CYBER SECTION

DEFINED EVENTS

Costs, loss or Third Party Claims incurred by, or made on, the Insured's operations domiciled within the Territorial Limits and arising directly due to a Cyber Incident, Cyber Crime, Cyber Extortion or a Data Breach **which occurred on or after the Retroactive date** shown in the schedule **but limited to the cover provided under Defined Events 1 to 4 below.**

1. Data breach response and restoration

The Company will:

1.1 pay on behalf of the Insured, any reasonable and necessary costs resulting from an actual or suspected Data Breach:

1.1.1 for an Expert to investigate and report to the Insured on the Data Breach;

1.1.2 to comply with any data protection legislation (such as notifying any Supervisory Authority or Data Subjects);

1.1.3 to purchase credit and identity theft monitoring services for the benefit of Data Subjects affected by a Data Breach, **subject to the prior written consent of the Company**;

1.1.4 for an Expert to manage and protect the reputation of the Insured **up until a maximum of 60 days** after the Data Breach; and

1.1.5 for Legal Defence Costs incurred to respond to or defend action taken by any Supervisory Authority.

1.2 reimburse the Insured for any legally insurable administrative fines and penalties imposed by any Supervisory Authority as a direct result of the Data Breach.

1.3 pay on behalf of the Insured, any reasonable and necessary costs to restore the Insured's Data and Software after a Data Breach to the closest possible condition in which they were immediately before the Data Breach.

2. Business interruption (if stated as included in the schedule)

The Company will pay for the Insured's Reduction of Gross Profit **during the Interrupted Period** which has been directly caused by a Cyber Incident.

3. Cyber extortion and cyber crime (if stated as included in the schedule)

The Company will reimburse the Insured for:

3.1 any Ransom paid by the Insured **(provided the payment of such Ransom is legally permissible and the Insured has received the prior written consent of the Company to make such Ransom payment)** and any reasonable and necessary costs to resolve Cyber Extortion. At the request of the Company, the Insured must notify any relevant law enforcement authorities of the Cyber Extortion;

3.2 any loss of money as a direct result of Cyber Crime.

4. Third party liability (if stated as included in the schedule)

4.1 Confidentiality and privacy liability

The Company will reimburse any sums the Insured becomes legally liable to pay arising from:

4.1.1 a Third Party Claim or a claim against the Insured by an Employee for a Data Breach relating to Confidential Information or Personal Data of a Third Party, or

4.1.2 subject to the provisions of Specific Exclusion 11, an infringement of any data protection laws, including any Legal Defence Costs relating to the above incurred **with the Company's prior written consent**.

4.2 Network security liability

The Company will reimburse any sums:

4.2.1 the Insured becomes legally liable to pay arising from a Third Party Claim made against the Insured for a Data Breach, Theft of Data or a DoS Attack on a Third Party's Computer Systems, which is directly caused by a Malicious Act or Malware on the Insured's Computer Systems that the Insured failed to prevent, and

4.2.2 any Legal Defence Costs relating to the above incurred **with the Company's prior written consent**.

4.3 Media liability

The Company will reimburse any sums the Insured becomes legally liable to pay arising from the Insured's Online Media Activities that directly causes a Third Party Claim for:

4.3.1 defamation;

4.3.2 breach of copyright, title, slogan, trademark, trade name, service mark, service name or domain name; or

4.3.3 breach or interference of privacy rights;

including any Legal Defence Costs relating to the above incurred **with the Company's prior written consent**.

DEFINITIONS

Each word or term defined below that appears elsewhere in this section's wording, will commence in capital letters for easy identification that it is a defined word or term.

Computer Network: means one or more Computer Systems which are connected or otherwise able to exchange Data.

Computer Systems: means the information technology and communications systems (such as Hardware, Infrastructure, Software, or Electronic Media) used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying or transmitting Data.

Confidential Information: means any form of commercially sensitive business and/or trade secrets not publicly available, whether or not such information is marked as 'confidential'.

