digi CARE

Warranty Terms & Conditions

Warranty Summary

Welcome to a world where you can **Live Free**.

Under these terms and conditions, the Digimune DigiCare warranty guarantees the integrity of its cybersecurity products and the ability of these products to prevent cybercrime, fraud and identity theft against you, the end-user.

Subject to the terms and conditions below, you are protected against:

Hacking-Inflicted Device Damage

In the event that your electronic device is hacked during a cyberattack, we will provide technical support to rectify and restore your electronic device up to the value stated in the DigiCare Warranty Certificate.

If we are unable to repair your device, we will replace it with a similar make and model up to the value stated in the DigiCare Warranty Certificate.

Cyber Extortion

In the event that you are a victim of a cyber extortion attack, we will provide you with technical support.

If the attack can be stopped without paying the extortion amount, we will provide indemnification up to the value stated in the DigiCare Warranty Certificate to restore your electronic device.

If it becomes apparent that the extortion amount needs to be paid to unlock your electronic device, we will indemnify you for the amount you pay up to the value stated in the DigiCare Warranty Certificate, subject to approval from us.

Loss of Funds

In the event that an unauthorised third party gains access to your protected device and obtains stored information, which enables the hacker to cause financial loss to you, you are covered under this warranty.

The onus lies with you to proof that the loss of funds was caused by the failure of the Digimune protection software.

Examples of loss of funds, where an unauthorised third party has obtained access to the device, by way of a hack, includes:

- EFT / Online Banking Fraud, where the hacker either transfers funds remotely frothe protected device or obtains security details from the protect device and made EFT's using this information.

- Online Shopping Fraud, where the hacker either made purchases remotely from the protected device or obtained security details from the protect device and has made purchases using this information.

Policy Definitions

In this policy, wording is defined as follows:

- **We / Us / Our:**
  Digimune (Pty) Ltd. – an authorised distributor of cybersecurity software products and services outlined within this agreement

- **You / Your / Yours:**
  The end-user who purchased the approved software from Digimune

- **Cybersecurity Software Product:**
  Any approved product sold to you by Digimune

- **Warranty:**
  These terms, together with the DigiCare Warranty Certificate

- **DigiCare Warranty Certificate:**
  The certificate(s) annexed to this agreement, including any other certificates which may, at any time hereafter, whether in substitution for or in addition to the existing schedules, be annexed to this agreement

- **Digital System:**
  Your digital system, including desktop, laptop, smart phone or other devices used by you to access your data, information or digital money.

- **Digital Identity:**
  Your name, address, identification number, bank or credit card account number – any information relating to, or method of, your personal identification that is accessible online via a computer device on which Digimune software is installed

- **Keys to Digital Identity:**
  Include any online device security, such as a password, a passphrase, a Personal Identification Number (PIN), OTP (One time PIN), username, account number, or any other authentication method used to control, restrict and / or allow access to your money

- **Hacking Incident:**
  Any electronic attack of a malicious or unauthorised nature, initiated by a third party, with the intention or purpose of disrupting, disabling, damaging, destroying, altering, encrypting, overloading, or interfering with the device or software systems or records, or destroying the integrity of the data or stealing controlled information

- **Digital Identity Theft:**
  Includes, but is not limited to, the fraudulent use of your personal identity to establish credit accounts, secure loans, enter into contracts or commit crimes

- **Cyber Extortion:**
  A crime involving a hacking incident or threat, coupled with a demand for money or some other response in return for stopping or remediating the attack – via malicious activity, such as ransomware or distributed denial-of-service (DDoS) attacks, to steal data and threaten to expose it

- **Money:**
  Varying amounts of currency that is stored in a digital account and used for digital payments, e.g. credit / debit card payments, app payments, online songs, electronic funds transfer (EFT)

- **Financial Loss:**
  Any loss where money was stolen

- **Funds Transfer:**
  Online money transfer from the end-user to a third party account

- **Bank:**
  Any bank, savings, association, credit union, or any other person or business that directly holds your money. The bank typically issues keys to your digital identity (e.g. a PIN code) to access and enable online money transfers.

