber response, cyber restoration, cyber expense, court attendance costs, cyber extortion and business interruption, cyber liability and media liability.

As an element of cover we may also appoint a third party breach response provider, either RPC/Resecure or Cyber Scout following an actual or suspected cyber events, cyber extortion or data breach first discovered for the purpose of identifying the cause and making necessary and reasonable recommendations as to how the cause might be terminated or mitigated.

The cover has a maximum aggregate limit of liability of £5,000,000 and a maximum aggregate cyber-crime sub limit of £100,000.

The key exclusions for this product include;

Software and firmware vulnerabilities where patches have not been applied within 30 days of release,

Any bodily injury, mental injury or death *however this exclusion shall not apply to any third party claim seeking compensatory damages for mental anguish or distress,*  
 Any loss arising out of damage or loss of use of tangible property,  
 The loss of value of data,  
 Any guarantee, warranty, contractual term or liability assumed or accepted by the insured under any contract or agreement except to the extent that liability would have attached in the absence of such contract or agreement *however this exclusion shall not apply to any Payment Card Industry Liability,*  
 Loss of money or securities, or the decrease in financial value of an asset *however this exclusion shall not apply to any financial loss arising out of cybercrime covered under the Policy,*  
 Any loss arising from the fraudulent or reckless collection and/or processing of personal data by the insured without the permission of the data subject,  
 Any loss arising from the insureds use of illegal or unlicensed software,  
 The failure of infrastructure other than the insured computer system,  
 The overloading of bandwidth connections or webservers solely because the demand for the insureds website exceeded that which the servers are designed to process unless the reason for such demand is the direct result of a cyberattack,  
 Any spam and/or unsolicited marketing communications knowingly sent by the insured,  
 Other Insurance Clause and  
 Other standard market exclusions apply.

- **Target Market:** This product is designed for UK domiciled small and medium-sized enterprises with a turnover of less than £200 Million.
- **Not intended for:** This product is not suitable for UK domiciled enterprises with a turnover of more than £200 Million, retail customers, or risks domiciled outside of the UK. There are also specific sectors that we do not cover which includes adult entertainment, payment processors, energy industries, search engine, political organisations, investment/state banks, currency exchange, council/local authority, social networks and coach or bus operators.
- **Territorial reach:** United Kingdom including the Channel Islands and Isle of Man. Cover may also be available for subsidiary companies domiciled and risks located outside the above territories subject to internal underwriting guidelines, risk appetite, licensing requirements and sanction regulations.
- **Optional additional cover/extensions:** There are optional additional covers/extensions which the customer is able to select in order to meet their needs. Information on our optional additional cover/extensions is provided in the table below.

Optional Add-on / Extension	Demands and needs
Cyber Crime	This covers financial loss arising from; the transfer of funds to a third party as a result of a fraudulent misleading instruction, the fraudulent input, destruction or modification of data to the insured computer system and the insured liability to make payment to their telephone service provider as a result of a cyberattack on their computer system.

<p>Payment Card Industry Liability</p>	<p>If the payment service provider brings a claim against the insured for an actual or alleged breach of any contractual duty under a payment card processing agreement with the payment service provider, we will pay for contractual fines or penalties arising out of the insureds failure to comply with PCI data security standards including card reissuance costs, card fraud recoveries and the costs of a mandatory audit in order to demonstrate compliance with PCI data security standards and defence costs.</p>
--	---

## 1.2 Distribution strategy for this product

- **Sales method:** This product is sold as a standalone product via a broker platform called Realytix.
- **Advised or non-advised sales:** All our products are sold through Brokers and therefore we expect Brokers to provide the advice to the end customer.
- **Assessment of customer demand and needs:** We expect distributors to have effective assessment processes in place for establishing the customer's eligibility and demands and needs and offering this product only where it is appropriate for the customer's stated demands and needs.
- **Commission:** An assessment of the commission structure for brokers has been carried out and it is deemed to be appropriate and reasonable.

## 1.3 Product Information and Approval Process

In accordance with the FCA's Product Intervention and Product Governance Sourcebook ('PROD') rules, we have completed product reviews and fair value assessments across all of our products. The fair value assessments considered product performance against a number of areas including, but not limited to:

- Conduct Risk MI
- Complaints Data
- Commission Ranges
- Loss Ratios
- Broker Surveys
- Customer Understanding & Support Reviews

We will undertake ongoing product reviews on a yearly basis and any significant or material changes to this product will go through the product approval process again.

## 1.4 Outcome of the Product Review and Fair Value Assessment

As a result of the product governance activities undertaken across this product, we can confirm the following:

- The product remains consistent with the needs of the identified target market
- The product continues to provide fair value
- The intended distribution strategy remains appropriate

Date Fair Value assessment completed	<b>Q3 2023</b>
Expected date of next assessment	<b>Q3 2024</b>