Continuing Standing Charges: means any fixed costs which continue to be payable in full by the Insured **during the Indemnity Period.**

Cyber Crime: means Theft of money from the Insured as a direct result of a Third Party's unauthorised electronic transfer from the Insured's bank account or alteration of Data on the Insured's Computer Systems where the Insured is unable to recover such sums.

Cyber Extortion: means any credible threat by a Third Party to cause a Defined Event to occur unless a Ransom is paid or any demand for a Ransom by a Third Party to end a Cyber Incident caused by the Third Party.

Cyber Incident: means Malicious Act, Malware, Human Error, DoS Attack, Theft of Data, having an impact on the Insured's Computer System or the Computer System of a Service Provider or a reasonable suspicion of the same.

Data: means any digital information, irrespective of the way it is used or displayed (such as text, figures, images, video or software) stored outside the random access memory.

Data Breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data or Confidential Information transmitted, stored or otherwise processed on the Insured's Computer Systems or the Computer System of a Service Provider.

Data Subject: means any identified or identifiable natural person who is the subject of Personal Data.

Directors and Officers: means any of the Insured's past, present or future directors, officers or senior

management.

DoS Attack: means any Malicious Act causing total or partial deprivation, disruption or unavailability of the Insured's Computer Systems or the Insured's Computer Network by an overloading stream of requests, including distributed denial-of-service attacks.

Electronic Media: means any information technology devices (such as external drives, CD-ROMs, DVD-ROMs, magnetic tapes or disks, USB sticks) that are used to record and store Data.

Employee: means any person performing services or providing labour for the Insured under an express or implied employment contract. This includes external staff hired by the Insured to provide services, working within the Insured's operational structure and under the Insured's functional authority. **This excludes Directors and Officers.**

Expert: means any person or legal entity appointed by or in consultation with the Company and/or the Incident Response Provider (such as a forensic accountant, lawyer or public relations consultant).

Hardware: means the physical components of any Computer Systems used to store, transmit, process, read, amend or control Data, including Electronic Media.

Human Error: means any negligent or inadvertent information technology operating error (such as the choice of Software to be used, a set-up error, or any inappropriate one-off operation) by an Employee.

Incident Response Provider: means AVeS Cyber Security (Pty) Ltd (Reg. No. 2001/028605/07) with telephonic contact details of **0861 000 373**.

Indemnity period: means the period starting after the Insured's Computer Systems commenced to be partly or wholly unavailable and **ending not later than ninety (90) days later.**

Infrastructure: means any communication equipment, air conditioning, uninterrupted power supply installations, standalone generators, frequency inverter units, transformers and any other facilities that are used to maintain the functioning of electronic facilities that support Computer Systems and Data.

Internet: means the worldwide public data network that allows the transmission of Data.

Internet Service: means services to enable the use of the internet, such as

1. Internet service providers responsible for the provision of Services, Hardware and technical equipment for accessing and use/operation of the Internet;
2. domain name system service providers;
3. other Internet and external network service providers responsible for Internet exchanges, Tier 1 network providers; and,
4. cable network, satellite and radio communication network operators.

Insured: means in addition to the Insured stated in the schedule, includes the Insured's Directors and Officers.

Insured's Computer Systems: means Computer Systems under the Insured's control owned, leased, licensed or hired by the Insured.

Interrupted Period: means the period of time commencing **after the Waiting Period**, during which the Insured's Computer Systems or the Computer Systems of a Service Provider continue to be partly or wholly unavailable and **ending on the earlier of**

1. **seven (7) days after the Insured's Computer Systems are wholly available again; or,**
2. **the end of the Indemnity Period.**

Legal Defence Costs: means any costs, expenses and/or fees for Experts, investigations, court appearances, arbitrations or other dispute resolution processes, surveys, examination and/or procedures that are necessary for the Insured's civil, commercial, administrative and/or criminal defence. **This does not include the Insured's general expenses (such as salaries and overheads).**

Malicious Act: means any unauthorised or illegal act intending to cause harm or to gain access to, or disclose Data from, Computer Systems or Computer Networks through the use of any Computer System or Computer Network.