- **Cancellation Date:**
  The date on which benefits payable under this agreement are no longer available to you

Cover Terms

This warranty is solely applicable to our cybersecurity software products that were purchased from us and installed on your device, by you, for the sole purpose of preventing cybercrime.

Under the terms of this warranty, we guarantee the integrity of our cybersecurity products and the ability of these products to prevent cybercrime against yourself.

The warranty further commits, at our option and discretion, to re-instate, repair, replace, negotiate, and pay on your behalf, or reimburse you for damage caused by a hacking incident or cyberextorsion event due to cybercrime, subject to the following terms and conditions:

- The approved cybersecurity software products purchased by you are installed, with the latest update, and used in the appropriate manner, as per the operation manual.
- If approved cybersecurity software products, when used as specified, fail to prevent cybercrime, we will compensate you for claims made according to the terms set out in this warranty.
- This warranty only covers events where you are a natural person who used your own personal or company-allocated digital system when the loss occurred.
- If a company-allocated digital system was used, you must prove that your company device was installed with a licensed cybersecurity software product purchased from us, and that the product has been updated according to the manufacturer recommendations and instructions, at the time of the incident.

Exclusions

Please note the following is not covered in terms of this warranty:

- If you are not a natural person
- Where your digital operating system is not up to date or in line with the requirements of the version of the cybersecurity software products purchased from us
- Any claim against loss, due to the use of unlicensed software

- Claims submitted after 31 days of the alleged hacking incident
- Claims for identity theft of any kind
- Any form of financial loss, other than Loss of Funds as described and covered by this warranty
- Claims for interest, damages, third party claims, fees incurred, and other costs that may be a consequence of the alleged hacking incident or cyberextorsion event
- Claims made where you have deliberately or inadvertently shared or given your digital identity and / or “keys” (login details) to any third party, irrespective of the reason, including (but not limited to) phishing, vishing and splicing scams
- In-store (e.g. shop) and other card transactions not originating from your digital system
- Currencies or accounts such as the Bitcoin ledger or other crypto-currency ledgers, that store digital value, but are not a registered bank
- Where you or members of your immediate family or a joint account holder has a past criminal record or history of fraud
- When your government or quasi-government takes claimants money for whatever reason (or as part of war-like acts and military uprisings, terrorist activities, or syndicated online fraud schemes)
- We do not cover you in the event of personal fraud, dishonesty, misrepresentation or wilful acts. You will lose all rights to claim under this warranty if:
    - You, or anyone acting on your behalf, uses any fraudulent means to obtain any benefit under this warranty
    - A claim occurs due to a deliberate, or wilful / intentional act committed by you, or with your involvement or anyone acting on your behalf

- Information or documents in support of a claim, whether created by you or on your behalf, is not true, is not complete, or is fraudulent

- The quantum of a claim is deliberately exaggerated by you, or anyone acting on your behalf

Compensation

For any claim to be considered, you must provide us with evidence that you suffered a loss in terms of this warranty, and proof that you have not been compensated for the loss.

This also means that you could never be compensated twice for the same event. Similarly, if a covered event is covered by two different warranties, we will pay only our portion of it.

- You cannot claim more than the actual loss. We will never pay more than the value of the actual claim / loss, or the stated benefit, whichever is lesser – even if you are over insured.

- You cannot claim more than the benefit limit. The compensation will be based on the maximum benefits, as noted in the DigiCare Warranty Certificate.

Claim Procedure

- **Step 1: Inform Us**
  Inform us, as soon as possible, of an incident that could lead to a claim, within 31 days after the event. Give us all the relevant details.

- **Step 2: Inform Police**
  Inform the police immediately, within 24 hours, after the event that led to the claim.

