Security Policy

June 2022 | Version 1.0

Callouts like this are a summary of our security policy and contain the most important and relevant points for you. Please read the full security policy because it applies to you.

Introduction

There is no such thing as 'perfect security'. We have to create a balance between increased levels of security and making transacting with us convenient to you.

Our security responsibilities

We will ensure that:

- We host our website in a secure server environment that uses a firewall and other advanced security measures to prevent interference or access from outside intruders.
- The information you give to us that is stored on or passes through our systems is protected. Encryption is used to protect the personal information you give us where it is appropriate.
- The links from our systems to systems under the control of third parties (for example our payment gateway) are secure.
- We perform regular backups of data to ensure it can be recovered in the case of a disaster.
- We log all access to our system. If any unauthorised behaviour should occur, this will assist us in identifying and resolving the issue.
- We take reasonable steps to secure your payment information and use a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of the transaction concerned.

We are responsible for hosting our website securely, protecting your information you give us, securing our links, backing-up our data, logging access, and taking reasonable steps to secure payment information.

Our security disclaimers

Please note the following:

- The third parties whose systems we link to are responsible for the security of information while it is collected by, stored on, or passing through the systems under their control.
- We will use all reasonable endeavours to ensure that our website and your information is not compromised. However, we cannot guarantee that no harmful code will enter our website (for example viruses, bugs, Trojan horses, spyware or adware). You should be aware of the risks associated with using websites (addressed below).
- If you experience a problem or loss that is caused by: (i) information you provided to us; (ii) your computer being compromised in some way; (iii) or by something beyond our control.

Email: **support@michalsons.com** | Phone: 086 011 1245

We cannot take responsibility for causing the problem. We will, however, do our best to help you if we can.

Your security responsibilities

Recommended steps

You should:

- Install and activate appropriate security software on your computer. This should include anti-virus, anti-spyware and anti-spam software.
- Run regular scans of your computer for viruses.
- Update your security software to ensure you are always running the current version.

You should have security software on your computer, scan it regularly, and keep the software up-to-date.

Additional steps

Other steps you should take to help protect your computer include:

- Check your Internet browser's security settings for ways to make your browsing more secure.
- Make sure that you have entered secure pages when filling in your sensitive personal information. Look for a small yellow lock commonly seen at the bottom right of your browser and http changes to https on the address bar.
- Log out after you have transacted electronically.

You should also keep your Internet browser secure, only enter sensitive personal information on secure pages, and log out.

Protecting your password

You should:

- Never share your password with anyone.
- Never send your password via email.
- Make your password as strong as possible.

Credit card information

Safe and secure

Transacting with us electronically (including transacting and using your credit card on our website) is safe and secure. It is much the same as transacting in person face-to-face.

Payment processing

We do not get involved in any credit card transactions directly. All credit card transactions are handled or acquired for us via Paygate who are the approved payment gateway for our bankers ABSA. No credit card details are stored on our website. Paygate uses the strictest form of encryption, namely Secure Socket Layer 3 (SSL3). You may go to ${payment_gateway_website_URL} to view their security certificate and security policy.

Payment verification

A Certificate Authority (or CA) ${certificate_authority_hyperlink} checks, verifies, and certifies our service provider's company registration documents and domains to ensure that nobody can impersonate them to obtain your payment Information.

Secure URL

Once you begin the checkout process you will notice that the site URL will change from "http" to" https" and a small padlock will appear at the bottom of your screen. This is indicative of a secure Internet transaction.

Verification programs

We do not currently support the Verified by Visa program [insert hyperlink - https://usa.visa.com/personal/security/vbv/index.html] or the MasterCard SecureCode [insert hyperlink - http://www.mastercard.com/us/personal/en/cardholderservices/securecode/index.html]. You can still use your Visa or MasterCard credit card as payment for an order, but we will not ask you to enter your Verified by Visa password or MasterCard SecureCode.

Phishing

Secure URL

You must only log in to your account from a page that begins with https://www.identipet.com.

No confirmation through links

We will never ask you to confirm your username and password or other sensitive information by clicking on any links in an email other than the email link we send you at registration to verify your email address. Be aware of "phishing" attacks where criminals attempt to obtain your sensitive information by sending you an email, masquerading as an email from us, asking you to access your account or verify information via links in the email, or diverting you to a fake Identipet website. Please report any suspected phishing attacks to us immediately to prevent any harm to you or other users.

We will not generally ask you to confirm your personal information through links. If someone does, it may be a phishing attack.

Contact us

Please report any suspicious or unauthorised activity relating to your use of our website to us directly, because it will help make our website as secure as we can.

Our right to take action

We reserve the right to take whatever action we may deem necessary at any time to preserve the security and reliable operation of our system. You undertake not do (or permit anything to be done) that may compromise the system under our control.

Email: **support@michalsons.com** | Phone: 086 011 1245