POLICIES AND PROCEDURES
MANAGEMENT & ADMINISTRATION

Table of Contents

Preface

The purpose of policies and procedures are to provide a framework for quality and responsible performance in each of the respective areas. Policies are intended to be helpful, not hindering. SSICS has a commitment to continuous improvement. Policies will be regularly reviewed and updated or changed as required to be the best possible guidelines they can be for the time. **The current policies were reviewed and updated in September 2020**

SSICS Society Policies and Procedures include the following manuals:
- Service Delivery
- Personnel
- Health and Safety
- Management and Administration
- Governance

The objectives of the Management and Administration Policies are to:
- Provide a framework for quality organizational management and leadership.
- Provide guidelines and procedures for effective, accountable and ethical service delivery and associated organizational activities.
- Ensure clarity and consistency on the part of Directors, Managers, Employees and Volunteers.
- Establish expectations and procedures for organizational review, planning and improvement.
- Provide a structure to enable SSICS to meet and maintain accreditation standards.

Employee refers to paid employees, contractors and volunteers unless otherwise specified. Employees, contractors and volunteers have different roles to play in the management and administration of SSICS, although paid employees generally hold more responsibility and accountability.

1. General

1.1 Code of Ethics

POLICY:

SSICS will maintain a Code of Ethics that provides standards which all directors, employees, and volunteers must follow in the performance of their duties. The Code of Ethics, together with the other policies and procedures, form the philosophy, principles and values for quality service delivery. The Code of Ethics will guide ethical decision making and protect the rights, dignity and safety of program participants.

PROCEDURE:

1. Employees will adhere to the Code of Ethics, and to the requirements of their professional organization where applicable. It is the responsibility of employees to identify potential conflicts between the SSICS ethical standards and those of their professional organization, and to discuss these with their supervisor.

2. Directors, employees and volunteers will acknowledge in writing that they have read and understood the Code of Ethics.

3. The Code of Ethics will be reviewed on an ongoing basis to ensure its relevance and completeness. Changes will be communicated in writing to all directors, employees and volunteers.

4. Alleged violations of the Code of Ethics will be investigated by the organization. Investigations will follow complaint and disciplinary procedures specified in SSICS Personnel and Governance Policies and union collective agreements.

1.2 Organizational Structure

POLICY:

A description of the SSICS organizational structure, including lines of accountability and supervision, will be current and available to employees, and to program participants and others upon request.

PROCEDURE:

1. Organizational structure, lines of reporting and supervision will be reviewed as part of an annual management review.

2. Changes to organizational structure or lines of accountability will be approved by the Executive Director. Whenever possible reviews and changes to structure will involve the employees impacted prior to implementation whenever possible.

3. A current organizational structure will be presented in an organizational chart and distributed or posted to communicate this information to employees and others. Changes to the organizational structure will be communicated to employees and other stakeholders as soon as possible.

4. Adaptations or changes to organizational structure documents will be approved by the Executive Director prior to distribution.

1.3 Community Profile and Communication

POLICY:

SSICS will plan and implement communications and education activities to keep stakeholders and the community informed of the services and activities of the organization and the ways in which services may be accessed. Communication will whenever possible to reduce any negative stigma experienced by the populations served by SSICS.

PROCEDURE:

1. SSICS will undertake specific public education strategies and activities at Board of Directors, management and service delivery levels.

2. SSICS will maintain current and accurate information regarding the mission, policies, services and operations for dissemination to program participants and the community including:

   - Orientation information and Handbook for Person Served
   - Pamphlets, brochures, website and other material outlining services
   - Code of Ethics
   - Complaint procedures
   - Organizational chart
   - Annual Report
   - Annual Audited Financial Statements

3. SSICS will engage in public education and training activities to reduce the stigma of program participants, increase community profile, increase accessibility of services, and increase the understanding of services offered. SSICS communication and public information will be reviewed on a regular and ongoing basis to ensure they are accurate, complete and current.

1.4 Media Contact

POLICY:

Contact with the media, including information inquiries from media, will be coordinated and directed by the Executive Director or Board of Directors Chair. Employees will only interact with the media when authorization has been given by the supervisor or Executive Director. Media contact related to general service information or program specifics may typically be delegated to program staff by their supervisor, Executive Director or Communications Coordinator.

PROCEDURE:

1. Requests for information from the media, or plans for employee communication with the media (eg. to promote an event or service), will be directed to the Communications Coordinator or Executive Director for review.

2. The Executive Director may assign media contact tasks and roles to specific employees or determine the parameters of media contact within a specific job role.

3. Press releases, advertising or media scripts will be approved by the Communications Coordinator or Executive Director prior to release.

1.5 Social Media

POLICY:

SSICS encourages the use of social media for the purposes of information, promotion and connecting individuals in relation to SSICS programs and services. Use of social media by employees will observe the need to maintain a positive image and reputation of the organization, and will follow basic communications, privacy and ethical policies and procedures. Employees will to follow the procedures outlined in this policy when using the internet and social media, recognizing that social media is a fast moving technology and it is impossible for one policy to cover all circumstances.

PROCEDURE:

1. Employees are required to read and follow the Social Media Code of Conduct. Inappropriate personal social media activity could result in investigation and, in some cases, disciplinary measures.

2. Although the social media activity of employees via personal accounts is not governed by this policy, such activity may also be a reflection on SSICS or affect Seneca's interests, and is therefore subject to the SSICS Code of Conduct.

3. Each SSICS-affiliated social media account must have a designated account administrator and be linked to an appropriate SSICS email account.

4. SSICS will monitor use and delete any SSICS-affiliated social media account if it is no longer being actively used, or modify or delete content on any SSICS-affiliated social media account at its discretion.

5. Account administrators or others will not post, and may remove, inappropriate, offensive or illegal content. Account administrators or others will not share confidential information or post photos of SSICS employees or persons served through social media accounts without their consent.

6. Only approved SSICS social media accounts may post about emergency events or inclement weather unless otherwise directed a SSICS manager or Executive Director.

7. SSICS will provide training and ongoing individual consultations related to social media issues, including launching SSICS-affiliated social media accounts.

