

## FUNDS PROTECT BUSINESS POLICY WORDING

This Policy is a formal agreement between you and Phishield UMA (PTY) Ltd (hereinafter referred to as 'We/Us') who have a mandate to act on behalf of Bryte Insurance Company Limited.

Phishield UMA (PTY) Ltd is duly registered and incorporated in accordance with the company's laws of the Republic of South Africa, having Registration number 2012/1301796/07 and Financial Services Provider number 46418 that carries on business as an underwriting management agency.

Bryte Insurance Company Limited is duly registered and incorporated in accordance with the company's laws of the Republic of South Africa, having Registration number 1965/006764/06 and Financial Services Provider number 17703 and carries on business as a registered short-term insurer.

All documentation associated with regards this Policy shall be read together as one contract and any word or expression to which a specific meaning has been attached in any part of the Policy or the cover explanation shall bear specific meaning wherever it may appear.

### DESCRIPTION OF POLICY

We agree to indemnify Your Business against a Loss of Funds up to the limit stated in the Policy Schedule which is incurred due to an Insured Event as specified in this document which results in a Loss of Funds.

### CONDITIONS OF COVER

The insurance cover is conditional upon Your Business having an active approved Internet Security Software system running on all Access Devices used. Please note that this does not include any free or trial versions of Internet Security Software.

This Policy will only come into effect following payment of the Premium by Your Business and the receipt thereof by or on behalf of us.

### DEFINITION OF TERMS

By "*Access Device*" we mean:

Any device, mechanical or otherwise, or method, including without limitation, a password, a passphrase, a personal identification number (PIN) or any other authentication method whatsoever, designed to control and or restrict and or allow access to your account.

By "*Account*" we mean:

Any demand deposit (i.e. cheque account), savings, cash portion of a brokerage account, credit card, loan or other account held in Your Business name or under Your Business identification number held directly with an Outside Entity, which Your Business can access via the internet for the purpose of transacting electronically. This account must be established by Your Business primarily for business purposes.

By "*EFT Duping Event*" we mean:

EFT or deposit scams involving the use of altered or fraudulent teller receipts, internet payment confirmations or deposit slips to trick you into believing a payment has been made into your account and cleared and you have transferred monies out of your Account and suffered a financial loss.

By “*EFT Fraud Event*” we mean:

A Funds Transfer from your bank account to a third party who has manipulated the details of Your Payee to induce you into transferring monies from your account. This includes transactions where Your Payee’s identity has been stolen, falsified, fraudulently altered or used and you have transferred funds.

This does not include online classified sites for example (but not limited to) Gumtree, OLX, Junkmail etc. for goods or services purchased from unknown or unverified parties.

By “*Employee*” we mean:

Any person and or entity acting directly and or indirectly for and on behalf of Your Business.

By “*Fund Transfer*” we mean:

Any transfer of funds initiated in person or through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing or authorising an Outside Entity to debit or credit Your Business Account.

Fund transfer includes but is not limited to:

- point-of-sale transfers;
- automated teller machine transfers;
- direct deposits or withdrawals of funds;
- transfers initiated by telephone;
- transfers resulting from debit card transactions, whether or not initiated through an electronic terminal.

A Funds Transfer does not include a transfer of funds by an Outside Entity or its employee.

By “*Insured Event*” we mean:

The following events, as defined in this document, which results in a Loss of Funds, are covered:

- EFT Fraud Event
- EFT Duping Event
- Unauthorised Funds Transfer Event

By “*Internet Security Software*” we mean:

One of the following software packages or any other internet security software approved by us:

- Avast Internet Security
- AVG Internet Security
- Kaspersky Internet Security
- Bitdefender Internet Security
- Norton Security
- McAfee Security
- ESET Security
- Trend Micro Maximum Security

and specifically excludes free or trial versions of the above-mentioned providers or any other internet security software that may be available.

