Sunrise Credit Union Limited
Code for the Protection of Personal Information

6.10 Principle 10 – Compliance

FOREWORD

Sunrise Credit Union Limited is committed to keeping members' personal information accurate, confidential, secure and private. This document sets forth the protective measures necessary to fully incorporate privacy practices into all information handling activities, and to foster the necessary levels of employee awareness and engagement.

This privacy code applies throughout Sunrise Credit Union Limited.

1.0 INTRODUCTION

1.1 Purpose & Scope

This document defines Sunrise Credit Union Limited (SCU)'s Privacy Code, which provides guidelines that SCU uses to protect the privacy of personally identifiable member and employee data that is collected, used, disclosed or communicated to SCU in the course of its business. This Code is based on the 10 privacy protection principles laid out in the Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information* and applies to all aspects of information handling within SCU.

Credit Unions are member-owned and controlled financial institutions and, as such, have an inherent responsibility to be open and accessible while, at the same time, adhering to the highest standards for the protection of members' personal privacy.

In adopting this Code for the Protection of Personal Information, what has been accepted practice becomes a documented commitment to the member.

1.2 Roles and Responsibilities – Privacy Officer

The prime responsibility for compliance with all of the principles of SCU's Privacy Code resides with SCU's Privacy Officer. However, this does not, in any way, relieve any other SCU employee from an obligation to comply with the law.

1.3 Roles and Responsibilities – Employees

All employees are responsible for maintaining the confidentiality of all personal information to which they have access. All employees are required to sign a "Rules of Conduct" agreement as a condition of employment, which, among other practices, confirms employee's commitment to safeguarding of all confidential information. This confirmation is reaffirmed annually.

2.0 PRIVACY POLICY STATEMENT

2.1 Policy Statement

The Board of Directors and the Management of SCU are committed to ensuring the application of this policy in relation to the collection, usage, disclosure, and processing of personal data.

3.0 PRIVACY POLICY

SCU's Privacy Policy is based on the CSA Privacy Code and informs the public of our commitment to individual privacy.

3.1 Appoint Privacy Officer

SCU will designate a Privacy Officer who is accountable for SCU's compliance with the principles of this Code. SCU shall identify internally and to the system, the designated individual who is responsible for the organization's day-to-day compliance with the principles.

3.2 Phased in Compliance

SCU will follow a phased in implementation of the Privacy Legislation.

3.3 Staff Training

The Privacy Officer will develop information and training materials to ensure employees clearly understand their obligations to protect personal information and the procedures to be employed under the SCU Privacy Code.

3.4 Annual Review of Privacy Code

The Privacy Officer will review the Privacy Code on an annual basis and provide any recommendations or changes to senior management and the Board of Directors. The Privacy Officer also will report to the Board on the disposition of all inquiries to SCU from their members, the public, other organizations, and government agencies.

4.0 Sunrise Credit Union Limited Code for the Protection of Personal Information

4.1 Summary of the 10 Privacy Principles

Ten interrelated principles form the basis of Sunrise Credit Union's (SCU) Code for the Protection of Personal Information ("the Code"). Each principle must be read in conjunction with the accompanying commentary.

4.1.1 *Accountability*

SCU is responsible for personal information under its control and shall designate an individual who is accountable for SCU's compliance with the principles of the Code.

4.1.2 *Identifying Purposes*

The purposes for which personal information is collected shall be identified by SCU at or before the time the information is collected.

4.1.3 *Consent*

The knowledge and consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate.

4.1.4 Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by SCU. Information shall be collected by fair and lawful means.

4.1.5 Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

4.1.6 Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.1.7 Safeguards

Security safeguards appropriate to the sensitivity of the information shall protect personal information. SCU will employ the same standard of care as it takes to safeguards its own confidential information of a similar nature.

4.1.8 Openness

SCU shall make readily available specific, understandable information about its policies and practices relating to the management of personal information.

4.1.9 Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. An individual is entitled to challenge the accuracy and completeness of the information and have it amended as appropriate.

4.1.10 Compliance

An individual shall be able to question compliance with the above principles to SCU's Privacy Officer. SCU shall put policies and procedures in place to respond to an individual's questions and concerns.

5.0 Definitions

The following definitions apply in this Code.

"Collection"

The act of gathering, acquiring, or obtaining personal information from any source, including Third Parties, by any means.

"Consent"

Voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of SCU seeking consent. Implied

consent arises where consent may reasonably be inferred from the action or inaction of the member.