8. Staff will refrain from posting derogatory comments about other staff, persons served, or SSICS stakeholder, partners, vendors, suppliers or individuals that could cause reputational harm.

9. Social media platforms may enable an individual to "friend" someone into their social network. "Friending" a person served by a SSICS employee is not consistent with the need to keep a personal and profession separation and may blur the boundaries of a professional relationship. Staff are responsible for ensuring their interaction with clients is through SSICS official methods and meets guidelines outlined by their professional association or regulatory body where applicable.

10. Use of personal blogs or social media by employees to discuss their work and add to the "industry conversation" is permitted as long as confidential information is not revealed and the blogger clearly identifies that opinions expressed in the blog are those of the individual and not of SSICS. Employees using social media willinclude a simple and visible disclaimer advising that the views expressed are their own and noton behalf on the organization.

11. Staff should contact their supervisor or the Executive Director if they have concerns regarding appropriate social media use by themselves or others.

12. SSICS may collect information from social media postings in the course of vetting applicants for work. In the case of this occurring with current employees the employee will be notified and relevant information gleaned from social media will be disclosed.

1.6 Cultural Competence and Diversity

POLICY:

SSICS will recognize the value of diversity and respond positively and openly to the specific cultural needs of employees and program participants. Cultural needs include ethnicity, religion, age, gender, sexual orientation, disability or other special characteristics. SSICS will review hiring, human resource management and service delivery practices on an ongoing basis to ensure the best possible cultural and diversity practices.

PROCEDURE:

13. Employee and volunteer recruitment and hiring practices will not present barriers to applicants of different cultural groups.

14. Ongoing employee training and program development will be provided in topics related to diversity and cultural sensitivity to ensure worksites and services are welcoming and relevant to program participants.

15. A plan, with strategies to promote cultural competence, will be included in the Management Report and Performance Improvement Plan. The plan will include a review of the cultural characteristics of the people served by SSICS, strategies to employ people representative of the common cultural groups.

1.7 Accessibility Plan

POLICY:

SSICS will ensure that services are as accessible as possible to all people eligible for service by developing, implementing and maintaining an accessibility plan. Barriers to access will be identified and addressed wherever possible to minimize the impact on individuals`.

PROCEDURE:

1. The Accessibility Plan will be reviewed and updated by the Executive Director and managers annually.

2. The Accessibility Plan will include consideration of the following potential barriers: architecture, environment, attitudes, finances, employment, communication and transportation.

3. Services will be wheelchair accessible when possible. Where services are not accessible because of physical or architectural barriers SSICS will arrange accessibility in another location when possible.

4. Adaptive devices and related equipment will be provided when appropriate and reasonable for the purpose of ensuring the hearing impaired, visually impaired, physically or mobility challenges, learning or reading impaired are able to participate in services.

2. Quality Improvement

2.1 Strategic Planning

POLICY:

SSICS will engage in organizational review and strategic planning processes on an ongoing basis that includes participation from Board of Directors, managers, employees and volunteers. The strategic plan will establish and review goals and priorities and be presented in a Strategic Plan that is always up to date and relevant.

PROCEDURE:

1. The strategic planning process will take place on an ongoing basis, involving regular updating and reviewing by the Board of Directors, and a complete review annually.

2. The strategic planning process will consider information collected from the following sources:

   - Program participants
   - Employees and volunteers
   - Funders
   - Community stakeholders
   - Service outcomes, business practices and other performance management systems
   - Information and research presenting the current best practices in the areas of concern to SSICS

3. The strategic planning process will include consideration of the following:

   - Purpose, philosophy and mission
   - Populations served, and the expectations of program participants and the community
   - Key strategies for accomplishing short and long term goals
   - Organizational capacity and business practices, including financial and human resources, risk management practices and operational policies
   - Community relations, profile and communications

- Governance and leadership
- Emerging needs, challenges and opportunities
- SSICS activities in relation to external contexts including funders, government, legal and regulatory

4. The Strategic Plan will be organized into the following categories: quality programs and services, growth and innovation, communications and community relationships, and organizational capacity.

5. The Strategic Plan will be made available to employees, program participants and other stakeholders.

2.2 Management Report and Performance Improvement Plan

POLICY:

An Management Report and Performance Improvement Plan will be prepared annually by the Executive Director. The report will provide a review of the operation of SSICS in relation to the implementation of the Strategic Plan. The Performance Improvement Plan will provide thorough and, evidence-based information for quality improvement.

PROCEDURE:

1. The report will be based on information collected from program participants, community partners, employees and other stakeholders.

2. The report will include:

   - An overview of current services and activities.

   - Service delivery outcomes including efficiency, effectiveness, access to services and satisfaction of program participants.

   - A review of business practices including administration, management, leadership, health and safety, legal compliance, and finances.

   - Goals, priorities, strategies and actions for quality improvement.

3. The report will be documented and available to the Board of Directors, employees, funders, and other stakeholders.

2.3 Input from Program Participants and other Stakeholders

POLICY:

SSICS will collect information from program participants and community stakeholders regarding their experience and satisfaction with service delivery. This information will be reviewed and contribute to organizational improvement.

PROCEDURE:

1. Information from program participants will be collected on an ongoing basis by each service or program area. Whenever possible information will be collected using a standard survey for the service area.

2. Information from community stakeholders will be collected on a bi-annual basis with a standard survey.

3. Complaints, suggestions, and other feedback from program participants received on an ongping basis will be considered valuable information for quality improvement and included with all other information reviewed. Employees will document such information as they receive it and submit it to their supervisor or the Executive Director.

4. A summary of information collected from program participants and surveys will be included in the Management Report and Performance Improvement Plan.

2.4 Input from Employees

POLICY:

SSICS will collect information from employees regarding service delivery, employee job satisfaction and other aspects of organizational functioning. Information collected will be reviewed and used for organizational improvement.

PROCEDURE:

1. Information from employees will be collected on annually through surveys and program reports, and on an on-going basis through staff meetings, planning sessions and regular contact with supervisors.

2. Information from employees will be treated with the appropriate level of confidentiality. The only information passed on to others will be that which is relevant as contribution to organizational planning and review.