By "*Loss of Funds*" we mean:

The principal amount of monetary loss incurred by Your Business due to an Insured Event, exclusive of interest and fees, for which you have not received reimbursement in any way from any source whatsoever. The loss must be caused by an Insured Event, which occurred during the period of cover and for which You have sought reimbursement from the Outside Entity that holds the Account from which the funds transferred.

By "*Outside Entity*" we mean:

Any bank, savings association, credit institution, or any other person or business that directly holds an account belonging to Your Business, or that issues an Access Device and agrees with Your Business to provide fund transfer services.

By "*Policy*" we mean:

The contract between the Insurer and the policyholder which determines the claims which the Insurer is legally required to pay.

By "*Policy Schedule*" we mean:

The document which outlines the cover provided under the Policy which details the name of the policyholder, Policy benefits and states the cover amount provided.

By "*Premium*" we mean:

The amount and details of the premium payment obligations are specified in the Policy Schedule. The due date for the payment of premium is specified in your Policy Schedule. In the event that your claim was unsuccessful and rejected, we will not reimburse you for the premiums that you have paid. Premium is payable in advance annually or monthly in order for the cover to be active. In the event of non-receipt of premiums, no claims will be payable.

By "*Unauthorised Transfer of Funds Event*" we mean:

A Fund Transfer from Your Business account initiated by a person without the actual authority to initiate such transfer and from which Your Business receives no benefit. This includes the fraudulent use of Your Business name, address, identification number, bank or credit card account number, Access Device, any other identifying information or any other method of identifying Your Business which results in a Loss of Funds due to a Funds Transfer.

Unauthorised Transfer of Funds Event does not include a Fund Transfer initiated:

- by a person or Employee who you know or are familiar with and who you have authorised to make use of the Access Device;
- from any personal account.

By "*Your Business*" we mean:

The policyholder as specified in the Policy Schedule.

By "*Your Payee*" we mean:

A supplier or customer that you have transacted with (made a payment to or received from).

## TERRITORIAL LIMITS

There are no territorial limits for this Policy i.e. you are covered anywhere in the world, subject to relevant local legislation and regulatory requirements.

## SCOPE OF THE POLICY

Your Business policy will only cover you if

- You report the Insured Event which caused a Loss of Funds to us within 90 days of discovery;
- You first discover the Insured Event while Your Business device is protected by the active approved Internet Security Software.

## WHAT IS NOT COVERED

This Policy shall not apply to any Loss of Funds arising directly or indirectly in the event of the following:

- Any dishonest, criminal, malicious or fraudulent acts Your Business participated in, directed, or had prior knowledge of;
- Any Loss of Funds due to fraudulent intent by you or any person acting in concert with you;
- Any physical injury, sickness, disease, disability, shock, mental anguish, and mental injury, including required care, loss of services or death at any time resulting therefrom;
- Any Loss arising from an Insured that is not reported to us within 90 days after it is first discovered by Your Business;
- Any Loss from an Employee's account or for personal transactions;
- Any Unauthorised Loss of Funds arising directly or indirectly from destruction, confiscation or seizure by order of any government or public authority;
- Any Loss of Funds, including expense or damages, arising directly or indirectly from any Insured Event, for which an Outside Entity is legally liable;
- Any costs or claim recoverable from a third party;
- Any events that occurred before the inception date;
- Any Loss of Funds due to unlicensed software use, computer viruses or similar destructive media;
- Any consequential loss or damage which is not directly caused by an Insured Event;
- Any Loss of Funds incurred due to Internet Security Software which is a free or trial version;
- Any Loss of Funds for an Insured Event that first occurs after the termination of the Policy or termination of the approved Internet Security Software.
- Any Loss of Funds for Insured Events that occur after termination of the Policy.

Termination of your Internet Security Software shall not reduce or eliminate the 90 day period in which you can report to us an Insured Event subject to proof that the required approved Internet Security Software was active when the Loss of Funds occurred.

## PERIOD OF COVER

All premiums are to be paid monthly or annually in advance. Cover will be active for the period for which premiums have been received.

