1. BUI Security Services (Pty) Ltd ("BUI"), the provider of MXDR, provides you the Client a guarantee for a period of 12 (twelve) months from date of purchase that should one of the following incidents transpire:

   1.1. Network Security Breach

   1.2. Cyber Extortion Threat

2. This guarantee is valid only if the Client maintains active subscription to BUI's MXDR service throughout the 12-month warranty period, and adheres to all implementation, onboarding, and operational recommendations provided by BUI.BUI shall provide specialist services up to or pay up to a maximum cumulative guarantee as reflected on the Purchase Order.

3. BUI's obligations under this warranty are contingent upon the Client maintaining the specified security controls throughout the warranty period. Any failure to do so renders this warranty null and void.

4. This guarantee is provided for a period of 12 (twelve) months from the date of purchase of the guarantee, provided BUI is notified within 7 (seven) days of the Client becoming aware of the Network Security Breach or Cyber Extortion Threat.

   4.1. The Client has the following security controls implemented at the time of the Network Security Breach, Cyber Extortion Threat

      4.1.1. Endpoint Detection and Response (EDR) or equivalent modern threat detection tools must be deployed on all desktops, laptops, and Sensitive Systems, including real-time monitoring and reporting capabilities (all systems (including all hardware, software and physical components thereof and the data stored thereon) visible to external networks and/or used to store/process nonpublic, confidential, proprietary, or POPIA related information) running a Microsoft operating system and kept up to date as per the software providers' recommendations.

      4.1.2. Critical vulnerabilities (CVSS 9.0–10.0) must be remediated within 14 days of vendor release unless a documented exception exists. High severity (CVSS 7.0–8.9) within 30 daysof release by the provider.

      4.1.3. The following password controls implemented on Sensitive Systems:

         4.1.3.1. Password length of at least 8 (eight) characters.

         4.1.3.2. User account password configured to be changed at least every 120 (one hundred and twenty) days unless passwords are at least 14 (fourteen) characters in length or multi factor authentication is implemented. Passwords configured which cannot within reason be deemed weak or known e.g., including the Client's name or P@ssword1.

         4.1.3.3. User accounts configured to lockout because of at most 10 (ten) failed authentication attempts.

         4.1.3.4. The Client shall implement centralized password management solutions or identity protection solutions such as Microsoft Entra ID Protection or equivalent.

4.1.4. The following recovery controls:

4.1.4.1. Generate backups at least weekly or have replication implemented.

4.1.4.2. At any point in time have a backup or replicated copy which is disconnected, offline or cannot be overwritten from the production environment.

4.1.4.3. Test the ability to restore data from backups or read from replicated copies at least every six (6) months.

4.1.5. If the Client's Computer System includes a company network:

4.1.5.1. Firewalls configured to restrict access to digitally stored Sensitive Information.

4.1.5.2. All administrative/remote access interfaces (e.g., RDP, SSH) must not be exposed to the internet and must be accessed via secure Zero Trust solutions (ZTNA) or VPN using multi-factor authentication (MFA) at minimum.

4.1.5.3. The system and/or activity logs for all Sensitive Systems including firewalls and Active Directory as implemented in the Client's environment stored for a minimum period of 6 (six) months.

5. Limitations of Guarantee:

5.1. Network Security Breach means unauthorised access to, unauthorised use of, theft of data from or transmission of malicious code to the Client's computer system. Which shall be limited to the following reasonable and necessary costs and expenses incurred by the Client within one (1) year of notifying BUI of the Network Security Breach:

5.1.1. to restore, re-collect, or replace data, including expenses for materials, working time, and overhead cost allocation at the affected location associated with restoring or replacing data.

5.1.2. if it is determined that data cannot be restored, re-collected, or replaced, the actual costs incurred up to such determination.

5.1.3. of certified specialists, investigators, forensic auditors, or loss adjusters retained by BUI to conduct a review or audit to substantiate that a Network Security Breach is or has occurred, or to determine the scope, cause, or extent of any theft or unauthorised disclosure of information or data or Privacy Breach; and

5.1.4. all other reasonable and necessary costs and expenses incurred by the Client to contain the Network Security Breach

5.1.5. all other reasonable and necessary costs to comply with governmental privacy legislation or Guidelines mandating, or recommending as best practice, including but not limited to reasonable and necessary legal expenses, communication expenses through mail, call centre (for a period of up to 90 days unless otherwise required by applicable law, regulation or

agreed to by BUI and website, and customer support expenses including credit monitoring and identity theft education and assistance.

5.1.6. all reasonable and necessary expenses incurred by the Client and approved by the BUI within one (1) year of the Client notifying the BUI of the Network Security Breach, for retaining the services of a public relations consultant and for related advertising or communication expenses at the direction of said consultant, solely for the purpose of averting or mitigating any material damage to the Client's brand or reputation as a result of an actual Network Security Breach.

5.1.7. This does not include costs or expenses incurred by the Client to:

5.1.7.1. identify or remediate any software errors or vulnerabilities.

5.1.7.2. update, replace, upgrade, recreate or enhance any part of the Client's Computer System to a level beyond that which existed prior to the Network Security Breach, Cyber Extortion Threat or Internet of Things Damage Event;

5.1.7.3. research or develop any data, including but not limited to trade secrets or other proprietary information; or

5.1.7.4. establish, implement, maintain, improve, or remediate security or privacy practices, procedures or policies.

5.2. Cyber Extortion Threat means a credible threat or series of related threats, including a demand for funds or property, directed at the Client to intentionally damage, destroy or corrupt, introduce Malicious Code to, or commit a Theft of Data from the Client's Computer System. Which shall be limited to:

5.2.1. the lesser of 50% or the remaining balance of the guarantee for the funds or property paid by the Client with the prior written consent of BUI, to a person reasonably believed to be responsible for a Cyber Extortion Threat for the purpose of terminating such threat.

5.2.2. reasonable and necessary fees and expenses of the cyber extortion negotiator to investigate and determine the cause of and to end a Cyber Extortion Threat

5.2.3. all other reasonable and necessary expenses incurred by the Client, with the prior written consent of BUI within the guarantee period, as a direct result of a Cyber Extortion Threat. Provided the overall payment for the expenses and payment to terminate the Cyber Extortion Threat does not exceed the expenses the Client would have incurred had the payment for the expenses and payment to terminate the Cyber Extortion Threat not been paid.

5.2.4. Payment to terminate the Cyber Extortion Threat and for a cyber extortion negotiator will not be covered where this is deemed illegal in the jurisdiction where the Client or BUI has operations.