3. A summary of information collected from employees will be included in the Management Report and Performance Improvement Plan.

2.5 Outcomes Management

POLICY:

SSICS will have clear and specific outcomes identified for each service area and evaluate the degree to which these outcomes were achieved.

PROCEDURE:

1. Service delivery outcomes will be developed and reviewed with input from employees, funders, and other stakeholders for each service area.

2. Service delivery objectives and desired outcomes will be presented in clearly and simple language to program participants and community stakeholders as part of the orientation to SSICS services.

3. Regular evaluation of movement toward, or achievement of, outcomes will be an ongoing and regular part of service delivery.

4. Information will be collected from program participants, including their perceived level of satisfaction and service effectiveness. Outcome information will be collected during service delivery and whenever possible once service delivery has ended.

5. Information will be collected by employees and supervisors on an ongoing basis from referral sources and community partners including satisfaction with, and effectiveness of services.

2.6 External Reviews

POLICY:

SSICS may engage external resources to review, evaluate or accredit various aspects of its operations or specific services and projects. External resources will be confirmed to be credible and will be required to follow procedures determined or agreed to by SSICS.

PROCEDURE:

1. SSICS will comply with the requirements of funders for external reviews and accreditation.

2. External reviewers will confirm certification in their respective fields of expertise by providing credentials to SSICS upon request verifying an appropriate level of expertise.

3. External reviewers will conform to standards of confidentiality, ethical conduct and other requirements relevant of the nature of the review.

4. Agreements will be established between SSICS and external reviewers regarding the ownership, use and publication/dissemination of reports and other material resulting from reviews.

2.7 Complaints and Suggestions

POLICY:

SSICS will provide a safe, confidential and fair process to receive and review complaints from program participants, community members, employees and volunteers. Complaints will be reviewed and responded to in a timely manner.

PROCEDURE:

1. SSICS will inform program participants and the public of the complaint procedure in plain language, and provide a form for submitting a complaint or suggestion.

2. Complaints will be made in writing to the supervisor or Executive Director as soon as possible after the incident.

3. Complaints and appeals will be reviewed and a response given whenever possible within 14 days.

4. Each person involved with the complaint will be notified, to the extent possible and appropriate, of the outcome.

5. A decision may be appealed in writing within 30 days. If there is still no satisfactory resolution the complainant may appeal to the Chair of the Board of Directors.

6. When the complaint is specific to the Executive Director it will be made in writing to the Chair of the Board of Directors.

7. People submitting a complaint will not experience any consequences or barriers to service from the SSICS for bringing forth a complaint through the established policy.

3. Information Management

3.1 Information Management System

POLICY:

SSICS will maintain an information management system that collects, organizes and disseminates information in a timely and efficient manner. Access to information of a sensitive or confidential nature will be limited to those employees requiring the information for their work.

PROCEDURE:

1. SSICS will collect information in the following areas:

   - Input from program participants, employees and stakeholders
   - Case files, including records of program participants in group activities
   - Financial statements and budget information, including annual audit
   - Insurance policies, leases and other legal documents
   - Service and funding contracts and related information
   - Minutes of staff, safety and other internal meetings
   - Board and other business meetings
   - Personnel files
   - Job descriptions
   - Payroll and benefits information
   - Staff recruitment and hiring records
   - Health and safety information, including inspection, drill and incident reports
   - Policies and procedures
   - Service descriptions and SSICS promotional material

Paper-based information will be kept on SSICS worksites in designated areas following the appropriate confidentiality and access to records standards. Storage methods will be used to ensure security, safety and access by authorized employees. Information stored electronically will be kept on SSICS equipment or secured web-storage safeguarded to ensure security and access limited to authorized employees.

3.2 Records Management

POLICY:

Records of program participants, personnel files, and administration information will be organized and stored in a manner that ensures systematic, safe and confidential storage. Access will be limited to designated employees, and only those employees requiring access to perform their assigned work tasks. This applies to electronic and paper storage of information.

PROCEDURE:

1. All records of program participants, personnel files, and administration information records will be organized in a systematic manner and clearly labeled.

2. All records of program participants, will be stored in the secure file room designated for service deliver files, or the secure archive file room.

3. All personnel and confidential administration records will be stored with secure administration files.

4. During work hours confidential or sensitive information, including notes, will be locked in file cabinets or desks when not in use. Employees will return records to the central file when not in use and at the end of shift.

5. Confidential or sensitive information regarding program participants, personnel, and administration including working notes, will only be stored on individual computers if they are securely password protected.

6. Program participant, administrative and personnel records may only be removed from SSICS sites with authorization from their supervisor.

7. Archived records will be stored in the secure archive room. Records will be stored in a systematic manner in file cabinets tightly bunched to decrease potential fire damage.

8. To safeguard against destruction of electronically stored information in the event of a fire or natural disaster, relevant financial management information, policies and procedures, and original forms will be placed in fire proof storage.

3.3 Records Retention and Destruction

POLICY:

Information stored by SSICS will be destroyed by shredding or other secure methods after the designated time period has elapsed for the document. Electronic records will be destroyed by permanently deleting files from computers, storage devices and servers. and Destruction of records by an external company may take place if the company has the appropriate security status or if the destruction occurs under supervision at a SSICS site.

PROCEDURE:

1. Files to be retained indefinitely:

- Personnel files
- Audited financial statements
- Payroll records
- Society's Branch information
- Separation slips
- Bank ledgers and general ledger entries
- Board minutes

2. Files to be retained for a minimum of twenty-five years:

- Files of program participants, unless a longer period is required for specific files by a funder as specified by written agreement

3. Files to be retained for a minimum of seven years:

- Revenue Canada information
- Minutes of Board and other meetings
- Incident reports
- SSICS membership lists
- Budgets
- Funding contracts
- Current account information
- Cheque stubs
- Deposit slips and financial receipts
- Lease agreements

- Revenue and expenditure reports
- Annual program reports

4. Files to be retained a minimum of two years:

- Brief contact notes
- Insurance policies
- Lease agreements
- Appointment books
- Questionnaires and surveys
- Old policy, procedures and program manuals
- General correspondence
- Letters of support
- Applications for employment
- Job postings, hiring information and letters of applicant rejection

5. When a legal process or other investigation is initiated which requires the ongoing availability of certain records the required records will be retained until one year after the process has concluded.

