

Title: Personal Protection & Privacy Policy (PIPA)		
Document # 1.6 Governance	Prepared By: Darla Simpson, Director of Human Resources	Date Prepared: November 22, 2018
Effective Date: June 1, 2019	Reviewed By: Dave Putney, IT Lead	Date Reviewed: May 10, 2019
Codes and Standards: BC Personal Information and Privacy Act	Approved By: Brad White, President	Date Approved: June 28, 2019

Policy

At SES Consulting, we are committed to providing our employees and clients with a healthy, respectful work environment and a high-quality product that helps accelerate the transition to a carbon neutral economy. As providing this service involves the collection, use and disclosure of some personal information about our employees and clients, protecting their personal information is one of our highest priorities.

We have always respected our employees and client's privacy and safeguarded their personal information, and this policy reflects our compliance with British Columbia's *Personal Information Protection Act* (PIPA). PIPA, which came into effect on January 1, 2004, sets out the ground rules for how B.C. businesses may collect, use and disclose personal information.

Purpose

We will inform our employees and clients of why and how we collect, use and disclose their personal information, obtain their consent where required, and only handle their personal information in a manner that a reasonable person would consider appropriate in the circumstances.

This Personal Information Protection Policy, in compliance with PIPA, outlines the principles and practices we will follow in protecting employee and client personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of our employees and client's personal information and allowing our employees or clients to request access to, and correction of, their personal information.

Scope

This Personal Information Protection Policy applies to SES Consulting and to any service providers collecting, using or disclosing personal information on behalf of SES Consulting. This includes payroll and benefits companies with staff information, and all project subcontractors.

Responsibilities

1 Collecting Personal Information

- 1.1 Unless the purposes for collecting personal information are obvious and the employee or client voluntarily provides his or her personal information for those purposes, we will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.

1.2 We will only collect employee or client information that is necessary to fulfill the following purposes:

- To verify identity;
- To identify [client, customer, member] preferences;
- To deliver requested products and services;
- To guarantee a travel or hotel reservation;
- To provide [medical, dental, counselling] services;
- To enrol the client in a program;
- To ensure a high standard of service to our [clients, customers, members];
- To meet regulatory requirements

2 Consent

2.1 We will obtain employee or client consent to collect, use or disclose personal information (except where, as noted below, we are authorized to do so without consent).

2.2 Consent can be provided orally, in writing, electronically, through an authorized representative or it can be implied where the purpose for collecting using or disclosing the personal information would be considered obvious and the employee or client voluntarily provides personal information for that purpose.

2.3 Consent may also be implied where an employee or client is given notice and a reasonable opportunity to opt-out of his or her personal information being used for mail-outs or the marketing of new services or products and the employee or client does not opt-out.

2.4 Subject to certain exceptions (e.g., the personal information is necessary to provide the service or product, or the withdrawal of consent would frustrate the performance of a legal obligation), employees and clients can withhold or withdraw their consent for SES Consulting to use their personal information in certain ways. An employee's or client's decision to withhold or withdraw their consent to certain uses of personal information may restrict our ability to provide a particular service or product. If so, we will explain the situation to assist the employee or client in making the decision.

2.5 We may collect, use or disclose personal information without the employee's and client's knowledge or consent in the following limited circumstances:

- When the collection, use or disclosure of personal information is permitted or required by law;
- In an emergency that threatens an individual's life, health, or personal security;
- When the personal information is available from a public source (e.g., a telephone directory);
- When we require legal advice from a lawyer;
- For the purposes of collecting a debt;
- To protect ourselves from fraud;
- To investigate an anticipated breach of an agreement or a contravention of law;
- On behalf of another organization if the individual previously consented to the collection /disclosure and the personal information is disclosed to or collected by the organization solely for the purposes for which the information was previously collected, and to assist that organization to carry out work on behalf of the other organization.