"Privacy Officer" Designated Individual

The person within SCU who is responsible for collection, use, disclosure and protection of members' personal information and SCU's day-to-day compliance with the Code.

"Disclosure"

Making personal information available to others outside SCU.

"Member" Individual

The person who is a member and owner of the credit union. This code applies equally to the collection, use or disclosures of personal information about members and non-members. Where the term "member" is used, its intent is also to include non-members.

"*Organization*"

A term used in the Code that includes organizations, partnerships, associations, businesses, charitable organizations, clubs, government bodies, and institutions, professional practices and unions.

"Personal Information"

Any information that is about or can be linked to an identifiable individual. This does not include the name, title or business address or business telephone number of an employee of an organization.

"Subsidiary"

A company or organization wholly-owned or controlled by SCU, Credit Union Central of Manitoba (CUCM), Credit Union Central of Canada(CUCC), or other members of the Canadian financial co-operative sector.

"Third Party"

Any person or organization other than SCU, CUCM, or member.

"Use"

Refers to the treatment and handling of personal information within SCU.

6.0 The 10 Privacy Principles

6.1 *Principle 1 – Accountability*

SCU is responsible for personal information under its control and shall designate an individual who is accountable for SCU's compliance with the principles of the Code.

6.1.1.

Ultimate accountability for SCU's compliance with the principles rests with SCU's Board of Directors. Other individuals within SCU may be accountable for the day-to-day collection and processing of personal information, or to act on behalf of a designated individual.

6.1.2

SCU shall identify internally and to its members the designated individual who is responsible for the day-to-day compliance with the principles.

6.1.3.

SCU is responsible for personal information in its possession. SCU shall use contractual or other means to provide a comparable level of protection while the information is being transmitted to or processed by a Third Party.

6.1.4.

SCU shall implement policies and procedures to give effect to the principles, including:

- procedures to protect personal information;
- procedures to receive and respond to concerns and inquiries;
- training staff to understand and follow SCU's policies and procedures;
- annual review of the effectiveness of the policies and procedures to ensure compliance with the Code and consideration of revisions as deemed appropriate.

6.2 *Principle 2 – Identifying Purposes*

The purposes for which personal information is collected shall be identified by SCU at or before the time the information is collected.

6.2.1

SCU shall document the purposes for which personal information is collected prior to the information being collected.

6.2.2.

SCU shall make reasonable efforts to ensure that individuals are aware of the purposes for which their personal information is collected, including use by Third Parties.

6.2.3.

SCU shall collect personal information for the following purposes:

- to meet legal and regulatory requirements
- to provide ongoing service
- to set up, offer, and manage products and services that meet member needs.
- to aid in understanding member needs
- to assess conflicts of interest
- to perform internal and external audits

- to provide Corporate Governance Reports
- to perform credit checks
    - o to verify the members identity
    - o to determine eligibility for products and services
    - o to detect and prevent fraud and to help safeguard the member's and the credit union's financial interests.
    - o to carry out any other purpose that the member authorizes or that is permitted by law

6.2.4.

The identified purposes should be specified to the individual from whom the personal information is being collected. This can be done orally, electronically, or in writing. An application form with the purposes clearly identified, for example, may give notice of the purposes.

6.2.5.

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose.

6.3 Principle 3 – Consent

With few exceptions, the acknowledgment and consent of the individual is required for the collection, use, or disclosure of their personal information.

Note: In certain circumstances personal information may be collected, used, or disclosed without the knowledge and consent of the individual. These circumstances include:

- where disclosure is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- to avoid compromising information availability or accuracy and, if reasonable, to investigate a breach of an agreement or a contravention of the laws of Canada or a province;
- where the information is generally considered to be in the public domain;
- to act in respect of an emergency that threatens the life, health, or security of an individual;
- assist in the investigation of an offence under the laws of Canada, a threat to Canada's security, to comply with a subpoena, warrant or court order or rules of a court relating to the production of records, or otherwise as required by law.

6.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. In certain circumstances, consent may be sought after the information has been collected but before use (for example, when SCU wants to use information for a purpose not previously identified).

SCU may be required to collect, use, or disclose personal information without the individual's consent for certain purposes, including the collection of overdue accounts, or for legal or security reasons.

6.3.2.

The principle requires "knowledge and consent". SCU shall make reasonable effort to ensure that the individual is aware of the purposes for which their information will be used. To make

the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how their information will be used or disclosed.