3.4 Confidentiality

POLICY:

SSICS will maintain a high degree of confidentiality and act in a lawful and responsible manner when collecting, storing and using information from program participants and employees.

PROCEDURE:

1. SSICS will comply with all provincial and federal legislation and regulations, best ethical and professional practice, and other contract and legal requirements regarding the collection, protection and release of personal information.

2. The collection and use of personal information will be limited to what is required to effectively provide services, what is required by law and what is required of an employer.

3. When SSICS collects personal information the person will be informed of the purpose and range of information to be collected, and how it will be used and protected from inappropriate disclosure.

4. Consent from program participants, and their guardian when required, will be confirmed prior to the collection of personal information.

5. Consent from program participants, and their guardian when required, will be confirmed prior to the releaee or sharing of personal information with an external individual or organization.

6. Sharing of confidential personal information within SSICS will be limited to what is needed to proceed with a required action or activity, and shared only with those who need to know.

7. SSICS will have a designated Privacy Officer to act as a resource for employees and program participants on matters related to the collection, management, use and disclosure of personal information.

3.5 Privacy Officer

POLICY:

A Privacy Officer will be appointed by the Executive Director to ensure that SSICS is in compliance with laws, policies and procedures regarding confidentiality and privacy of personal information. A primary role of the Privacy Officer will be to respond to requests and concerns from individuals about the collection, security and sharing of their personal information.

PROCEDURES:

1. The Privacy Officer will work with the Executive Director, managers and staff to ensure systems and resources are in place so that:

   - Policies and procedures regarding confidentiality and privacy of personal information are current with federal and provincial legislation.
   - Employees are informed of policies and procedures relevant to Freedom of Information and Privacy.
   - Program participants are informed of their privacy rights.
   - Program participants are assisted with questions, concerns and complaints regarding privacy, confidentiality and their personal information.

2. The responsibilities of the Privacy Officer include:

   - Responding to requests from individuals to examine, copy or correct personal information collected and maintained by SSICS.
   - Overseeing the preparation of documents being released to others, including the redaction of third party and other irrelevant information.
   - Providing information to individuals, upon request, on how personal information is kept, used or shared.
   - Providing information to employees on Privacy and Freedom of Information legislation, policies and procedures.

3. The Privacy Officer will have familiarity with current privacy and freedom of information legislation and SSICS policies and procedures.

4. The Clinical Director will be the Privacy Officer unless an alternate is appointed by the Executive Director.

4. Technology

4.1 Technology Plan

POLICY

A Technology Plan will be prepared by the organization that describes how computer, communication, social media and other technology will be used to support SSICS activities. The plan will recognize the rapid rate of technology development and the need to strategically guide the management and improvement of technology to align with the needs and capacity of SSICS and its employees.

PROCEDURE

1. The Technology Plan will be updated annually and include information from employees about their technology use and skills, an assessment of administrative and service delivery needs, technology policies and procedure, and other emerging technology needs and issues.

2. An inventory of computer and communication equipment and projected lifespan will be maintained to plan for technology replacement.

3. Purchasing of computer hardware, software and other technology will be done centrally to ensure technology throughout SSICS is coordinated and efficient.

4. The Technology Plan will include a review of technology use patterns and the skills and capacity of employees to ensure technology improvements are effective and efficient.

5. The Technology Plan will include a review of current and emerging social media applications used and available to SSICS, and determine best practices for the use of such technology.

4.2 Computer Use

POLICY:

SSICS will maintain computers and related technology that are functioning effectively, have security features, and are available to employees for work requirements. Confidential electronic files will be managed and stored securely.

PROCEDURE:

1. Only designated employees will perform software downloads or other modifications to computers.

2. No software will be loaded onto computers except those that have been purchased by the SSICS. SSICS will comply with software licensing agreements.

3. Computers will be protected with current virus detection software and other appropriate internet security measures.

4. Employees will participate in an assessment of their computer skills, including basic use and security functions, and upgrade skills when necessary.

5. Computers will be password protected by the designated user, and confidential files will be password protected by the user. Passwords will be stored in a secure central location.

6. Computers and other electronic devices may be taken from the worksite by employees, including taken home after hours, providing measure are taken for their safety and security.

7. Employees on leaves of any kind will return their computer to SSICS for the duration of the leave.

4.3 Internet and Email Use

POLICY:

Internet, email and other communications systems will be used work purposes only. Employees will comply with specific guidelines around proper use, including following legal and ethical standards.

PROCEDURE:

1. All employees and other users of SSICS computers will agree to using the internet and email in a responsible and ethical manner including refraining from:
   - Illegal activities
   - Sending or accessing obscene or offensive content
   - Sending or forwarding non work-related e mails
   - Personal commercial or business use
   - Transmitting abusive, derogatory or false messages
   - Uses that impair the performance of the computer

2. Confidential information will not be sent in the body of an email. If confidential information is sent electronically it will be attached with a password protected file.

3. Computer users will be informed that technology belonging to SSICS including computers, email accounts and voice mail are not private and may be subject to access and control of the organization.

4. Personal use of internet and email is discouraged, although may be permitted at times subject to the employee following all relevant technology and communication and ethical behavior policies. SSICS may restrict or disallow personal use of technology at any time.

4.4 Data Security and Back up

POLICY:

Measures will be taken to ensure that the loss of data due to computer corruption, hardware failure, software malfunction, user error, power outage or surge is minimized.

PROCEDURE:

1. All SSICS computers will be designated as requiring daily, weekly or monthly data back-up based on the nature and priority of information stored. Data on computers will be backed up on schedule by the user. Training will be provided to all employees on data back-up procedures. Back up done will be done by a designated employee if the user is not yet familiar with data back-up procedures.

2. Backed up data will be stored off site, onsite in the fireproof safe, or in a cloud-based storage site.

3. Computers without a secondary power supply will be protected by surge protectors to protect against data loss during a power outage.

