CYBER PROTECT **BUSINESS POLICY**

A QUICK AND CONCISE GUIDE TO OUR CYBER LIABILITY PRODUCT OFFERING

WHAT IS COVERED

- 24hr Cyber Emergency Response Team
- First Party Losses
- Third Party Losses
- Suffered by Your Business
- As a result of a Cyber Emergency
- \+
- Loss of Funds due to fraudulent conduct of 3rd party

CYBER EMERGENCY RESPONSE TEAM

Unlimited 24/7 access to a dedicated team of cyber specialists providing:

- Proactive guidance on cyber security issues
- Coordination of post incident services
- Breach response and notification assistance
- Data privacy experts
- Crisis management
- Forensic investigation and remediation support

WHAT IS A CYBER EMERGENCY?

- Data breaches
- Hacking attacks
- Malicious software / malware attacks
- Denial of service attacks
- Cyber extortion attacks

Copyright 2020 (PTY) Ltd. All rights reserved.

Phishield UMA (PTY) Ltd (2012/1130796/07 is an Authorised Financial Services Provider (FSP No: 46418). Phishield is underwritten by Bryte Insurance Company Limited, a licensed insurer and an authorised FSP (17703).

CYBER PROTECT
BUSINESS POLICY

phishield

SCOPE OF COVER

Losses to Your Business (first party losses)	Liability for third party claims (third party losses)	Funds Protect
✓ Business Interruption Loss	✓ Third Party Claims	✓ Loss of funds from your bank account
✓ Data Restoration Costs	✓ Multimedia Liability Claims	✓ Whether authorised or unauthorised
✓ Cyber Extortion Costs	✓ Regulatory Expenses and Penalties	✓ Due to the fraudulent conduct of a 3rd party
	✓ PCI Fines and Penalties	

EMERGENCY RESPONSE COSTS

- Forensic Costs
- External legal fees
- Notification costs for data breaches
- Call centre for queries related to data breaches
- Credit monitoring costs

MAJOR FEATURES

- **Simple application form**
- **Minimal underwriting questions**
- **Low excess amount**
- **Customisable ratings available to suit Your Business needs**
- **Dedicated team of cyber specialists to mitigate losses during a Cyber Emergency**
- **Easy to understand product**
- **User friendly approach to cyber liability**
- **Funds Transfers include authorised and unauthorised transactions**
- **Business Interruption Loss offered at 100% of the cover limit**

COVER LIMITS AVAILABLE			
	R1 000 000	R2 500 000	R5 000 000
	R10 000 000*	R25 000 000*	R50 000 000*

**** Only available directly through Phishield. Please contact Phishield for a bespoke solution.***

Premiums and cover limits available are dependent on industry and annual turnover of the company. All cover is subject to underwriting approval. Sublimits and Excesses apply.

DISCLAIMER: This document does not constitute financial advice and the policy wording must be consulted for full details of the terms and conditions of the product. Terms and conditions apply.

KEY CONCEPTS

BUSINESS INTERRUPTION LOSS

Operating profits / operating expenses and costs incurred to minimise reduction of income

CYBER EXTORTION COSTS

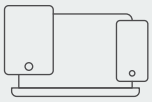
Costs to investigate and resolve Cyber Extortion Threats including ransom payments

CYBER EXTORTION THREAT

Unlawful demand of money by a cybercriminal who threatens to disrupt your Computer System and/or corrupt, destroy, damage, disclose or withhold data, hinder access to, or compromise Your Business website

MULTIMEDIA LIABILITY CLAIMS

Damages and defence costs Your Business is legally obligated to pay for defamation, infringement of IP, data extraction, non-conformance to legal requirements relating to discrimination on website, social media etc.



DATA

Electronic data and/or computer software

DAMAGES

Compensatory amount Your Business is legally obligated to pay as a result of a judgement, award or settlement

THIRD PARTY CLAIMS

A written notice of demand / pending legal action / regulatory action seeking compensation / regulatory penalties/legal remedies

PCI FINES AND PENALTIES

Contractual fines and penalties Your Business is legally liable for due to breach of PCI Security Standards e.g. credit card companies fines / penalties

REGULATORY EXPENSES AND PENALTIES

Fine/penalty by government / regulator following regulatory investigation. Includes associated legal expenses.