6.3.3.

SCU shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill explicitly specified and legitimate purposes.

6.3.4.

In determining the form of consent to use, SCU shall take into account the sensitivity of the information. Although some information (for example, medical and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. When in doubt, employees should consult the SCU Privacy Officer before taking action that could jeopardize an individual's privacy.

6.3.5.

SCU will not obtain consent to carry out processing functions, such as data processing, secondary support, testing new products, cheque processing, etc. On the other hand, an individual would not reasonably expect that personal information given to SCU would be given to a Third Party company selling insurance products, unless consent was obtained.

Consent will not be obtained through deception.

6.3.6

The way in which SCU seeks consent may vary, depending on the circumstances and the type of information collected, SCU will seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive.

Individuals can give consent:
- in writing, such as when completing and signing an application or applying for employment;
- through inaction, such as failing to check a box indicating that they do no wish their names and addresses to be given to other organizations;
- orally such as when information is collected over the telephone or in person;
- at the time they use a product or service
- through an authorized representative (such as a legal guardian or a person having power of attorney).

6.3.7.

An individual may withdraw consent at any time, subject to legal or contractual restriction provided that:
- reasonable notice of withdrawal of consent is given to SCU.
- consent does not relate to a credit product requiring the collection and reporting of

information after credit has been granted; and
- the withdrawal of consent is in writing and includes understanding by the individual that withdrawal of consent could mean that SCU cannot provide the individual with a related product, service or information of value.

SCU shall inform the individual of the implication of such withdrawal.

6.4 Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by SCU. Information shall be collected by fair and lawful means.

6.4.1

SCU shall not collect personal information indiscriminately. SCU shall specify both the amount and the type of information collected, limited to that which is necessary to fulfill the purposes identified, in accordance with SCU's policies and procedures.

6.4.2

SCU shall collect personal information by fair and lawful means, and not be misleading or deceive individuals about the purpose for which information is being collected.

6.5 *Principle 5 – Limiting Use, Disclosure, and Retention*

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6.5.1

When SCU uses personal information for a new purpose, the purpose shall be documented and will be provided to the Privacy Officer as required.

6.5.2

SCU may disclose personal information without consent to protect the interests of SCU or when required by law, for example, when requested:

- by subpoena or search warrant;
- by other court and government orders;
- by demands from other parties who have a legal right to personal information;
- by a person acting in a confidential or professional relationship with SCU such as an auditor or a solicitor.

6.5.3.

SCU shall protect the interests of credit union members and SCU employees by taking reasonable steps to ensure that:

- orders or demands comply with the laws under which they were issued;
- only the personal information that is legally required is disclosed and nothing more;

- casual requests for personal information are denied;
- personal information disclosed to unrelated Third Party suppliers on non-financial services are strictly limited to programs endorsed by SCU.

6.5.4

The individual's health records at SCU may be used for credit application and related insurance purposes or as required for the provision of individual health insurance or benefits. The individual's health records shall not be collected from, or disclosed to, any other organization.

6.5.5

SCU shall maintain guidelines and procedures with respect to the retention of personal information. These guidelines include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. SCU may be subject to legislative requirements with respect to retention of records.

6.5.6

Subject to any requirement to retain records, personal information that is no longer required to fulfill the identified purposes shall be destroyed, erased, or made anonymous. SCU shall develop guidelines and implement procedures to govern the destruction of personal information.

6.6 *Principle 6 – Accuracy*

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

6.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. SCU relies on the individual to keep certain personal information accurate, complete and current, such as name and address. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

6.6.2

SCU shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

6.6.3

Personal information that is used on an on-going basis, including information that is disclosed to Third Parties, will generally be accurate and up-to-date unless limits to the requirement for accuracy are clearly set out.

6.7 *Principle 7 - Safeguards*

Security safeguards appropriate to the sensitivity of the information shall protect personal information. SCU will take the same standard of care as it takes to safeguard its own confidential information of a similar nature.

6.7.1.

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. SCU shall protect personal information regardless of the format in which it is held.

6.7.2

The nature of the safeguards will vary depending on the sensitivity, amount, distribution and format of the information, and the method of storage. A higher level of protection will safeguard more sensitive information.

6.7.3

The methods of protection will include:

- physical measure, for example, locked filing cabinets and restricted access to offices;
- organizational measures, for example, controlling entry to data centers and limiting access to information to a "need-to-know" basis;
- technological measures, for example, the use of passwords and encryption;
- investigative measures, in cases where SCU has reasonable grounds to believe that personal information is being inappropriately collected, used or disclosed.