4.5 Public Use Computers

POLICY:

SSICS may designate certain computers to be made available to program participants or the general public. Use of these computers will be subject to program specific rules to ensure care and appropriate use, while also ensuring their availability to the intended people.

PROCEDURE:

1. Specific computers will be designated as "public use" or "program use" for use by program participants, visitors or other non SSICS employees. These will be the only computers to be used by anyone other than an SSICS employee.

2. People using public use or program use computers will have approval from employees designated for supervising the computer.

3. Users will be provided with an orientation to the computers and rules of use. They may be subject to supervision at the discretion of the supervising employee.

4. Public use and program use computers will have rules and guidelines posted by the workstation or provided to users in writing. Users may also be required to sign a use log and agreement before they are permitted access to the computer. Different SSICS worksites may have different rules and guidelines for computer use.

5. Public use and program use computers will be configured for easy multi-user functioning, and have the appropriate virus protection and security measures in place.

6. Employees will supervise computer use to the extent possible to ensure Users do not misuse the computers by damaging them, using them for improper or illegal activities or removing, altering or installing software. In such cases the user may be denied future access to SSICS computers.

4.6 Websites

POLICY:

SSICS will maintain websites as a communication and information resource for employees and the community. Information on websites will be current and relevant to ensure the effectiveness and intended purpose of the site. Maintenance and updating of the website will be done by designated people following proper standards of confidentiality and information management.

PROCEDURE:

1. Authority to update and maintain website content will be designated by the Executive Director.

2. Content on the website will be subject the same level of review and approval as other public and media communications. Content will be approved by program managers or Executive Director prior to publication.

3. SSICS will take reasonable care to ensure there are no links to external websites or documents with inappropriate content.

4. Confidential information will not be posted on the website. SSICS administrative information which is not intended for the public will be placed in a secure and limited access area of the website.

4.7 Disposal of Computers and Other Electronic Devices

POLICY:

All electronic equipment and storage devices will be erased and data made inaccessible before their disposal. This includes all devices with data storage including computers, voice mail systems, computer file storage devices, copiers, fax machines, cell phones and other communication devices.

PROCEDURE:

1. Disposal of any electronic devices containing confidential or sensitive information will be done by a person authorized to do so by the Executive Director.

2. When an SSICS electronic device is disposed of through the garbage or recycling process the file storage hardware will be destroyed or disabled.

3. When an SSICS electronic device is disposed of through sale or gifting for future use by others all data stored will be removed by an authorized technician.

5. Risk Management

5.1 Risk Management Plan

POLICY:

A Risk Management Plan will be prepared by the Executive Director. The plan will identify and assess actual and potential risks to SSICS, and present risk management actions include risk avoidance, prevention, reduction and transfer/insurance.

PROCEDURE:

1. The Risk Management Plan will be developed by the Executive Director on an annual basis and presented to the Board of Directors for approval.

2. The Risk Management Plan will include: an analysis of current and potential risks; identification of risk reduction strategies; insurance coverage; and quality improvement objectives and actions.

3. The Executive Director, with the assistance at times of other qualified resources, will provide the Board of Directors and managers with information on current best practices in risk management practices applicable to SSICS operations.

5.2 Insurance and Inventory of Assets

POLICY:

SSICS will carry a level of property and liability insurance to ensure the organization, its Directors, employees and volunteers are adequately protected in the event of theft, damage or loss of property, or legal action.

PROCEDURE:

1. Insurance will include comprehensive liability and property coverage, directors and officers errors and omissions, professional liability, vehicle comprehensive and liability, and, when required, exceptional insurance for events and projects.

2. In some cases insurance may be provided by a third party (i.e. Province of BC Master Insurance program).   In the case where the insurance provided by the third party does not meet the standard determined in the SSICS Risk Management Plan additional coverage will be purchased to achieve the appropriate level.

3. Insurance coverage will be reviewed annually prior to renewal.

4. Adding, deleting or altering insurance coverage requires approval from the Executive Director and Board of Directors.

5. Insurance documents will be stored securely in paper or electronic form in an accessible location in the SSICS administration office.

6. An inventory will be maintained detailing SSICS property in each work area, identifying items in excess of one hundred dollars in value. The inventory will be updated as purchases and disbursements occur.

7. A complete inventory of property will be maintained for the purpose of providing evidence of property in case of an insurance claim. The inventory of assets will be stored securely in an accessible location in the SSICS administration office.

5.3 Warrants, Arrests or Subpoenas

POLICY:

Employees will comply with legal warrants, arrests, investigations searches of employees, program participants, or other matters related to SSICS activities. Requests from lawyers do not in and of themselves constitute a legal requirement to require release of documents or information.

PROCEDURE:

1. When a request is made for any warrant, search or legal request for information a supervisor or Executive Director will confirm the authority and legitimacy of the request before providing access to worksites, files, or other material.

2. Employees will inform the supervisor immediately of any warrant, arrest, subpoenas, search or investigation related in any way to their work with SSICS.

3. Information release through a legitimate legal process will comply with the Freedom of Information and Protection of Privacy Act and the Personal Information Protection Act. Information will be released by a supervisor or Executive Director after consultation with the SSICS Privacy Officer. The required material will be placed in a sealed envelope and delivered directly to the authorized legal recipient.

4. Information requests from lawyers will typically be granted unless supported by a written official court request. Those requests may be considered through a review by the Privacy Officer, including confirming consent from the individual involved. In these cases a handling fee will typically be applied.

5.4 Reporting Waste, Fraud, Abuse and Ethical Breaches

POLICY:

SSICS encourages and expects any employee or volunteer to report waste, fraud, abuse or ethical breaches evident within SSICS. Reports of such events will be received confidentiality without any risk of reprisal or personal consequence.

PROCEDURE:

1. Reports of fraud, waste, abuse, ethical breach or other such wrongdoings will be made in writing or verbally to a supervisor or the Executive Director.

2. A supervisor receiving such a report will inform the Executive Director.

3. In cases of alleged wrongdoing by the Executive Director the report will be made in writing or verbally to the Board Chair.