Malware: means any unauthorised or illegal Software or code (such as viruses, spyware, computer worms, Trojan horses, rootkits, ransomware, keyloggers, dialers and rogue security Software) designed to cause harm or to gain access to or disrupt Computer Systems or Computer Networks.

North America: means the United States of America (being the 50 States of the Union plus the District of Columbia), Canada and any territory operating under the laws of or subject to the jurisdiction of courts of the aforementioned territories.

Online Media Activities: means any text, images, videos or sound distributed via the Insured's website, social media presence or e-mail.

Personal Data: means any information relating to a Data Subject, who can be identified, directly or indirectly, in relation to other information (such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person) as defined by any applicable data protection laws.

Ransom: means any money, bitcoins or other digital currency.

Reduction of Gross Profit: means an Expert's reasonable and documented projection of the net profit or loss before taxes the Insured would have earned, taking into account previous trading patterns and market conditions, plus any continuing Standing Charges, less any net profit the Insured actually earned (adjusted for any reasonable increased costs of working or cost savings made) **during the Interrupted Period.**

Service Provider: means any Third Party, except those providing electricity, satellite, cable, gas, water or other utility providers, telecommunications and Internet Services, that provides services pursuant to a written contract with the Insured.

Services: means any services for the processing, maintenance, protection or storage of the Insured's Hardware, Infrastructure, electronic Data or computer Software.

Software: means any digital standard, customised or individual developed program, or application held or run by a Computer System that comprises a set of instructions that are capable, when incorporated in a machine readable medium, of causing a machine with information processing capabilities to indicate, perform or achieve a particular function, task or result.

Supervisory Authority: means any supervisory authority, independent public authority, regulator, government organisation or statutory body authorised to enforce statutory obligations in relation to the control or processing of Personal Data in accordance with the Insured's respective applicable Data protection laws.

Terrorism: means any acts committed for political, religious, ideological or similar purposes, including the intention to influence any government and/or to put the public, or any section of the public, in fear.

Theft: means any Malicious Act of illegitimately copying or obtaining, for example, Confidential Information, Data or Personal Data, from Computer Systems.

Third Party: means any person or legal entity other than the Insured or Employees of the Insured.

Third Party Claim: means any demand or assertion by a Third Party against the Insured for damages or enforcement of a right before an administrative, arbitration, civil, commercial or criminal court.

Waiting Period: means the period of time as stated in the schedule commencing on a Cyber Incident which directly causes the Insured's Computer Systems to be partly or wholly unavailable.

LIMITS OF INDEMNITY

The total amount payable (inclusive of any costs, expenses, Legal Defence Costs as well as any payment made by the Company to the Incident Response Provider), for

1. **any claim or number of claims for any one event or series of events with one originating cause or source, will not exceed the Limit of Indemnity stated in the schedule against "Limit of indemnity (per event)";**
2. **all claims during any one (annual) Period of Insurance will not exceed the Limit of Indemnity stated in the schedule against "Limit of indemnity (per period of insurance)".**

In the event of any one originating cause giving rise to a claim or series of claims which form the subject of indemnity by more than one Defined Event under this Section, each Defined Event will apply separately and be subject to its own separate Limit of Indemnity **provided always that the total aggregate amount of the Company's liability shall**

be limited to the highest Limit of Indemnity available under any one of the Defined Events affording indemnity for the claim or series of claims.

Where more than one Period of Insurance of this Policy, following its renewal or replacement may apply to an originating cause or source, the Company's liability will be limited to the maximum Limit of Indemnity for any one such Period of Insurance.