6.7.4

SCU shall periodically remind employees, Directors, and Officers of the importance of maintaining the confidentiality of personal information. Employees and Directors are individually required to sign the "Rules of Conduct" annually, including commitment to keep member's personal information in strict confidence.

6.7.5

Third Parties shall be required to safeguard personal information disclosed to them in a manner consistent with the policies of SCU. Examples include cheque processing, credit collection, credit bureau, and card production.

6.7.6

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information.

6.8 Principle 8 - Openness

SCU shall make readily available specific, understandable information about its policies and practices relating to the management of personal information.

6.8.1

SCU shall be open about privacy policies and procedures with respect to the management of personal information and shall make them readily available in a form that is generally understandable.

6.8.2

The information made available shall include:
- the name or title and the address of the designated individual who is accountable for compliance with SCU's policies and procedures and to whom complaints or inquiries can be forwarded;
- the means of gaining access to personal information held by SCU;
- a description of the type of personal information held by SCU, including a general account of its use;
- a copy of any brochures or other information that explains SCU's policies, procedures, standards or codes;
- the types of personal information made available to related organizations, such as subsidiaries or other suppliers.

6.8.3

SCU may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, SCU may choose to make brochures available in its place of business, by mail, through on-line access, or through a toll-free telephone number.

6.9 Principle 9 – Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of their personal information, and shall be given access to that information. An individual is entitled to challenge the accuracy and completeness of the information and to have it amended as appropriate.

Note: In certain situations, SCU may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access include the following:

-providing access would likely reveal personal information about a third party (unless such information can be severed from the record or the third party consents to the disclosure, or the information is needed due to a threat to life, health or security);
- the personal information has been requested by a government agency to enforce any law of Canada, a province or a foreign jurisdiction, to carry out any investigation related to the enforcement of any law, the administration of any law, the protection of national security, the defense of Canada or the conduct of international affairs;
- the information is protected by solicitor-client privilege;
- providing access would reveal confidential commercial information, (provided this information cannot be severed from the file containing other information requested by the individual);
- providing access could reasonably be expected to threaten the life or security of another individual, (provided this information cannot be severed from the file containing other information requested by the individual);
- the information was collected without the knowledge or consent of the individual for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
- the information was generated in the course of a formal dispute resolution process.

6.9.1

Upon request, SCU shall inform an individual of the existence, use, disclosure, and source of personal information about the individual held by SCU, and shall allow the individual access to this information. However, SCU may choose to make sensitive medical information available through a medical practitioner rather than by communicating it directly to the individual.

6.9.2

For SCU to provide an account of the existence, use, and disclosure of personal information held by SCU, the individual may be asked to provide sufficient information to aid in the search. The additional information provided shall only be used for this purpose.

6.9.3

In providing an account of Third Parties to which it has, or may have, disclosed personal information about an individual SCU will be as specific as possible, including a list of Third Parties.

6.9.4

SCU shall respond to an individual's request within a reasonable time and at no cost, or at a reasonable cost, to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if SCU uses abbreviations or codes to record information, an explanation will be provided.

6.9.5

When an individual successfully demonstrates the inaccuracy of incompleteness of personal information, SCU shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to Third Parties having access to the information in question.

6.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by SCU. When appropriate, the existence of the unresolved challenge shall be transmitted to Third Parties having access to the information in question.

6.10 Principle 10 - Compliance

An individual shall be able to question compliance with the above principles to the designated individual accountable for SCU's compliance; SCU shall have policies and procedures in place to respond to an individual's questions and concerns.

6.10.1

The name of and how to contact the SCU Privacy Officer shall be communicated to SCU staff and the Manitoba credit union system.

6.10.2

SCU shall maintain procedures to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures will be easily accessible and simple to use.

6.10.3

Individuals who make inquires or lodge complaints shall be informed by SCU of the existence of relevant complaint procedures. If a complaint is not satisfactorily resolved by SCU's Privacy Officer, it may be taken to SCU's Board of Directors. If not resolved there, procedures shall be in place to refer it to a regulator. SCU shall inform individuals of their right to file a complaint with the Privacy Commissioner of Canada.

6.10.4

SCU shall investigate all complaints. If a complaint is found to be justified, SCU shall take appropriate measures, including revision of the personal information and, if necessary, amending SCU's policies and practices.