## NON-PAYMENT OF PREMIUM

If we do not receive the payment of your Premium we will not be liable to pay any Loss of Funds as detailed in this document. This includes any reversed Premiums or stopped Premiums.

## TERMINATION OF THE POLICY

You/We may cancel your Policy at any time by giving 30 days' written notice.

## AMENDMENT OF POLICY TERMS AND CONDITIONS

We may make changes to the terms and conditions of this Policy as and when we deem it necessary to do so. When we do, we will give you 30 days' written notice to your nominated email address.

## TRANSFERABILITY OF THE POLICY

This cover may not be transferred to another party or person.

## UPDATE OF PERSONAL INFORMATION OR PERSONAL CIRCUMSTANCES

It is very important that you keep us updated with your contact information and personal details, especially your email address, as all communication from us will occur via electronic means only. The onus is on you to ensure that you provide us with the correct email address and personal details and we will accept no liability for any errors in this regard. Personal details include, but are not limited to:

- Email address;
- Dishonesty; tell us about any convictions or offences related to dishonesty by you;
- Potential risk which may affect the terms and conditions of this Policy.

Inform us immediately of any changes to your circumstances that may influence the terms and conditions of this Policy.

## HONESTY IS ALWAYS THE BEST POLICY

Always provide us and the authorities with true and complete information. This applies to any other party that may act on your behalf. We act on the information you provide, therefore any information which is misleading, incorrect or false will prejudice the validity of your claim or may make this Policy null and void (you will no longer be entitled to any benefit and any premiums paid will be forfeited).

If a claim is also covered by an insurance policy that you may have, we will only pay you out for our portion. It is unethical and prohibited to benefit financially from a loss as defined in this document.

## SHARING OF INFORMATION

We respect the confidentiality of your information and will never misuse it. We require your personal information for claim purposes and to enable us to underwrite your risk fairly. Your personal information is further used by us for any decision pertaining to the continuance of your policy. We further require your personal information to enable us to comply with legal and regulatory obligations. Your personal information may be stored in a shared database by us and may be verified against legally recognised sources or databases. Your personal information may not be used for any other purposes other than for the purposes as set out above. We will never share any information with any entity, natural person or third party unless you have provided us with written permission to do so, or we are required by relevant legislation or regulation to provide such information.

## HOW WE PAY YOUR CLAIM

We have the choice to settle your claim in any of the following ways:

- Paying out cash to your Bank account or
- Pay out to your Credit Card.

## HOW TO CLAIM

- Contact Phishield Emergency Assist Line **+27(0) 11 083 5106**, or lodge an intent to claim on the website **www.phishield.com** as soon as possible after the incident. The sooner you notify us the quicker we are able to assist you.
- We will need to verify that your Policy is active and valid, and obtain the required information.
- Inform the Outside Entity to check and verify the Insured Event.
- Inform the police / authorities of the Insured Event as soon as possible, but no later than 24 hours after becoming aware of the event.

- In order to process your claim we may request some documentation to verify the claim. Any cost associated with obtaining the required documentation will be for your account. All requested information and documentation will be required within the set timeframe.
- You must report an incident or claim within 90 days of discovery of an Insured Event. This includes incidents for which you do not want to claim right away, but which may result in a claim in the future.
- The documentation you may need to provide includes, but is not limited to, the following;
  - Company registration documents;
  - Proof of business address;
  - Bank / credit card details;
  - The police report;
  - The police case number;
  - A letter from the Outside Entity stating that they will not reimburse the Loss of Funds incurred.
- You may be required to submit the proof of purchase of your Internet Security Software in order to validate a claim.
- You will need to let us know if you have insurance cover that covers the same event. We will not cover any Loss of Funds covered by a third party.
- Inform us if you become aware of any possible prosecution, legal proceedings or claim that could be lodged against you as a result of the incident for which you have already claimed for.

## OUR COMMITMENT TO YOU

We are committed to settle all valid claims within 72 business hours of obtaining all the necessary documentation. However, it is in the interest of all our clients that we investigate the validity of a claim. For this reason, delays in authorising claims may sometimes occur.

