

ComplianceSuite™ Cyber Warranty

SAMPLE ONLY

National Warranty Provider:
Cyber Retaliator Solutions (Pty) Ltd.
info@smbsecure.co.za

What's Included

The following are general descriptions of what's included with the SMBsecure™ Cyber Warranty:

Data Breach

A data breach is an incident where sensitive, protected, or confidential data is accessed, disclosed, or stolen by unauthorised parties. This can include personal data like names, financial records, or company proprietary information. Data breaches often occur due to weak security controls, vulnerabilities, or malicious attacks, and can lead to reputational damage, legal liabilities, and significant financial losses for the affected organisation.

The Warranty includes Cash and Remediation limited to the maximum sum of R1,000,000.

The Warranty includes costs to respond to a systems security incident, including:

- to obtain professional (legal, public relations and IT forensics) advice, including assistance in managing the incident, co-ordinating response activities, making representation to regulatory bodies and coordination with law enforcement;
- to perform incident triage and forensic investigations, including IT experts to confirm and determine the cause of the incident, the extent of the damage including the nature and volume of data compromised, how to contain, mitigate and repair the damage, and guidance on measures to prevent reoccurrence;
- for crisis communications and public relations costs to manage a reputational crisis, including spokesperson training and social media monitoring;
- for communications to notify affected parties;
- for remediation services such as credit and identity theft monitoring to protect affected parties from suffering further damages.

Cyber Extortion

Cyber extortion is a form of cybercrime in which attackers gain unauthorised access to a victim's systems, data, or network and threaten to release, damage, or disrupt unless a ransom is paid. Cyber extortion typically includes ransomware attacks, where attackers encrypt critical data and demand payment to decrypt it. Such incidents can cripple business operations, resulting in financial losses, reputational harm, and in some cases, the loss of crucial data.

The Warranty includes Cash and Remediation limited to the maximum sum of R500,000.

Cash Payment: 50% of the ransom amount paid in cash, Costs to investigate and mitigate a cyber extortion threat.

Business Email Compromise

Business Email Compromise is the unrecoverable actual direct financial loss of money as confirmed by the relevant financial institution following the reasonable attempts for recovery, which belong to the business or for which the business is legally responsible, as a direct result of a Network Security Breach by a third party.

The Warranty includes Cash Payment limited to the maximum sum of R250,000.

Reimbursement for the unrecoverable actual direct financial loss of money.

Terms and Conditions

The following are the specific terms and conditions applicable to the **SMBsecure™** Cyber Warranty:

THESE PRODUCT-SPECIFIC TERMS AND CONDITIONS NEED TO BE READ IN CONJUNCTION WITH THE SMBSECURE GENERAL TERMS AND CONDITIONS. WHERE ANY DISCREPANCY OCCURS, THE PROVISIONS OF THESE PRODUCT-SPECIFIC TERMS AND CONDITIONS SHALL APPLY.

1. Definitions:

Capitalised terms not defined in these Service Terms shall have the meaning ascribed to it in the General **Terms**.

Warranty Provider is defined as Cyber Retaliator Solutions (Pty) Ltd (**CRS**) as national distributor of **SMBsecure™**.