SPECIFIC EXCLUSIONS

The Company will not be liable for any claim arising directly, or indirectly from, or contributed to by, the following:

1 **any Cyber Incident, Cyber Crime, Cyber Extortion or Data Breach occurring prior to the Retroactive Date stated in the schedule;**

2. **any Third Party Claim made in North America;**
3. **failure, interruption, degradation or outage of Infrastructure of a Third Party or Service Provider that is not under the Insured's control (including communications, Internet Service, satellite, cable, electricity, gas, water or other utility providers);**
4. **Terrorism;**
5. **strike, riot or civil commotion;**
6. **war, including any state of hostile conflict (whether declared or not) that is carried on by force of arms and/or violence to resolve a matter of dispute between two or more states or nations, including acts of war such as invasion, insurrection, revolution, military coup or cyberwar;**
7. **discharge, dispersal, seepage, migration, release or escape of hazardous substances, contaminants or pollutants;**
8. **seizure, confiscation, demand, destruction or damage to the Insured's Computer System, due to the action, requirement or order of any government, regulator, court or other body acting within its lawful authority;**
9. **use of illegal or unlicensed Software;**
10. **fault, defect, error or omission in design, plan or specification of the Insured's Computer Systems making them unfit for purpose;**
11. **the Insured's conduct which is malicious, dishonest, deliberate or reckless;**
12. **loss of or damage to tangible property and any losses that are consequential in nature, including the loss of use of tangible property;**
13. **if paying, insuring and/or providing any benefit to the Insured would result in the Company breaching any sanction, prohibition or restriction under United Nations or the trade or economic sanctions, laws or regulations of the European Union, Federal Republic of Germany, United Kingdom or the United States of America;**
14. **where the Insured has failed to take reasonable steps to co-operate with, or prevent the imposition of an order, instruction or directive by any Supervisory Authority arising directly or indirectly from a Defined Event;**
15. **fines, punitive damages or penalties of whatever nature** (this Specific Exclusion shall not apply to Defined Event 1.2 but only to the extent that cover is specifically provided thereunder);
16. **investment or trading losses including without limitation any inability to sell, transfer or otherwise dispose of securities;**
17. **scheduled downtime, planned outages or idle period of Computer Systems or parts of Computer Systems;**
18. **failure by the Insured or a Service Provider to make a payment due or renew or extend any lease, contract, licence, or order to supply goods or services;**
19. **bodily injury, psychological harm (other than distress), trauma, illness or death;**
20. **theft, breach or disclosure of intellectual property such as patents, trademarks, copyrights** (this Specific Exclusion shall not apply to Defined Event 4.3 Media Liability but only to the extent that cover is specifically provided thereunder);

21. **Third Party Claims made by or on behalf of: any legal entity with effective control over the Insured; any of the Insured's subsidiaries; any legal entity over which the Insured or the Insured's subsidiaries have effective control; any person holding a majority shareholding interest over the Insured; any legal entity in which the Insured has a financial interest, irrespective of amount; or any partnership or joint-venture to which the Insured is a party;**
22. **Services that a Service Provider has subcontracted to a Third Party;**
23. **any negligent or inadvertent information technology operating error by a Service Provider or its staff;**
24. **contractual liability which exceeds liability which would otherwise arise in the absence of such contract(s);**
25. **inaccurate, inadequate or incomplete description of any goods or services or their price;**
26. **ex gratia or discretionary settlements or gestures of goodwill for Third Parties including discounts, service credits, rebates, price reductions, coupons, prizes, awards or other contractual or non-contractual incentives, promotions or inducements;**
27. **publication on any website where content can be published without registration, or any website or content that is not directly controlled by the Insured;**
28. **failure to remove website or webpage data controlled by the Insured after receiving a complaint or request from a Third Party;**
29. **a. any Cyber Incident, Cyber Crime, Cyber Extortion or Data Breach reported to insurers of any other policy attaching to a period prior to the Period of Insurance;**
    b. any Third Party Claims made prior to the Period of Insurance; or
    c. any Cyber Incident, Cyber Crime, Cyber Extortion or Data Breach discovered by the Insured or that should reasonably have been discovered by the Insured before the Period of Insurance;
30. **negligent advice, design, specifications, formula or other breach of professional duty;**
31. **In-game currencies, crypto-currencies, reward points and air miles;**
32. **loss or theft of a Third Party's money or property in the Insured's care, custody or control;**
33. **that portion of any loss payable under Defined Event 2 that occurs during the Waiting Period.**

SPECIFIC CONDITIONS

1. Assignment

The Insured may not assign any legal rights or interests in this section without the prior written consent of the Company.