## FRAUDULENT OR DISHONEST CLAIMS

If your claim is rejected (initially or after an investigation) due to fraud or dishonesty, you will forfeit any premiums paid, and you will need to pay us back for any expenses that we may have incurred relating to the claim. If you, or anyone acting on your behalf submits a claim, or any information or documentation relating to any claim, that is in any way fraudulent, dishonest or inflated, we will reject that entire claim and cancel your Policy, from the date on which the incident has been reported, or from the actual incident date, whichever date is the earliest. We will also report your fraud or dishonesty to the relevant authorities.

## COMPLAINTS AND DISPUTED / REJECTED CLAIMS

Should your claim be rejected, you will be notified in writing and will be provided with the reasons for rejection. If you disagree with the outcome (our final decision) of your claim with us, you may object in writing within 90 days from the date of rejection. You will need to make written representation to us with valid reasons as to why you disagree with our decision. The claim may be reconsidered and you will receive further written notification of the outcome of your dispute. Following directly on the first day after the 90 day period mentioned above, you will have a further 6 months to serve a formal summons on us. If you have not formally (in writing) raised your objection within any of these reasonable time frames, you will then no longer have the right to dispute the outcome.

Please send any formal notification of disputes to [complaints@phishield.com](mailto:complaints@phishield.com).

## HELP US STOP FRAUD

Fraud increases claim costs for all of us, and could in turn lead to increased fees. It is also a criminal offence that is punishable by law. We support the prevention of fraud. If you know of any fraud or suspect that someone is involved in fraudulent activities, please contact one of the following agencies:

### Southern African Fraud Prevention Services

Help-Line: 0860 101 248  
Telephone: +27(0)11 867 2234  
Fax: +27(0)11 867 2315  
Website: [www.safps.org.za](http://www.safps.org.za)



## Report a Crime

Website [www.reportacrime.co.za](http://www.reportacrime.co.za)

## South African Insurance Crime Bureau

Telephone: +27 021 1432/3/4/5

After hours: +27 72 313 6224

Fraudline: 0860 002526 (anonymous)

Website: [www.saicb.co.za](http://www.saicb.co.za)

## **STATUTORY NOTICE TO SHORT-TERM INSURANCE POLICYHOLDERS, SECTION 13 CERTIFICATION AND OTHER LEGAL REQUIREMENTS**

In terms of the Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS Act), you have the right to the following information as a short-term insurance policyholder or prospective policyholder: This notice does not form part of the insurance contract or any other document. Please read the contents of this document carefully.

### **STATUS OF THE FINANCIAL SERVICES PROVIDER IN TERMS OF THE FAIS ACT**

Phishield UMA (PTY) Ltd is an authorised Financial Services Provider (FSP 46418) and the company registration is 2012/1130796/07.

Key Individual: Trevor Case (ID number 7409165439080)

The name, address and contact details of the product suppliers are provided in the documentation covering each of the products purchased and provided. All conditions or restrictions imposed by the product supplier are set out in the applicable policy documentation.

Phishield UMA (PTY) Ltd is the underwriting manager and administrator and has a written mandate to act on behalf of Bryte Insurance Company Limited. There is no shareholding between the Insurer and the FSP. The FSP has been authorised since 2015 with the Financial Services Board.

### **FINANCIAL PRODUCTS PROVIDED AND AUTHORISATION**

The name, class or type of product and the nature and extent of the benefits provided are set out in the accompanying policy documentation provided by the product suppliers and include information about the nature and extent of their obligations to you and your obligations to them.

**Services the FSP is permitted to provide:** Short-term Insurance (Personal Lines & Commercial Lines Policies)  
Advice and Intermediary Service

The FSP accepts responsibility for the actions of the Representatives acting in the scope and course of their employment and regularly monitors the Fit and Proper Status of its representatives. The FSP confirms that according to their knowledge their representatives are Fit and Proper. The FSP will not be held liable in terms of prejudice in respect of services or advice provided by a Representative which falls outside the scope of authorisation, and any complaint in respect of any product which falls outside the definition of financial product of the FAIS Act, cannot be forwarded to the FAIS Ombud or Short-Term Insurance Ombudsman.