4. Allegations will be taken seriously, investigated, and treated with sensitivity and discretion. An investigation will follow SSICS Complaints and Suggestions policy and procedures.

5.5 Legal Counsel

POLICY:

SSICS may retain legal counsel from time to time for legal advice or action. This may involve different lawyers in different circumstances, as legal counsel will be retained based on their knowledge and experience on the subject matter

PROCEDURE:

1. The Executive Director will contact a lawyer for legal advice at any time relating to routine operational issues. Authority to proceed with legal action will be approved by the Board of Directors.

2. The Board of Directors may contact a lawyer for legal advice pertaining to the governance or business not related to routine operations after a Board motion has approved such action.

3. The Board will be informed of, and confirm as appropriate, the retention of particular lawyers or firms to act as counsel to SSICS.

4. The Executive Director or the Chairperson of the Board of Directors will represent the Society in communication on legal matters. Other representatives may be appointed by the Executive Director or Board.

5. Any SSICS employee will seek authorization from the Executive Director before contacting legal counsel regarding business or situations in any way related to SSICS.

5.6 Contracts and Legal Agreements

POLICY:

SSICS will be a responsible and reliable party in all contracts and agreements entered into. Contracts and agreements will be reviewed by individuals knowledgeable in the content area to ensure understanding, and all contracts and agreements will be signed by the Executive Director and/or Board of Directors. Contracts and legal agreements include, but are not limited to: service agreements and other agreements with funders, labour agreements, leases of property or equipment, mortgages and other loans, agreements for contracted services, purchase and sale agreements, user agreements (eg. software, web-based services), legal compliance agreements, permits and licenses, and insurance contracts,

PROCEDURE:

1. The Executive Director will review agreements prior to signing, and include others with specific expertise to interpret and advise on agreements when required.

2. The Executive Director will develop agreements with other parties when one does not exist or is provided, and include others with specific expertise to interpret and advise on developing these agreements when required.

3. Agreements and contracts will be signed by SSICS based on the requirement of the given document, where Board of Directors sign when required. In cases when two signature required, not specifying exclusively Board signatures, The Executive Director may sign with a Board Member. In cases where one signature is required the Executive director will sign on behalf of SSICS unless otherwise specified by the other party or SSICS Board of Directors.

4. The Board will be informed of, and confirm as appropriate, the retention of particular lawyers or firms to act as counsel to SSICS.

5. Contracts and agreements will be stored securely and confidentially in either paper or electronic form, and will not be shared or release without approval form the Executive Director.

6. The non compliance of SSICS or the other parties to terms of the agreement will be reported to the Executive Director for review and

action, and to the Board of Directors if the circumstances pose significant risk to the organization in any way.

7. Compliance with legal agreements and contracts will be reviewed by the Executive Director annually and noted in the Annual Management Report and Performance Improvement Plan

5.7 Compliance with Legal and Regulatory Requirements

POLICY:

The Executive Director will perform the duties of a Compliance Officer for SSICS and ensure the organization is at all times in all activities compliance with all forms of legal and regulatory requirements.

PROCEDURE:

1. The Executive Director will contact a lawyer for legal advice at any time relating to routine operational issues. Authority to proceed with legal action will be approved by the Board of Directors.

2. The Board of Directors may contact a lawyer for legal advice pertaining to the governance or business not related to routine operations after a Board motion has approved such action.

3. The Board will be informed of, and confirm as appropriate, the retention of particular lawyers or firms to act as counsel to SSICS.

4. The Executive Director or the Chairperson of the Board of Directors will represent the Society in communication on legal matters. Other representatives may be appointed by the Executive Director or Board.

8. Any SSICS employee will seek authorization from the Executive Director before contacting legal counsel regarding business or situations in any way related to SSICS.

9. Compliance with legal and regulatory requirements will be reviewed by the Executive Director annually and noted in the Annual Management Report and Performance Improvement Plan

6. Property Management

6.1 Facilities and Capital Replacement Plan

POLICY:

SSICS will prepare, maintain, and update a Facilities and Capital Replacement Plan. The plan will identify maintenance, replacement and improvement schedules, priorities and projected costs for SSICS property, buildings, vehicles, major appliances and other capital assets.

PROCEDURE:

1. A Facilities and Capital Replacement Plan will be prepared an annual basis and be presented as part of the Financial Plan to the Board of Directors for approval.

2. The plan will include: an identification of health and safety priorities for each building; a projection of major upgrades, repairs and replacement of buildings; projected replacement schedules and cost for equipment such as vehicles and major appliances; identification of additional improvements to buildings and property to ensure their functionality, accessibility and attractiveness.

3. The plan will provide general estimates of financial resources to be built into the annual maintenance budgets and to be retained in reserve for future capital needs.

6.2 Security of Facilities and Equipment

POLICY:

SSICS buildings, work areas, vehicles and other equipment will be kept secure when not in use, and only those people requiring use of the property will have access to the area or equipment outside of hours of operation.

PROCEDURE:

1. All buildings, work areas within each building and secure storage within each work area will have the appropriate locks or other devices. Keys will be restricted to designated employees for each area.
2. An inventory of key distribution and access codes will be maintained and updated on an ongoing basis.
3. Photocopier, computers and telephones will have access and security measures limiting access to designated employees.
4. Locks and access codes will be changed when required to limit unwanted access (e.g. after a security breach or a period of time without change).
5. People given access to facilities and equipment including employees, volunteers and contractors will be screened to determine the appropriate level of access to be granted.
6. Specific employees at each work site will be designated to secure that site at the end of the work day following a standard lock up checklist and protocol.
7. Employees accessing buildings outside of work hours will follow proper security measures for that site.
8. Security breaches, unsecured facilities, or other security concerns will be reported to a supervisor or Executive Director immediately.

6.3 Maintenance of Facilities and Equipment

POLICY:

SSICS buildings, work areas, vehicles and other equipment will be maintained in a safe and functional state.

PROCEDURE:

1. Regular health and safety inspections of work areas and vehicles will include the identification of building and equipment maintenance issues.

2. Facilities and equipment will comply with all regulations, zoning and specifications for their proper use.

3. Equipment will be replaced in a timely manner prior, whenever possible, to there being a safety or productivity concern.