DATA RESTORATION COSTS

Costs to regain, replace or restore data that is damaged, lost or corrupted due to a Cyber Emergency

UNDERWRITING REQUIREMENTS

The following factors may affect the outcome of the application:

- Installation of active, comprehensive, paid for internet security on all computer systems
- Data back-ups performed on a weekly basis and annual recovery testing
- Data to be stored separately to main computer system
- Security updated and patches installed and regularly updated
- Emails checked for viruses/malware via email filter
- Ongoing education of employees re secure use of workplace computers
- Documented account verification procedures for Funds Protect cover limits above R250 000

NOTE: Premiums may be loaded or cover may be declined based on the answers provided by the applicant**.**

CONDITIONS OF COVER

- **Computer Systems and Access Devices must be protected by Internet Security Software**
- **Up to date premiums**
- **See Funds Protect Business Cheatsheets for additional requirements re the Funds Protect Cover included in the Cyber Protect product**

DISCLAIMER: This document does not constitute financial advice and the policy wording must be consulted for full details of the terms and conditions of the product. Terms and conditions apply.

CYBER PROTECT
BUSINESS POLICY

phishield

WHO IS THIS PRODUCT SUITABLE FOR?

All SMEs who use computer systems to conduct business

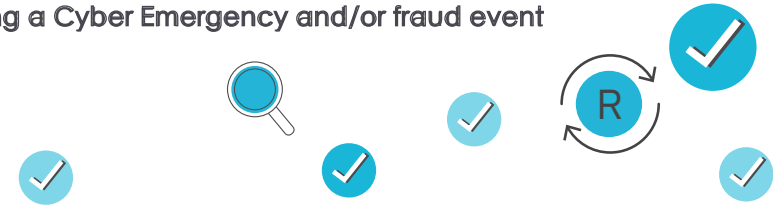
Any business that holds data (especially sensitive data such as client information)

Any business that transacts online

Any business that holds a bank account

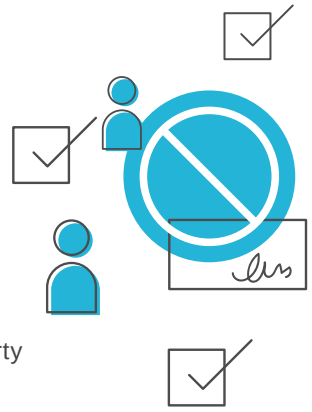
WHY CYBER PROTECT?

- Protects Your Business against financial costs/losses suffered as a result of a Cyber Emergency
- End-to-end services provided during a Cyber Emergency
- Protects Your Business against losses due to Funds Transfer from Your Business Account due to fraud (whether authorised or unauthorised)
- Prevent financial turmoil
- Dedicated team of cyber specialists to assist your business during a Cyber Emergency and/or fraud event



WHAT IS NOT COVERED

- Violation of regulations / laws re consumer protection, antitrust and restrictive trade practices
- Criminal, dishonest, intentional, wrongful acts committed by Your Business
- The interruption of services not under Your Business' operational control
- Confiscation, nationalization, requisition, destruction, damage or interruption of the computer system by governmental/public authority
- Physical damage to tangible property
- Unlawful collection, acquisition or use of data
- Liability assumed by Your Business under contract / agreement
- Claims against any director, officer or partner of Your Business
- Third Party Claims by /on behalf of a director, officer or partner of Your Business
- Third Party Claims due to the rendering/failure to render professional services / professional advice
- Breach of contract by Your Business for provision of professional services/advice to a third party
- Fraudulent claims submitted by Your Business



The exclusions listed above are not an exhaustive list and the policy wording must be consulted for more detailed information.

NOTE: For exclusions regarding Funds Protect, see the Funds Protect Business Product Cheat sheets. Depending on the Funds Protect Cover limit selected, there may be additional conditions of cover.

TERMS AND CONDITIONS APPLY. REFER TO THE POLICY WORDING FOR FULL DETAILS OF THE LIMITATIONS/RESTRICTIONS OF THE PRODUCT

DISCLAIMER: This document does not constitute financial advice and the policy wording must be consulted for full details of the terms and conditions of the product. Terms and conditions apply.