SECURE CITIZEN PRODUCT TERMS

Terms and Conditions

We welcome you as a user of this web – based application and/or mobile application and any services which may be provided in respect of such application (the "Secure Citizen Application") or other products or services provided via this website or its applications. We are providing the Secure Citizen Applications and any services to you, subject to these Product Terms, the Terms of Use, the Privacy Policy and the Subscriber Agreement for digital signing (collectively known as the "Terms").

These Product Terms will provide you with an explanation of the various features which are available as part of the Secure Citizen Application. These Product Terms are also intended to inform you about the personal information which will be collected, stored and utilised as part of the Secure Citizen Application.

The Terms, as may be amended from time to time shall be effective from the date on which you first access and/or use the Secure Citizen Application and govern both the online and offline access to and use of the Secure Citizen Application or any part thereof and related services for new and existing users.

These Terms provide legal protection for Secure Citizen, the Southern African Fraud Prevention Service ("SAFPS") and any other party who may provide a license in respect of the Secure Citizen Application or other products or services, including OneVault (Proprietary) Limited and Contactable (Proprietary) Limited and/or any other third party licensors and platform service providers (''the Licensors"); the Secure Citizen Application's content suppliers; and any subsidiaries of such parties (collectively known as "the Companies").

To the extent that any provisions of the Terms could or are intended to create or confer any benefits, rights or remedies on any one or more of the Companies, each of such Companies shall be a beneficiary or third party beneficiary thereto and shall at any time be entitled to accept and enforce any such benefits, rights or remedies as conferred upon it under the Terms.

The purpose of collecting, storing and verifying your personal information is to provide you with a Protective Registration and/or to certify and confirm your status as a Secure Citizen and to assist in the prevention of fraudulent incidents. Any personal information which is collected and stored on the Secure Citizen Application will be stored on the Secure Citizen Application itself and not on your mobile device. We will utilise your Personal Information for the purposes as set out in the Terms, for any other lawful purpose and for any other purpose for which you may provide your consent from time to time.

Consent and Agreement

The Terms apply to your use of the Secure Citizen Application and any related services. Please ensure that you have read and understand the Terms before accessing the Secure Citizen Application.

BY ACCESSING, USING AND/OR BROWSING THE SECURE CITIZEN APPLICATION AND ANY RELATED SERVICES:

- **YOU UNDERSTAND, ACCEPT AND AGREE TO THE TERMS;**
- **YOU CONSENT TO THE COLLECTION, STORAGE, USE AND TRANSFER OF YOUR PERSONAL INFORMATION, WHICH MAY INCLUDE YOUR BIOMETRIC INFORMATION AND INFORMATION RELATED TO YOUR LOCATION WHERE APPLICABLE, BY THE COMPANIES FOR VALIDATION OF YOUR IDENTITY; AND**
- **YOU FURTHER AGREE THAT YOU HAVE READ, UNDERSTOOD AND ACCEPT THE TERMS AND CONDITIONS OF THESE PRODUCT TERMS, THE TERMS OF USE, THE PRIVACY POLICY AND THE SUBSCRIBER AGREEMENT**.

We reserve the right to amend the Terms where such amendment is required. By using the Secure Citizen Application and any related services, you consent and agree to the Terms, as may be updated and amended from time to time.

Device Information

By using the Secure Citizen Application through your mobile phone, your device information will automatically be stored on the Secure Citizen Application. The device information which may be stored on the Secure Citizen Application is as follows:

- International Mobile Equipment Identity (IMEI) Number: - this is the number which is used in order to blacklist your device in the event that it is stolen and will also be used to link your Secure Citizen Application profile to your specific device;
- Your network provider;
- Your phone specifications: - this information is stored on the Secure Citizen Application in order to ensure that the Secure Citizen Application and all its features are compatible with your specific device;
- International Mobile Subscriber Identity (IMSI) Number: - this number is used to provide protection against hacking, it is collected and used in order to determine if any hacking of your device has taken place and can also be utilised in order to attempt to trace the source of such hacking; and
- Your sim card number: - this number is used to link your device to your Secure Citizen Application profile and will also be used to monitor any unauthorised attempts to access your Secure Citizen Application profile using your device.

In order for you to have access to these features of the Secure Citizen Application, it is required that your mobile device's location services are switched on.

Biometric Information

Biometric information is regarded as special personal information under the Protection of Personal Information Act 4 of 2013, it is therefore important that you understand that the Companies will be collecting and storing such information on the Secure Citizen Application, as well as the purpose for which such information will be used.

Facial Verification

Upon registration for the Secure Citizen Application, you will be required to take a real time selfie for the purposes of a liveness test in order to confirm and validate your identity. This image will be stored on the Secure Citizen Application and will be compared against your identity document as stored by the Department of Home Affairs, in order to further validate your identity.

The real time selfie which you have uploaded onto the Secure Citizen Application as part of the liveness test will be stored and compared against the identity of any person who attempts to access your Secure Citizen Application profile. If such images do not match, the image of the unauthorised person who attempted to access your profile will be stored on the Secure Citizen Application in an imposter database and will be used to protect you against any further fraudulent attempts which may be made to access your profile.