- 1.1. **Business Email Compromise** means the unrecoverable actual direct financial loss of money as confirmed by the relevant financial institution following the **Client's** reasonable attempts for recovery, which belong to the **Client** or for which the **Client** is legally responsible, as a direct result of a **Network Security Breach** by a third party.
- 1.2. **Computer System** means any computer, communications system, server, cloud infrastructure, microcontroller, interconnected electronic, wireless, web, or similar systems (including all hardware, software and physical components thereof and the data stored thereon) used to process data or information in analogue, digital, electronic or wireless format.
- 1.3. **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:
 - 1.3.1. the lesser of 50% or the remaining balance of the Warranty for the funds or property paid by the **Client** with the prior written consent of WARRANTY PROVIDER, to a person reasonably believed to be responsible for a **Cyber Extortion Threat** for the purpose of terminating such threat.
 - 1.3.2. 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**
 - 1.3.3. all other reasonable and necessary expenses incurred by the **Client**, with the prior written consent of WARRANTY PROVIDER within the **Warranty 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. (In other words, the Cyber Warranty will not cover costs that end up being more expensive than just dealing with the damage caused by the threat. This is to ensure that the solution to the problem is cost-effective).
 - 1.3.4. 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 WARRANTY PROVIDER has operations.
- 1.4. **Malicious Code** means software designed to infiltrate or damage the **Client's Computer System** without the **Client's** consent.
- 1.5. **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 WARRANTY PROVIDER of the **Network Security Breach**:
 - 1.5.1. 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.
 - 1.5.2. if it is determined that data cannot be restored, re-collected, or replaced, the actual costs incurred up to such determination.
 - 1.5.3. of certified specialists, investigators, forensic auditors, or loss adjusters retained by WARRANTY PROVIDER 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; and

- 1.5.4. all other reasonable and necessary costs and expenses incurred by the **Client** to contain the **Network Security Breach**
- 1.5.5. 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 WARRANTY PROVIDER and website, and customer support expenses including credit monitoring and identity theft education and assistance.
- 1.5.6. all reasonable and necessary expenses incurred by the **Client** and approved by WARRANTY PROVIDER within one (1) year of the **Client** notifying WARRANTY PROVIDER 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**.
- 1.5.7. This does not include costs or expenses incurred by the **Client** to:
 - 1.5.7.1. *identify or remediate any software errors or vulnerabilities.*
 - 1.5.7.2. *update, replace, upgrade, recreate or enhance any part of the **Client's Computer System** to a level beyond that which existed prior to the **Warranty Event**;*
 - 1.5.7.3. *research or develop any data, including but not limited to trade secrets or other proprietary information; or*
 - 1.5.7.4. *establish, implement, maintain, improve, or remediate security or privacy practices, procedures or policies.*
- 1.6. **Warranty Period** means 12 (twelve) months from the Cyber Warranty's purchase date, or cancellation of PRODUCT WARRANTY IS ASSOCIATED TO whichever is shorter.
- 1.7. **Warranty Event** means a **Network Security Breach**, **Cyber Extortion Threat**, or **Business Email Compromise** as cyber incidents provided for by the SMBsecure Cyber Warranty.

2. Service description:

- 2.1. WARRANTY PROVIDER, the provider of SMBsecure provides you, the **Client**, a Warranty for the **Warranty Period** that a **Warranty Event** transpire, WARRANTY PROVIDER shall provide specialist services up to or pay up to a maximum cumulative Warranty as reflected on the Sales Order Form.

3. Warranty conditions:

- 3.1. This Cyber Warranty is provided for the **Warranty Period**, provided WARRANTY PROVIDER is notified on the Cyber Warranty hotline number +27 12 023 1959 or +27 72 266 2599 or email info@smbsecure.co.za within 7 (seven) days of the **Client** becoming aware of the **Warranty Event**.
- 3.2. The Cyber Warranty shall only be payable:
 - 3.2.1. Should the **Client** have selected the SMBsecure Product option on the Sales Order Form; and
 - 3.2.2. have active and up to date SMBsecure implemented at the time of the **Warranty Event**;
 - 3.2.3. have minimum stated cyber controls in-place.

4. Client service and support:

- 4.1. Where the **Client** raises a valid request for Cyber Warranty reimbursement, the WARRANTY PROVIDER Cyber Incident Response process will be followed.

5. Ownership

- 5.1. The **Client's** rights are limited to those stated or incorporated by reference in this Product Terms and the General Terms and Conditions.
- 5.2. WARRANTY PROVIDER and its third-party providers retain all ownership and other rights and interests in, and to the tools and technologies that WARRANTY PROVIDER uses in its Cyber Incident Response Handling and containment services, including underlying intellectual property rights, equipment, licences, equipment, as well as any systems comprising of those as mentioned earlier.

