Security Policy

1. 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. This includes using your credit card on our website (see below).
- the links from our systems to systems under the control of third parties (for example our payment gateway) are secure.
- regular backups of data are performed to ensure it can be recovered in the case of a disaster.
- all access to our system is logged. 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.

2. Please note the following disclaimers:

- We are governed by the laws of the Republic of South Africa
- 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 information you provided to us, your computer being compromised in some way or by something beyond our control, we cannot take responsibility for causing the problem. We will, however, do our best to help you if we can.

3. You are responsible for your own internet security

- 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.

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 credit card details. Look for a small yellow lock commonly seen at the bottom right of your browser and http changes to https on the address bar.
- Sign out after you have transacted electronically.

4. You should:

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

5. Credit card information

5.1 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.

5.2 Payment processing. We do not get involved in any credit card transactions directly. All credit card transactions are handled or acquired for us via Virtual Card Services who are the approved payment gateway for our bankers, Standard Bank. No credit card details are stored on our website. Virtual Card Services uses the strictest form of encryption, namely Secure Socket Layer 3 (SSL3). You may go to http://website.vcs.co.za/customer-info/general-security/ to view their security certificate and security policy.]

5.3 Payment security. All payers' credit card details are secured by secure sockets layer ("SSL") encryption whilst in transmission and reinforced through various encryption processes in order to provide protection for all sensitive payment information. We do not access any of the credit card details. These are encrypted and stored in our secure Payment Card Industry ("PCI") environment. When required for purposes of a transaction between you, as a merchant, and a payer, we retrieve and forward encrypted credit card details to you. You never access or store any payer's credit card details.

5.4 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.

6. Phishing

6.1 Secure URL. You must only log in to your account from a page that begins with: https://

6.2 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 AfriCanyon website. Please report any suspected phishing attacks to us immediately to prevent any harm to you or other users.

7. Contact us

You must report any suspicious or unauthorised activity relating to your use of www.knysnaribadventures.co.za by contacting info@knysnaribadventures.co.za. This will help make us as secure as we can.