Voice Verification

You will be required to enrol your voice onto the Secure Citizen Application. Your voice will be stored on a secure database and will be used to validate and verify your identity. Your voice can also be used by you to access your Secure Citizen Application profile. If your voice enrolment fails for any reason, the Secure Citizen Application will still allow you to continue with your registration.

In the event that any person attempts to access your Secure Citizen Application profile and the voice of such person does not match your identity as the user of the Secure Citizen Application, then the voice of such unauthorised person will be stored on an imposter database and the information stored on such database will be used to protect you against any further unauthorised attempts by such unauthorised person to access your profile.

Finger Verification

You may, in future, be required to register and enrol your fingerprint onto the Secure Citizen Application, for use as a login process to the Secure Citizen Application.

The purpose for which your biometric information is collected and stored is to enable the Companies to verify your identity as a user of the Secure Citizen Application. This stored information can also be used for any other lawful purpose and for any other purpose for which you may provide consent. The Companies will to the extent possible, validate any biometric information which you may upload onto the Secure Citizen Application and such validation will be used with the intention of preventing and protecting you against identity or application fraud.

Know Your Customer

The Companies will be accessing the National Population Register in order to obtain your demographical data which may include your age, nationality, gender, marital status, immigration status and life status. This demographical data will be used for the purpose of confirming the accuracy and correctness of all the documentation which you have uploaded onto the Secure Citizen Application. It will therefore be utilised to validate your identity as a South African citizen and a valid user of the Secure Citizen Application.

Proof of Address

You will be required to upload a picture of your documentary proof of residence onto the Secure Citizen Application. If you indicate that you are the owner of the property which is reflected on the proof of residence, the Companies will verify the accuracy of this indication with the Deeds Office registry. If you indicate that you are the tenant of the property as reflected on the proof of residence, the Companies will endeavour to confirm the existence of a rental agreement, including affidavits, where applicable, with the landlord of such property. We will also carry out any other reasonable checks in order to confirm your address, including confirmation of residence from church leaders or traditional leaders.

Provided that your device's location services are switched on and you have approved access to your location by the Secure Citizen Application, such information will be used to determine your habitual location (where you are habitually during certain hours of the day). This information will be used to further validate and confirm your address.

Fraud

The Companies will collect information from various sources, including members of SAFPS, on confirmed fraudulent incidents which are supported by substantiating documentation, facts or information. The Companies will upload all such information relating to any and all confirmed fraudulent incidents which have been committed using your identity onto the Secure Citizen Application and such information will be used in order to protect you against any future incidents of this nature.

Document Sharing

You will be able to obtain a Secure Citizen certificate only once your identity has been fully verified in accordance with the Terms.

Through the use of this feature of the Secure Citizen Application, you will have the ability to share any one or more documents which you have uploaded onto the Secure Citizen Application with any institution of your choice, provided that such institution is a member of SAFPS. These documents may include details of any Protective Registration which you have applied for (whether directly through the SAFPS website or via a Link into the Secure Citizen website, software and/or applications provided to you by an SAFPS member), as well as any Secure Citizen certificates which confirm your status as a

Secure Citizen.

Alternatively, you will also have the ability to provide your authorisation and consent to SAFPS for the purpose of SAFPS sharing any one or more of the documents which you have uploaded onto the Secure Citizen Application with an institution of your choice.

THE FOLLOWING REQUIREMENTS NEED TO BE MET IN ORDER FOR SAFPS TO ISSUE YOU A SECURE CITIZEN DIGITAL CERTIFICATE

- ID Verification and image
- Biometric collection (voice, face, liveness)
- Proof of address must be submitted, verified and valid in terms of Financial intelligence Centre Act 38 of 2001 (FICA)
- The Terms of the Secure Citizen Application must be accepted

If any of the above requirements have not been met or you fail one of the verification processes, then the Secure Citizen Certificate will not be issued.

Disclosures required in terms of section 43 of the Electronic Communications and Transactions Act 25 of 2002

In respect of **Secure Citizen** as follows:

Full name: Secure Citizen Proprietary Limited
Registration number: 2019/547916/07
Country of incorporation: South Africa
Email address: info@securecitizen.co.za

In respect of **SAFPS** as follows:

Full name: The Southern African Fraud Prevention Service
Registration number: NPC 2000/020784/08
Country of incorporation: South Africa
Telephone number: 0860 101 248
Email address: SecureCitizen@safps.org.za

In respect of the **Licensors** as follows:

Full name: Contactable (Proprietary) Limited
Registration number: 2012/154640/07
Country of incorporation: South Africa
Telephone number: 010 100 3647
Email address: privacy@staycontactable.com

Full name: OneVault Proprietary Limited
Registration number: 2011/126825/07
Country of incorporation: South Africa
Telephone number: 087 310 5890
Email address: info@onevault.co.za