4. Faulty or dangerous equipment or unsafe work areas will be restricted from use, and repaired or replaced before use is resumed.

6.4 Equipment Use

POLICY:

SSICS worksites and equipment are for use by employees only for work-related purposes. This includes vehicles, telephones, fax, computers, photocopier, office equipment and other equipment.

PROCEDURE:

1. Use of equipment and work space for other than SSICS activities, or by people other than SSICS employees may be permitted, at times, with the approval of the supervisor or Executive Director. Costs for personal use of equipment, including phone and fax long distance, cellular phone air time, photocopy supplies or other office supplies will be reimbursed the employee upon request. Use of equipment for approved non work purposes will typically be limited to outside of regular office hours.

2. Unauthorized use of SSICS worksites and equipment may result in disciplinary action.

7. Financial Management

7.1 Financial Plan and Budget

POLICY:

A Financial Plan and Operating Budget will be prepared by the Executive Director to ensure the responsible management of resources, and ensure that SSICS is financially stable in the present and future. The plan will review systems for accounting and cost management, budgeting and cost projection processes, forecast future activities and financial needs, and plans for raising funds. The budget will include income and revenue projections for each program area, and will be reviewed regularly to monitor the financial status throughout the year.

PROCEDURE:

1. The annual Financial Plan will be developed by the Executive Director and presented to the Finance Committee for discussion and amendments, and then the Board of Directors for final approval.

2. The Financial Plan will include: an annual budget; analysis of financial needs; identification of issues such as cost controls, accountability, and legal compliance; and quality improvement objectives and actions.

3. The financial (fiscal) year for the organization will be from April 1 to March 31. Activities which may require external reporting or financial planning on a time period other than this (i.e. overlapping two fiscal years) will be reported on SSICS financial statements within the established fiscal year format.

4. Budgets will include projected income and detailed expense projections. Budgets will be in place to cover each program, each projects and overall administrative support. These budgets will be combined into an annual consolidated budget that will be approved by the Board of Directors within two months of the commencement of the fiscal year.

5. The Board may approve an interim budget if significant income or expense items have yet to be determined.

6. Budgets for new programs, or changes to budgets during the year, require new or amended budgets before expenses are incurred.

7. The overall annual budget will be reviewed and adjusted as required mid-year, and presented to the Finance Committee and Board for approval if significant changes occur.

7.2 Accounting Practices

POLICY:

SSICS accounting practices will conform to generally accepted bookkeeping and accounting practices as defined by the Canadian Institute of Chartered Accountants.

PROCEDURE:

1. All accounting, billing, coding and payroll tasks will be completed by employees trained and experienced in the relevant accounting practices.

2. When guidelines and specific practices regarding accounting practices with SSICS are developed or changed the new practice will conform to standards of the Canadian Institute of Chartered Accountants.

3. An annual financial audit will be commissioned to comment and advise on accounting practices and make recommendations for areas of change and improvement.

4. Audits of specific programs or projects will be commissioned if required by funders or regulations.

7.3 Financial Reporting

POLICY:

Financial reporting will provide clear, accurate and complete disclosure of financial activity and status in a timely fashion. Reporting will comply with legal requirements including, but not limited to, the BC Societies Act, Revenue Canada, and terms of contracts and agreements. Financial reporting will permit SSICS to identify financial issues and concerns at the earliest point possible.

PROCEDURE:

1. Monthly financial statements will be prepared by the Financial Administrator for distribution to program managers, Executive Director, and the Finance Committee of the Board of Directors. Reports will include income and expense to date and a comparison against budget. Reports may also include items such as comparison to previous year and projected and actual income/expense variances.

2. Additional financial reports or financial analysis to provide specific information not readily available in the monthly statements will be prepared as needed by the Financial Administrator, managers, or Executive Director.

3. Reports will be provided to funders or other external authorities in compliance with contract requirements or specific request. Reports will be reviewed and approved by the Executive Director prior to release.

4. Financial records will be stored securely at the administrative site and kept confidential.

5. There will be a clear separation of duties and responsibilities in all financial activities to ensure there is accountability and the appropriate level of checks and balances in managing income and expenses. Accounting and payroll functions will be performed by individuals separate from individuals with expense authorization functions.

7.4 Spending Authority

POLICY:

Authority to spend funds will be limited to the Executive Director and employees delegated by the Executive Director. Purchases and expenses will be within specific spending limits and in compliance with expense projections in approved budgets unless approval is obtained.

PROCEDURE:

1. No payment will be issued without the approval of the Executive Director or a manager delegated with expense approval authority.

2. Managers will typically approve expenditures within their program areas. In the absence of the manager, the Executive Director will approve an expense in that program area.

3. Managers require approval from the Executive Director to spend beyond the limits of an established program budget and for any expense in excess of $ 1,000.

4. The Executive Director requires approval from the Board of Directors for any unbudgeted expense in excess of $5,000.

5. The Executive Director may delegate spending authority to others at times, including employees and contractors. In these situations the terms, conditions and limits of the spending authority will be agreed upon in writing. This includes the assignment of a petty cash float to an employee for program use.

7.5 Borrowing

POLICY:

SSICS may borrow funds from time to time for projects, capital expenses, improvements, or other significant expenses through a proper legal lending agreement. The Board of Directors will be informed of borrowing details and terms, and approve the agreement.

PROCEDURE:

1. SSICS may maintain a line of credit at a financial institution to be used to cover any expenses within the annual budget or exceptional expenses approved by the Board of Directors.

2. Entering into a loan or mortgage agreement requires approval from the Board of Directors.

7.6 Audit

POLICY:

SSICS will appoint a qualified external auditor to complete an annual review of financial activity and records. SSICS will comply with the BC Societies Act, Revenue Canada and terms of funding contracts regarding audit requirements.

PROCEDURE:

1. The audit will be completed at the end of each fiscal year, with the audited statements prepared for presentation at the Annual General Meeting. The Board of Directors will approve the audited statement prior to public release.

2. The audit will include a review of all financial activity and records for the fiscal year with a particular focus on payroll and other items agreed upon by SSICS and the auditor.

