SAMBA CO-OPERATIVE LIMITED

POPI Compliance and Security Policy

1. Introduction

This POPI Compliance and Security Policy describes how we handle information when used by our software and services. This Policy was last revised on June 2021.

In compliance with POPI, Samba Co-operative Limited has the following responsibilities:

1. Samba Co-operative Limited is responsible for the storing and safekeeping of our members' information, such as email addresses, phone numbers, banking account details, and other information used to conduct business with our members.

2. Samba Co-operative Limited is responsible for the storing and safekeeping of suppliers' information, such as email addresses, phone numbers, account details, and other information used to conduct business with the suppliers.

1.1 Privacy Principles

As a buying association Samba Co-operative Limited is responsible for the acquiring, storing, safeguarding and destroying of our members' and suppliers' information. Samba Co-operative Limited will only submit this information on request to the government. Samba Co-operative Limited adheres to the following rules and regulations regarding personal information:

1. **Choice and Consent:** Samba Co-operative Limited will not contact or solicit you unless you have given us your consent to do so when application for membership was done.
2. **Data storage:** Samba Co-operative Limited will store data for the period that is required by law for the resolution of any future enquiries that might arise.
3. **Data security:** Samba Co-operative Limited will take measures to ensure data is kept safe and secure, preventing loss or unauthorised access to personal information via our internal systems or our website.
4. **Data access:** Samba Co-operative Limited will supply our members' of any of their personal information, should they require.
5. **Data consistency and validity:** Samba Co-operative Limited will keep records of all the changes that were made on any of our data.

1.2 Compliance

Samba Co-operative Limited is compliant with the following:

1. **Protection of Personal Information Act (POPI)**
2. **CPA Section 11**
3. **Electronic Communications Act of 2002 (ECT)**

1.3 Information Request and Removal

In the event that any of your personal information changes, for example:

1. Cell phone number
2. Email address
3. Physical address

We advise you to contact Samba Co-operative Limited to correct the changes. In the event that you require us to remove your personal information, you can contact us to remove your information, after the period as stated by law has been met. Requests for personal information will be handled in accordance with the POPI Act and written requests must be given in order to provide you with any personal information.

1.4 Contact Us

Information Officer is: **Louis Nel (Chief Executive Officer)**
Email address: **louis@sambakoop.com**
Telephone: 051-448 0111
Physical address:
146 Charlotte Maxeke Street
Bloemfontein
9301

2. Servers and Security

2.1 Server Setup

Samba Co-operative Limited uses two database servers:

1. The main server is used for all transaction processing and storing all of the personal data that are used. This server is only accessible from outside our offices by Secure VPN and through a Firewall.
2. The secondary server is used to update our website.

The website is hosted by Network and Computing Consultants (Pty) Ltd (NCC), Bloemfontein, on secure servers and uses the HTTPS protocol.

Firewalls and data protection

Internet traffic goes through a Fortigate firewall to protect intrusion from outside into our systems. Users have access to the internet through a proxy server, the proxy server reports any attempts that are made from unauthorised intrusions.

2.2 Data Storage

Data Hosting

Website data is hosted NCC's secure server, using a secure HTTPS protocol.
Users are only able to access their own data through the use of membership number and password to log onto the secure website.

2.3 Security

1. There is restricted access to our premises.
2. No entry is allowed to the server room for any unauthorised personnel.
3. An alarm system and armed response is in place for after-hours protection.
4. CCTV camera placement at both entrance points to the building.
5. CCTV system records all activities at the entrance points.

2.4 Application Security

System logs are generated and kept for all system intrusion attempts that are made.
Logs are generated for unauthorised database attempts to access the database.

2.5 Data Backup

Backups
Full backups are made of Database, Email and system every day and stored in a secure safe onsite. There is also a backup that gets made every hour to an offsite storage device.

2.6 System Access Control

System Login
The system was developed to ensure that users only have the ability to access the applications and application screens that they were authorised to use by management. Users are forced to change their passwords every month and the same password cannot be used more than once. Only the database administrator has the ability to change another user's password. When a new user is created, the database administrator gives access rights to the user, as requested by management, given in writing and signed off after completion. Users must keep their password safe and private.

User logs
Any changes that a user makes to a member's information gets captured by the system in an audit log that can be used to track the user that made the changes. Enquiries on members' details are captured on the same log file.

Login attempts and successful logins are kept in a separate log file to monitor user activity. A system log is kept for all queries that are made on the members.

Administrator
Admin users can change their passwords. These users have additional rights:

1. Admin users have access to all applications.
2. They can change another user's password, but not view it.
3. Admin users can create new users.
4. They can assign access rights to other users.

System logs and validations
All data that is imported into the system is validated through various methods to ensure that no errors can occur in the processing of the data. New members whose data is captured for the first time, is given a membership number, this number is unique and is generated by using a CDV check to ensure that no duplicate numbers can be generated.

2.7 3rd Party and Database queries

Copycor Rentals
Copycor Rentals is the service provider which Samba Co-operative Limited uses for postage of the statements for members who do not want their statements to be sent using email. A contract has been signed by Samba Co-operative Limited and Copycor Rentals.

SACCRA
In accordance with NCR legislation, Samba Co-operative Limited must supply all Credit Bureaus with our members' financial details, this is done by supplying SACCRA with the information in the following manner:

1. Data is submitter from the Samba Co-operative Limited system to Experian using secure connection.

Database queries
Only the database administrator has the ability to generate custom queries on the database. These queries have to be requested by senior management and deleted once completed.

2.8 Disaster Recovery plan

The disaster recovery plan of Samba Co-operative Limited consists of the following:

1. Full Disaster Recovery plan gets done every 6 month.

3. Controls and Internal Access Data

3.1 Physical Access to Data

The following physical measures have been put in place:

1. Access control to the offices at all time.
2. 24 Hour armed response.
3. CCTV at all access points.

3.2 Staff

Employment contracts that protects the personal information of the members and suppliers have been signed by all employees. No employee is allowed to leave the premises with any personal information of a member or supplier. Employees are only able and allowed to access the information that they have been given permission to by senior management.

1.3 Employee and service Providers

1. Credit and criminal checks are done on all employees before they are employed.
2. Employees who resign or leave Samba Co-operative Limited for any other reason's passwords get revoked by the system.
3. New employees are firstly trained on how to use the system, before they are assigned with their own usernames and access privileges.
4. Strict privacy contracts are signed with all external suppliers that have access to our members' information.

3.4 Policies for the Access to Information

Paper records

Paper records are used for new application for membership, personal loans, limit increases, hire purchases and budget accounts. These records are stored in a locked safe after the application has been approved. Users are not allowed to remove any documents from Samba Co-operative Limited's premises.

Laptops and USB storage

Laptop user can only login to the system remotely using a Secure VPN connection.

USB storage devices are only used for the backup of personal documents and no member information is allowed to be stored on the devices. Users are also unable to run any queries to get bulk information of members from the system, as only the database administrator is able to extract this information with prior approval from senior management.

Monitoring

Samba Co-operative Limited has got the following measures in place to protect against unauthorised access to personal information:

1. Users are assigned with specific access privileges when they are activated on the system.
2. Users' passwords must be changed every month and the same password cannot be used.
3. Only the database administrator has direct access to the database and is only allowed to perform queries and other functions after permission is given by senior management.

……..
……..
……