2. Claim reporting

General Condition 6.1.1 is cancelled and restated as follows:

It is a condition of this section that the Insured must as soon as reasonably practicable and at their own expense report in writing

2.1 any actual or suspected Data Breach, Cyber Incident, Cyber Extortion, or Cyber Crime which may result in a claim under this policy to the Incident Response Provider and the Company;

2.2 any Third Party Claim or circumstance which may give rise to a Third Party Claim to the Company.

3. Cancellation

If a claim has been reported to the Company, no pro-rata refund of premium will be repayable under this section upon cancellation of this policy or this section for the period from the effective date of the cancellation to the end of the period of insurance.

4. Confidentiality

The Insured must not disclose the existence of this policy except to senior management or professional advisers of the Insured or where under a legal obligation to do so or for tender purposes unless the Company has given its prior written consent. **The Company at its sole discretion, may decline to pay a claim for Cyber Extortion** or may cancel the cover immediately from the date that any such disclosure

is made that is in contravention to this Specific Condition.

5. First amount(s) payable

5.1 If the Company has directly indemnified any Third Party, the Insured must immediately reimburse the Company for the amount of the applicable First amount payable that was included in such indemnification; or

5.2 If the Company so requires, the Insured must pay the First amount payable directly to the Third Party to comply with any settlement;

5.3 If a single event (or events arising from the same original cause) results in a claim being payable under more than one Defined Event, only one First amount payable shall be payable by the Insured which will be the highest of the respective applicable First amounts payable reflected in the schedule. For the purposes of determining the First amount payable in terms of this Specific Condition, the uninsured amount under the Waiting Period of Defined Event 2 is deemed to be a First amount payable.

6. General Exclusions 3 (Computer losses) and 6 (Cyber exclusion)

The above General Exclusions will not apply to this section **but only to the extent that cover is specifically provided under the Defined Events of this section and not otherwise excluded by a Specific exclusion of this section or limited in any way by any other limiting provision of this section.**

7. Incident Service Provider claims process and services provided

7.1 The Insured must report the happening or suspected happening of a Defined Event to the Incident Service Provider as required by Specific Condition 2.1;

7.2 The Insured will receive acknowledgement of the reported incident;

7.3 The Insured will receive support and guidance through the incident management process until the incident is finalised;

7.4 The incident management and co-ordination function of the Incident Service Provider will create, track and monitor progress of all cyber security incidents, including communication between Public Relations and Legal organisations on behalf of the Insured;

7.5 Remote and onsite incident response will assist the Insured with technical incident response activities (off-site or on-site) to appropriately assess, remediate and handle the incident in consultation with the Insured;

7.6 The Incident Service Provider's Digital Forensics and Incident Response (DFIR) Services leverage extensive knowledge and experience as a trusted security advisor in the region to drive and support incident response activities during or following a cyber security incident;

7.7 The Insured will have access to the 24x7x365 Hotline for Cyber emergencies and general queries relating to this section;

8. Information disclosure

Any information supplied by the Insured or on behalf of the Insured (where by proposal form or otherwise) will be the basis of this section's contract of insurance. The Insured must notify the Company, as soon as reasonably practicable, of any material change in risk of which the Insured becomes aware or ought reasonably to be aware, including without limitation any acquisition by or of the Insured during the policy period. **The Company will not pay for any Defined Event resulting from any material change in risk unless the Company has agreed in writing to that material change in risk beforehand and received adequate additional premium as determined by the Company.**

The Company has recorded answers obtained to questions about the insured business and its processes and procedures relating to this section's cover. These are reflected in this section's schedule and the Insured is in terms of the requirements of this Specific Condition, specifically required to inform the Company in writing of any changes or inaccuracies in the reflected information.