3 Using and Disclosing Personal Information

- 3.1 We will only use or disclose employee or client personal information where necessary to fulfill the purposes identified at the time of collection or for a purpose reasonably related to those purposes such as:
- To conduct employee or client surveys in order to enhance the provision of our services;
 - To contact our clients directly about products and services that may be of interest;
 - To a client by whom we've been contracted to deliver a product or service to a private individual on the client's behalf.
- 3.2 We will not use or disclose employee and client personal information for any additional purpose unless we obtain consent to do so.
- 3.3 We will not sell employee and client lists or personal information to other parties.

4 Retaining Personal Information

- 4.1 If we use employee and client personal information to make a decision that directly affects the employee and client, we will retain that personal information for at least one year so that the employee and client has a reasonable opportunity to request access to it.
- 4.2 Subject to policy 4.1, we will retain employee and client personal information only as long as necessary to fulfill the identified purposes or a legal or business purpose.

5 Ensuring Accuracy of Personal Information

- 5.1 We will make reasonable efforts to ensure that employee and client personal information is accurate and complete where it may be used to make a decision about the employee and client or disclosed to another organization.
- 5.2 Employees and clients may request correction to their personal information in order to ensure its accuracy and completeness. A request to correct personal information must be made in writing and provide sufficient detail to identify the personal information and the correction being sought. A request to access personal information should be forwarded to the Director of Human Resources or their designate Privacy Officer.
- 5.3 If the personal information is demonstrated to be inaccurate or incomplete, we will correct the information as required and send the corrected information to any organization to which we disclosed the personal information in the previous year. If the correction is not made, we will note the employee and client correction request in the file.

6 Securing Personal Information

- 6.1 We are committed to ensuring the security of employee and client personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

Security measures used include, but are not limited to:

- Locked filing cabinets, restricted access to information on a "need-to-know" basis, User Id's and Passwords, anti-virus software, data encryption, firewalls, and data back-ups.
- We use appropriate security measures to destroy computer hard drives that contain personal information before they are discarded.
- We continually review and update our security policies and controls as technology changes to ensure ongoing personal information security.

- 6.2 We will use appropriate security measures when destroying employees', clients' personal information such as shredding paper documents and secure-deleting electronically stored information.
- 6.3 We will continually review and update our security policies and controls as technology changes to ensure ongoing personal information security.

7 Providing Employees and Clients Access to Personal Information

- 7.1 Employees and Clients have a right to access their personal information, subject to limited exceptions.
- Disclosure would reveal personal information about another individual
 - Health and safety concerns
- 7.2 A request to access personal information must be made in writing and provide sufficient detail to identify the personal information being sought. A request to access personal information should be forwarded to the Director of Human Resources or their designate Privacy Officer.
- 7.3 Upon request, we will also tell employees and clients how we use their personal information and to whom it has been disclosed if applicable.
- 7.4 We will make the requested information available within 30 business days, or provide written notice of an extension where additional time is required to fulfill the request.
- 7.5 A minimal fee may be charged for providing access to personal information. Where a fee may apply, we will inform the employees and clients of the cost and request further direction from the employees and clients on whether or not we should proceed with the request.
- 7.6 If a request is refused in full or in part, we will notify the employees and clients in writing, providing the reasons for refusal and the recourse available to the employees and clients.

8 Questions and Complaints: The Role of the Privacy Officer or designated individual

- 8.1 The Privacy Officer or designated individual is responsible for ensuring SES Consulting's compliance with this policy and the *Personal Information Protection Act*.
- 8.2 Employees and clients should direct any complaints, concerns or questions regarding SES Consulting's compliance in writing to the Privacy Officer. If the Privacy Officer is unable to resolve the concern, the employees and clients may also write to the Information and Privacy Commissioner of British Columbia.

Contact information for SES Consulting's Privacy Officer is privacyofficer@sesconsulting.com, 604.568.1800

Definitions

Personal Information – means information about an identifiable individual, including name, age, home address and phone number, social insurance number, marital status, religion, income, medical information, education, employment information. Personal information does not include contact information (described below).

Contact information – means information that would enable an individual to be contacted at a place of business and includes name, position name or title, business telephone number, business address, business email or business fax number. Contact information is not covered by this policy or PIPA.

Privacy Officer – means the individual designated responsibility for ensuring that SES Consulting complies with this policy and PIPA.