6. Data Protection

- 6.1. The **Client** owns and controls all rights, title and interest in all cyber incident reports, forensic data and related information generated by WARRANTY PROVIDER arising from a **Warranty Event**.
- 6.2. WARRANTY PROVIDER will use and process the cyber incident reports, forensic data and related information solely to the extent necessary for the performance of the Cyber Incident Response Handling.
- 6.3. Cyber incident reports, forensic data and related information may be retained and disclosed by WARRANTY PROVIDER as required to comply with applicable laws, regulations, subpoenas or court orders. Where allowed by law, WARRANTY PROVIDER will provide reasonable prior written notice to **Client** to permit **Client** to seek a protective order and will cooperate in **Client's** activities under this paragraph at the **Client's** expense. With written authorisation from the **Client**, WARRANTY PROVIDER will disclose only information reasonably necessary to meet the applicable legal order or requirement.

7. Client Obligations

- 7.1. **Client** agrees that during the provision of the Cyber Incident Response Handling to **Client**, WARRANTY PROVIDER or appointed service providers, investigators and affiliates will be granted required authorised access to the **Client's** IT environment to contain and investigate the cyber security incidents and threats.

8. Disclaimer:

- 8.1. Without limiting WARRANTY PROVIDER express obligations under these product terms, WARRANTY PROVIDER hereby disclaims all warranties, conditions and representations, express, implied, statutory or otherwise, concerning any other Cyber Security Service, software, documentation or other materials unrelated to this Cyber Warranty, including but not limited to, those implied warranties of merchantability, satisfactory quality, fitness for a purpose, and non-infringement. WARRANTY PROVIDER does not represent that the Cyber Warranty Service will be uninterrupted, error-free, or meet customer requirements.

FAQ

The following provides answers to some frequently asked questions (FAQ) to help you to understand some key aspects of the SMBsecure™ Cyber Warranty:

1. General Information

1.1. What geographical region does the warranty cover? *This warranty only applies to clients domiciled in South Africa. However, if a system/user with SMBsecure installed is located outside of South Africa and experiences a warranty event, the warranty will remain in effect.*

1.2. How do I know who the service providers are?

Service providers will be appointed from an approved list of service providers, updated from time to time. A list will be made available at the point that the warranty event occurs.

2. Warranty Incidents

2.1. Is there a limit on the number of warranty incidents?

Warranty payments will be limited to the maximum warranty amount.

The warranty amount is reduced by each reimbursement paid during the warranty period. If multiple cyber incidents occur and the total reimbursements exceed the warranty amount, no further reimbursements will be made. Refer to Clause 1.3 in the Warranty T&Cs for more details.

2.2. When does the Warranty limit reset?

The warranty is valid for 12 months. The limit resets when a new warranty is activated.

2.3. Is there a limit per warranty event?

No, there is no limit per warranty event. However, there is a maximum warranty amount set per module (e.g., Data Breach, Cyber Extortion, Business Email Compromise).

2.4. What is the Cyber Warranty Activation Date?

The activation date is the date the warranty is initiated as per the SMBsecure Cyber Warranty order fulfilment process.

2.5. How long is the warranty period?

The warranty period is 12 months from the Cyber Warranty Activation Date.

2.6. Is the warranty period a rolling 12 months from the current subscription month?

No, the warranty period is 12 months from the date of purchase and is annually renewable.

3. Limitations and Conditions

3.1. Non-payment will render the warranty null and void.

How To Request Reimbursement

The following provides details about how to request reimbursement from the SMBsecure™ Cyber Warranty:

Lodge a warranty reimbursement request with your SMBsecure™ Authorised Service Partner (ASP). The ASP will in-turn contact Cyber Retaliator Solutions (CRS) – the national distributor of SMBsecure™ and Warranty Provider who will review that warranty conditions have been met and that the Cyber Warranty is not voided, prior to commencing with any reimbursement processing.

Notify your SMBsecure™ ASP and/or contact the CRS Cyber Warranty hotline number +27 12 023 1959 or +27 72 266 2599 or email [info@smbsecure.co.za](mailto:info@ smbsecure.co.za) within 7 (seven) days of you becoming aware of the **Warranty Event**.