### **INDEPENDENT STATUS OF THE FSP AND PROFESSIONAL INDEMNITY INSURANCE**

In the past 12 months the FSP has earned more than 30% of its income from the Insurer. The FSP and Representatives have no financial interest in any other Insurer or product supplier. The Representatives and FSP carry professional Indemnity Insurance as required.

### **CONFLICT OF INTEREST POLICY**

A copy of the FSP's Conflict of Interest is available on request or may be viewed online at [www.phishield.com](http://www.phishield.com). The FSP has common shareholders with Phishield SA (PTY) Ltd, who acts as an intermediary / broker on behalf of the Insurer on some of the policies administered by the FSP. All potential conflicts or conflicts which may unfairly prejudice a policyholder are carefully monitored and avoided where possible.

### **COMPLAINTS**

If you have a complaint, please contact the FSP Key Individual or the Complaints Officer. He/She will assist you to address the concerns you have. Please note that in terms of the FAIS Act, all complaints must be addressed to us in writing. Should we not be able to address the concerns to your satisfaction, you may wish to lodge a complaint with any of the Ombud and/or Ombudsman whose details appear below. If you wish to learn more about our complaints policy and procedure, please contact our complaints officer via email ([complaints@phishield.com](mailto:complaints@phishield.com)) or consult our websites for a copy of the complaints policy. We subscribe to the highest ethical code and we require all our representatives to adopt this in their dealings.

### **SHARING OF INFORMATION AND CONFIDENTIALITY**

Insurers share information with each other regarding policies and claims with a view to prevent fraudulent claims and to obtain material information regarding assessment of risks proposed for insurance. By reducing the incidents of fraud and assessing risks fairly, future premium increases may be limited. This is done in the public interest of all current and potential policyholders. The sharing of information includes, but is not limited to information sharing via the information Data Sharing System operated by TransUnion ITC on behalf of the



South African Insurance Association. By the Insurer accepting or renewing this insurance, you or any other person that is represented herein, gives consent to the said information being disclosed to any other insurance company or its agents.

You also similarly give consent to the sharing of information in regard to past insurance policies and claims that you have made. You also acknowledge that information by yourself or your representative may be verified against any legally recognised sources or databases.

By insuring or renewing your insurance, you hereby not only consent to such information sharing but also waive any rights of confidentiality with regard to underwriting or claim information that you have provided or that has been provided by another person on your behalf.

In the event of a claim, the information you have supplied with your application together with the information you supply in relation to the claim, will be included on the system and made available to other insurer's participating in the Data Sharing System.

## **IMPORTANT – FAIS GENERAL CODE OF CONDUCT**

Section 21 of the General Code of Conduct states that no provider may request or induce in any manner a client waive any right or benefit conferred on the client by, or in terms of, any provisions of this code, or recognise, accept or act on any such waiver by the client and such waiver is null of void.

Please also take note of the following:

- You must be informed of any material changes to the information provided above.
- If the information above was given to you verbally, it must be confirmed to you in writing within 30 days.
- If any complaint of the broker or Insurer is not resolved to your satisfaction, you may submit a complaint to the Registrar of Short-term Insurance or to the FAIS Ombudsman. (Details below)
- Polygraph or any lie detector test is not obligatory in the event of a claim and the failure thereof may not be the sole reason for repudiating the claim.
- If the premium is paid by debit order:
  - It may only be in favour of one person and may not be transferred without your approval;
  - The Insurer must inform you at least 30 days before the cancellation thereof, in writing, of its intention to cancel such debit order.
- The Insurer and not the Intermediary must give reasons for repudiating your claim.