3. Recommendations from the audit will be reviewed by the Finance Committee and Executive Director to plan for any improvements as part of the financial plan for the following year.

4. The Auditor for the upcoming year will be appointed by members of the Society at each Annual General Meeting.

5. The annual audited financial statement will be available to public and summarized in the Annual Report.

7.7 Petty Cash

POLICY:

Petty cash floats may be used at times to facilitate the day to day operations of a program, project or event. Cash on hand will be limited to what is required for day to day program and administration operations to minimize the risk of theft or loss.

PROCEDURE:

1. Petty cash will be signed out to designated employees who will assume responsibility for reconciling the amount and maintaining records of expenses.

2. Programs may be issued a single petty cash disbursement or ongoing float depending on operational needs.

3. Cash will be reconciled and fully accounted for with receipts on a monthly basis, or more frequently at times.

4. Petty cash will be stored securely with access limited to designated employees.

5. Spending limits, method and timing or reconciliation, and other such details on how petty cash is managed may be determined on a program by program or case by case basis by the supervisor, Executive Director or Financial Administrator.

7.8 Sale of Property

POLICY:

The sale or donation of equipment or property will be based on fair market value and/or benefit to a worthy cause. Employees or directors will not benefit from any advantage over the general public when equipment or property is sold or donated.

PROCEDURE:

1. Property will be disposed of at fair market value to employees and the general public or at a lesser value to worthy community causes consistent or complimentary to the mission of SSICS.

2. Employees will have a fair and equal opportunity to purchase property designated for disposal at the determined fair market value.

3. Sale or other disposal of items in excess of $5,000 in fair market value requires the approval of the Board of Directors.

7.9 Purchasing

POLICY:

SSICS will purchase goods and services from suppliers or contractors based on quality, cost and convenience of the transaction. Purchasing from local sources whenever possible will be a consideration.

PROCEDURE:

1. When purchasing major items or services, valued over $ 5,000, several quotes on the product or service and price will be obtained. An evaluation of quality, cost and convenience will determine the final purchasing decision. In cases where SSICS has an ongoing relationship with a supplier or contractor who has provided good value to SSICS the requirement for multiple quotes may be waived by the Executive Director.

2. Purchasing practices, ongoing purchasing commitments, and relationships with preferred suppliers will be reviewed on an ongoing basis by the Executive Director and Financial Administrator as part of the financial planning process.

3. Purchasing will only be done by SSICS employees with designated spending or purchasing authority, except in the case of approved work-related expenses of employees.

7.10 Investment of Funds

POLICY:

Funds exceeding the amount required for regular operations and operating contingencies will be invested to earn revenue. Investments will be managed in a prudent manner, have low risk exposure, and be consistent with the overall SSICS financial plan.

PROCEDURE:

1. The nature and terms of investments will be part of the overall financial plan. Investment planning will ensure adequate funds are available for operations including cash on hand and that invested funds are available as a contingency if needed.

2. Funds will be invested at the discretion of the Board of Directors based upon safe and prudent considerations.

3. The Board will determine the extent to which the Executive Director and Financial Manager may manage the renewal and re-investment of low risk investments at current financial institutions (eg. term deposits). Investments of greater than $50,000, of a term greater than one year, or at a new financial institution require the approval of the Board of Directors.

4. Investments will be insurable, including securities that are insurable by the Canadian Deposit Insurance Corporation or insurable property.

5. SSICS may obtain external investment advice. Any financial advisors will be approved by the Board of Directors after being determined to have experience and credentials and be free of any conflicts of interest.

6. The use of investment earnings will comply with any terms of externally or internally-restricted funds held by SSICS.

7.11 Fundraising and Marketing

POLICY:

Fundraising and marketing activities will be coordinated, well-planned and ethical to maximize effectiveness and maintain a positive relationship with the community and donors. Fundraising activities may be conducted for ongoing operations and for specific projects and capital campaigns. Fundraising practices will comply with the Ethical Fundraising and Financial Accountability Code of Imagine Canada.

PROCEDURE:

1. SSICS will maintain its status as a federally registered charity organization and will comply with Revenue Canada regulations required of registered charities.

2. A review of compliance with the Ethical Fundraising and Financial Accountability Code will be done on an annual basis as part of the Financial Plan.

3. Fundraising may be initiated and implemented by the Board of Directors and employees. In each case the specific fundraising activity will be approved by the Executive Director. New fundraising activities significantly different than typical activities done in the past will be approved by the Board of Directors.

4. Fundraising events and campaigns undertaken by other groups or individuals in collaboration with, or for the benefit of, SSICS will comply with standards and ethics consistent with the mission of SSICS that do not reflect negatively on the image of SSICS.

5. Public communication and public relations materials related to fundraising will follow communication policies and procedures and require the approval of the Executive Director.

7.12 Charitable Donations

POLICY:

SSICS will accept charitable donations of cash, cash equivalent such as securities, or major items of property that would benefit the organization. Donations of small property items and other "gifts in kind" will not be eligible for a tax receipt. All donations will be used to further the mission of the organization.

SSICS will comply with Canada Revenue regulations in all matters pertaining to issuing charitable receipts. Tax receipts may only be issued for donations that legally qualify as gifts. Donations of services, such as time, skills, and effort are not considered transfers of property and therefore, are not eligible for a tax receipt.

PROCEDURE:

1. Charitable receipts will be issued for donations of 20 dollars or more.
2. Charitable receipts will be issued annually.
3. Cash equivalents such as securities, or planned giving options such as life insurance policies are eligible for a tax receipts.
4. Major property eligible for tax receipt may include land, buildings, vehicles or other major items determined by SSICS to have value.
5. The tax receipt amount for donations of cash equivalent or property will be based on the fair market value on the donation on the day of transfer to the organization. SSICS will complete any appraisal deemed necessary to determine fair market value.
6. Gifts-in-kind not considered to be major may be accepted by SSICS if the items benefit service delivery (eg. food, clothes, furniture etc), but will not receive tax receipts.
7. SSICS respects the privacy of its donors and only publish names of donors with their permission.