Where a cash benefit is applicable, cash benefit to be paid by CRS within 30 days of a successful reimbursement from the underwriters.

Any queries, complaints or concerns pertaining to the SMBsecure™ Cyber Warranty can be submitted by emailing info@smbsecure.co.za or by directly contacting your SMBsecure™ ASP.

DISCLAIMER: Cyber Retaliator Solutions (Pty) Ltd. will not be held liable for reimbursement not covered by this warranty or should the underwriter or upstream provider not reimburse for any reason. All technical implementations and cyber security minimum controls are the sole responsibility of the warranty customer which can be managed / implemented on-behalf of the warranty customer by authorised managed service partners (SMBsecure ASP).

PRINT THIS PAGE, COMPLETE FULLY AND ATTACH TO YOUR WARRANTY REIMBURSEMENT REQUEST(S)!!!!

Minimum Cyber Controls

The following is checklist of the minimum cyber security controls required to be in-place (implemented) on the affected system or SaaS Portals or by the affected person prior to a Cyber Warranty Event:

Review all requirements regularly to ensure warranty event requirements are met.

- Did you have anti-virus and/or anti-malware software implemented on all desktops, laptops, and Sensitive Systems (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 non-public, confidential, proprietary, or POPIA related information) running a Microsoft operating system and up to date as per the software providers' recommendations?
 - Yes
 - No
- Did you have Critical, Common Vulnerability Scoring System (CVSS) severity 9.0-10.0, security related patches and updates applied on Sensitive Systems within 1 (one) months of release by the provider?
 - Yes
 - No
- Did you have the following password controls implemented on Sensitive Systems:
 1. Password length of at least 8 (eight) characters?
 - Yes
 - No
 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?
 - Yes
 - No
 3. Passwords configured which cannot within reason be deemed widely used or easily guessable e.g., including the Client's name or P@ssword1?
 - Yes
 - No

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

- Yes
- No

○ Did you have the following recovery controls in place at the time of the cyber event:

1. Backups generated at least weekly or have replication implemented?

- Yes
- No

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

- Yes
- No

3. Testing of the ability to restore data from backups or read from replicated copies at least every six (6) months?

- Yes
- No

○ If your computer system includes a company network, did you have the following in place at the time of the cyber event:

1. Firewalls configured to restrict access to digitally stored sensitive information?

- Yes
- No

2. Administrative/remote access interfaces such as Remote Desktop Protocol (RDP) are not accessible via the open internet. Where such interfaces are required, these are accessible exclusively over secured channels such as Zero Trust Network Access (ZTNA), Multi-factor authentication (MFA) or Virtual Private Network (VPN) connections?

- Yes
- No

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 1 (one) month?

- Yes
- No

○ Did you have email security protocols implemented for your email domain at the time of the cyber event:

1. Domain-based Message Authentication, Reporting, and Conformance (DMARC)?

- Yes
- No

2. Mail Transfer Agent Strict Transport Security (**MTA-STS**) to enforce Transport Layer Security (**TLS**) encryption for email transmission between servers, preventing interception and ensuring secure communication?

Yes

No

○ Did you have data encryption and access control (quarantine or lockout) measures in-place for any lost, stolen or compromised devices holding sensitive data on computers, USB storage drives or mobile devices in place at the time of the cyber event?

Yes

No

○ Did you provide sufficient cyber awareness training to computer users and have a cybersecurity awareness training program in place at the time of the cyber event?

Yes

No

○ Did you provide an option for users to confirm recipients when sending emails which contain sensitive data to avoid such emails being sent to the wrong people at the time of the cyber event?

Yes

No

○ Did you provide an option for users to encrypt and password protect correspondence which contain sensitive data to prevent unauthorised access during transit or when such correspondence is stored on recipient devices at the time of the cyber event?

Yes

No

Checklist Completed By:

FULL NAME :

JOB TITLE :

CONTACT EMAIL ADDRESS :

CONTACT MOBILE NUMBER :