- **Step 3: Supply Supporting Information**
  If you haven't already dealt with this when you first reported the claim, please ensure that you send us the claim form within 31 days including:
  - Full written details of the claim (on our standard forms, if required)
  - Any other documentation we think is necessary to handle the claim (such as police documents, receipts, invoices)
  - Proof of value and insurable interest, if required by us

- **Step 4: Assist with Any Legal Proceedings**
  Your assistance will be required should we decide to start legal proceedings against any party responsible for the loss or damage. Note that any such legal action may be taken in your name.

- **Step 5: Sign Release**
  You may have to sign a release before we will compensate you.

Unless we specifically offer to pay or make provision for payment, the entire claim procedure above is done at your own expense.

General Terms

- You must be a citizen of the Republic of South Africa to have cover under this warranty. The cover under this warranty is for the worldwide use of your devices.
- This warranty is subject to South African law. If any of the terms or conditions of this warranty are in breach of existing legislation, they will be amended, so to comply with South African law.
- This agreement is attached to the insured as noted on the DigiCare Warranty Certificate. The agreement may not be transferred.
- You must make sure that all the information you give us about yourself, and yourrisk profile, is accurate.
- You must take reasonable steps to prevent any loss or damage, or we may not compensate you for any loss.
- Your fees must reach us on time. All fees are payable in advance, before the warranty incepts. No claims will be covered during a period of non-payment of fees.
- We reserve the right to cancel this warranty, with immediate effect, should we find material facts that could influence our ability to provide cover under this warranty – such as misrepresentation or financial enrichment. We will give you 31 days written notice, if we want to change the conditions of this warranty.

Processing & Protection of Personal Information

Your privacy is of the utmost importance to us. We will take the necessary measures to ensure that all information, including personal information provided by you, or which is collected from you, is processed following the provisions of the Protection of Personal Information Act 4 of 2013 and is stored safely and securely.

You hereby agree to give honest, accurate, and up-to-date personal information, and to maintain and update such information when necessary.

The information you provide to us will be stored on databases and shared with other parties in the industry to gather industry statistics, improve the quality of risk assessment, and combat fraudulent claims. It is important to understand that this information will remain at the disposal of these parties, even after your warranty with us ends.

You accept that your personal information may be used for the following reasons:

- To establish and verify your identity in terms of the Applicable Laws
- To enable us to fulfil our obligations in terms of this warranty
- To enable us to take the necessary measures to prevent any suspicious or fraudulent activity, in terms of the Applicable Laws
- Reporting to the relevant regulatory authority / body, in terms of the Applicable Laws

We may share your information for further processing with the following third parties, which third parties must keep your personal information secure and confidential:

- Payment processing service providers, merchants, banks, and other persons that assist with the processing of your payment instructions
- Law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime
- Regulatory authorities, industry ombudsmen, governmental departments, local and international tax authorities, and other persons that we, following the Applicable Laws, are required to share your personal information with
- Credit Bureaus
- Our service providers, agents and sub-contractors that we have contracted with to offer and provide products and services to any customer in respect of this warranty
- Persons to whom we cede our rights or delegate our authority to in terms of this warranty

You acknowledge that any personal information supplied to us, in terms of this warranty, is provided according to the Applicable Laws. Unless consented to by yourself, we will not sell, exchange, transfer, rent or otherwise make available your personal information to any other parties and you indemnify us from any claims resulting from disclosures made with your consent.

You understand that if we have utilised your personal information contrary to the Applicable Laws, you have the right to lodge a complaint with us within ten days. Should we not resolve the complaint to your satisfaction, you have the right to escalate the complaint to the Information Regulator.

For any queries relating to this document
please contact us via the details below.

SOUTH AFRICA
Workshop 17
32 Kloof Street
Cape Town
8001

t: +27 (0) 11 463 1309

general enquiries: connect@digimune.com
support: support@digimune.com
claims: claims@digimune.com

UNITED KINGDOM
C/O Haggards
Heathmans House
19 Heathmans Road
London
SW6 4TJ