## **CUSTOMER RESPONSIBILITY**

It is important that all of the information provided by you or on your behalf is complete and accurate. Should this not be so, the possible consequences of incomplete, misrepresented or non-disclosed information associated with your application include the cancellation of the products applied for and the forfeiture of any monies paid to date, the repudiation of all claims irrespective of their cause or nature, and the possible institution of criminal action against you. Whilst reasonable steps have been taken to ensure that the products applied for by yourself are suitable for providing cover appropriate to the purchase you have made, no analysis of your financial needs or risk profile has or will be made by the FSP or those associated with it. It is therefore vital that you take particular care to ensure that the product or products you have purchased are appropriate and adequate for your needs.

Do not sign any blank or partially completed application form and complete all forms in ink. Keep all documents handed to you and make notes as to what is said to you. Do not be pressured into buying a product not suitable to your needs.

## **REMUNERATION, FEES AND COMMISSION**

The FSP collects an underwriting and administration fee for each policy sold on behalf of the Insurer. A breakdown of the premium can be found on the policy schedule. Included in the breakdown of the fees are the commission amounts, administration fees and any other additional fees applicable to the policyholder.

## **CONTACT DETAILS**

### **UMA DETAILS (POLICY ADMINISTRATOR):**

#### **Phishield UMA (PTY) Ltd**

Registration number: 2012/1301796/07;  
FSP number: 46418  
Physical address: Fourways View Office Park, Block B, 1210 Sunset Avenue, Fourways  
Telephone: +27 11 083 5106  
Email: [info@phishield.com](mailto:info@phishield.com)  
Complaints resolution: [complaints@phishield.com](mailto:complaints@phishield.com)  
Compliance Officers: Compliance Trust represented by Mr JD Wessels  
Telephone: 011 794 1189

**CLAIMS ADMINISTRATOR DETAILS:**

**RODEL Administration Services (Pty) Ltd**

Registration number: 1997/013419/07  
FSP number: 5431  
Physical address: Glen Eagle Office Park, Zerwick Emporium, 6 Monument Road, Glen Marais, Kempton Park  
Telephone: 011 100 1999  
E-mail: [info@rodelsa.co.za](mailto:info@rodelsa.co.za),  
Website: [www.rodelsa.co.za](http://www.rodelsa.co.za)  
Compliance Officers: Askari Compliance Services – Warren Neil – 082 923 6260, [warren@askaricompliance.com](mailto:warren@askaricompliance.com)  
Complaints resolution: [jenny.erasmus@rodelsa.co.za](mailto:jenny.erasmus@rodelsa.co.za)

**YOUR PRODUCT SUPPLIER / INSURER DETAILS:**

**Bryte Insurance Company Limited**

Registration number: 1965/006764/06  
FSP number: 17703  
Physical address: 15 Marshall Street, Ferreirasdorp, Johannesburg, 2001  
Telephone: +27 11 370 9111  
Website: [www.brytesa.com](http://www.brytesa.com)  
Email: [fais@brytesa.com](mailto:fais@brytesa.com)  
Complaints: [fais@brytesa.com](mailto:fais@brytesa.com)

**REGULATORY BODIES**

**Short-term Insurance Ombudsman**

P.O. Box 32334, BRAAMFONTEIN, 2017  
Sunnyside Office Park, 32 Princess of Wales Terrace, 5th Floor, Building D, Parktown, 2193  
Tel: (011) 726-8900, Fax: (011) 726-5501  
[info@osti.co.za](mailto:info@osti.co.za) / [www.osti.co.za](http://www.osti.co.za)

**FAIS Ombudsman**

P.O. Box 74571, LYNWOODRIF, 0040  
Tel: (012) 470-9080 / 0860 432 766, Fax: (012) 348-3447  
E-mail: [info@faisombud.co.za](mailto:info@faisombud.co.za),  
Website: [www.faisombud.co.za](http://www.faisombud.co.za)

**Financial Services Board**

PO Box 35655, MENLO PARK, 0102  
Tel: 012 428 8000, Fax: 012 347 0221  
Website: [www.fsb.co.za](http://www.fsb.co.za)