9. Inspection and audit

The Company or any Experts or Company representatives may inspect and/or audit the Insured (including but not limited to the Insured's premises, records, Computer Systems or Computer Network) and/or as far as is possible, any Service Provider, at any reasonable time and during the period of insurance and up to one year of expiry or cancellation of this policy or this section of the policy. The Insured must provide all

relevant details and information that the Company may require.

10. Insured's obligations on the happening or suspected happening of a Defined Event

In addition to any requirements specified under General Conditions 6 and 7, it is a condition precedent of this section that the Insured:

10.1 must provide to the Company with evidence demonstrating the occurrence and description of the likely consequences of any Defined Event;

10.2 must take all reasonable and necessary measures to minimise the duration and effect of any Defined Event;

10.3 must do and permit to be done all such things as may be practicable to establish the cause and extent of the Defined Event;

10.4 must preserve any Hardware, Software and Data and make these available to the Company or the Incident Response Provider;

10.5 must comply with any reasonable recommendations made by the Company or the Incident Response Provider;

10.6 must not (without the Company's prior written consent), admit liability for, pay, settle or prejudice any Third Party Claim;

10.7 must assist the Company in investigating, defending and settling any Third Party Claim, and assist any lawyer or other Expert appointed by the Company on the Insured's behalf to defend the Third Party Claim;

10.8 at the Company's expense, co-operate with and assist the Company when required including providing information and securing the co-operation and attendance in court of witnesses employed by the Insured;

10.9 at the Company's expense, enforce any legal rights the Insured or the Company may have against any Third Party who may be liable to the Insured for a Cyber Incident, including giving the Company authority to bring court proceedings in the Insured's name against a Third Party and to settle those proceedings;

10.10 at the Company's expense, execute any documents that the Company requires to secure the Company's rights under this policy.

11. Law and jurisdiction.

This section will be governed by the laws of the Republic of South Africa whose courts will have jurisdiction in any dispute between the Insured and the Company.

12. Laws or regulations

If any provision of this section conflicts with the laws or regulations of any jurisdiction in which this policy applies, this section must be varied by the parties to comply with such laws or regulations. No indemnity is payable where such indemnity is illegal in terms of such laws or regulations.

13. Operation of cover

Cover under this section is conditional on the following:

13.1 Non Third Party Claims: The Defined Event must have occurred within the Territorial Limits and be first discovered by the Insured and reported to the Incident Response Provider and the Company during the period of insurance.

13.2 Third Party Claims: The claim must first be made against the Insured within the Territorial Limits during the period of insurance and reported to the Company during the period of insurance.

Any circumstance of which the Insured becomes aware of and reports to the Company during the period of insurance which results in a Third Party Claim will be deemed to have been reported and the Third Party Claim made during the period of insurance.

14. Other Insurance

General Condition 2 is cancelled and restated as follows: **The Company will not pay any claim if the**

Insured is covered for that claim by another insurance policy. It is a further condition of this section that the Insured may not insure any First amount payable or Waiting Period applicable under this section under any other insurance policy.

15. Severability

Any unenforceable provision of this section will not affect any other provisions and, if practicable, will be replaced with an enforceable provision with the same or similar intent as that unenforceable provision.

16. Variations

Other than as set out in General Condition 13, variations to this section require the prior written agreement of the parties.

17. Obligatory risk management services

It is a condition precedent of this section that the Insured:

17.1 activates the Obligatory Risk Management Services referred to in the schedule within 7 days of incepting cover under this section and remains so activated for the duration of the Period of Insurance;

17.2 takes all steps to comply with any reasonable risk mitigation action plans or alerts issued by the Obligatory Risk Management Services. In the event that the Insured does not comply with this clause 17.2, the Limit of indemnity shall be reduced to 80% of the amount reflected in the schedule.