

NeXafe Solutions Corp. (NeXafe) incorporates into its Privacy Policy the provisions of Part 1 of the Personal Information and Electronic Documents Act (PIPEDA - Government of Canada), the principals of the Personal Information Protection Act (PIPA - Government of Alberta) and the ten Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information (CAN/CSA-Q830-96).

1. Accountability

NeXafe's Privacy Officer is accountable for ensuring compliance with NeXafe's Privacy Policy, including by all individuals within NeXafe who may be responsible for the day-to-day collection and processing of personal information.

NeXafe is responsible for all personal information in its possession or control, including information that has been transferred to a third-party for processing. NeXafe will use contractual or other means to provide an appropriate level of protection when a third-party processes information on behalf of NeXafe.

NeXafe will maintain our commitment to privacy by:

- implementing procedures to protect personal information,
- establishing procedures to receive and respond to complaints and inquiries,
- training staff and communicating to staff information about the company's policies and practices, and
- developing information to explain the company's policies and procedures.

2. Identifying Purposes

NeXafe will identify the purpose for which personal information will be collected at or before the time the information is collected.

NeXafe will document the purposes for which personal information is collected in order to comply with the Openness principle and the Individual Access principle.

NeXafe will only collect information necessary for the defined purposes.

NeXafe will verbally or in writing, inform the individual from whom personal information is requested, and the purpose for the collection of the personal information at or before the time for which personal information is collected.

When personal information is collected for a new purpose not previously identified, NeXafe will identify this purpose to the individual prior to use of the collected information. Unless the new purpose is required by law, consent will be obtained from the individual before the information is used for that purpose.

NeXafe collects personal/contact information to:

- Manage customer accounts

- Follow-up with individuals to determine their interest in the products and services provided by NeXafe and inform them of new products, services, or promotions
- Screen individuals for employment or contracting suitability
- Manage and administer personnel (including performance appraisals, security, access control and disciplinary measures)
- Manage and administer compensation and benefits programs
- Administer payroll
- Administer occupational health and safety programs
- Monitor and track skills and competency development
- Meet legal and regulatory requirements (e.g., Employment Standards Legislation, Canada Customs and Revenue Agency reporting requirements)
- Facilitate NeXafe audits when required to do so
- Provide contact information of NeXafe staff to NeXafe insurers
- Provide such information as may be required for the administration of NeXafe programs

NeXafe is not responsible for the management of Personal Information collected by its customers through the use of NeXafe products and services. However, NeXafe employs reasonable measures to ensure the safety and protection of its customers' information. NeXafe employs strict policies and procedures to protect and maintain the confidentiality of this information. These measures are outlined in the contracts signed by NeXafe customers. Furthermore, NeXafe considers all information collected by its customers as confidential and does not access or use its customer's information other than for customer service, data maintenance, auditing, or trend analysis (e.g., benchmarking).

3. Consent

NeXafe obtains consent as required for the collection, use and disclosure of personal information and uses reasonable efforts to ensure that individuals understand how their personal information will be used.

NeXafe obtains consent at the same time personal information is collected. However, it may, at times, obtain consent to use and disclose personal information after it has been collected, but before it is used or disclosed for a new purpose.

The sensitivity of the information and the reasonable expectations of the individual determine the form of consent. Express consent will be requested when the information is likely to be considered sensitive; implied consent will be accepted when information is less sensitive. In some cases, consent may be obtained through an individual's authorized representative (such as a legal guardian or a person having power of attorney).

NeXafe may use written, verbal, or digital means for obtaining consent for the collection, use or disclosure of information.

In certain circumstances, personal information may be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the

individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent.

Consent may be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice. NeXafe and/or the Privacy Officer then inform individuals of the implications of withdrawing consent.

4. Limiting Collection

NeXafe limits the amount and type of personal information collected to that which is necessary for the identified purpose.

NeXafe collects information by fair and lawful means.

NeXafe may collect the following information from employees, contractors, and suppliers:

- Demographic and contact information including home address and telephone number, date of birth, and social insurance number
- Training, experience, and skills as necessary to establish competence, and regulatory, employer or industry standards compliance
- Education and employment history
- Banking or financial information
- Health information
- Security background checks

NeXafe may collect the following personal information from customers of NeXafe:

- Names and contact information, including home address and telephone numbers
- HSE program documentation (e.g., policies, procedures, practices, and forms) and data included in reports of incidents, hazards, workplace inspections, preventive maintenance programs, safety meetings, safety training and other relevant indicators of safety performance
- Demographic information about the customer(s) for NeXafe programs, including the number of employees, and interest in programs or functionalities for system planning purposes
- Financial information, if members are involved in programs with financial eligibility requirements, or where payment is required for programs or services.

NeXafe may collect personal information through the following means:

- Solicited and unsolicited resumes and correspondence
- Completed application forms (paper or online format) for employment, benefits, grants and bursaries, business, and other program registrations, etc.
- Worksite audits, inspections, and assessments in person and through telephone interviews
- Online forms through the website

5. Limiting Use, Disclosure and Retention

NeXafe does not use or disclose personal information other than for the purpose for which it was collected, except with the consent of the individual or:

- As required or authorized by law;
- In the event that it is required by legal counsel representing NeXafe;
- As required to collect a debt owed by the individual to NeXafe;
- As required to comply with a subpoena, warrant or court order;
- When the information is publicly available; or
- To a public authority in the event of imminent danger to any individual.

Only NeXafe employees or contractors with a business need-to-know, or whose duties so required, are granted access to personal information.

NeXafe has developed guidelines and implemented procedures with respect to the retention of personal information. NeXafe retains personal information only as long as it is necessary for the identified purpose, or as required by law. Where personal information is used to make a decision about an individual, NeXafe retains the information, or the rationale for making the decision, long enough to allow the individual access to the information after the decision has been made.

Personal information that is no longer required to fulfill the identified purposes or required by law to be retained is destroyed, erased, or made anonymous.

6. Accuracy

NeXafe provides our best efforts to ensure that personal information collected, used, and disclosed is as accurate, complete, and up to date as necessary for the purposes for which it is to be used.

Personal information is kept sufficiently accurate, complete, and up to date to minimize the possibility that inappropriate information may be used to make a decision about the subject individual.

NeXafe updates personal information as and when necessary to fulfill the identified purpose or upon notification by the individual who is the subject of the information.

7. Safeguards

NeXafe protects personal information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification, or destruction, regardless of the format in which it is held.

NeXafe has developed and implemented information security policies and procedures that outline physical, organizational, and technological measures in place to protect personal information as appropriate to the sensitivity of the information. These same measures are employed in the safeguarding and protection of information resources of NeXafe customers.

NeXafe protects personal information disclosed to, or processed by third parties by contractual agreements which address the following as necessary:

- Identifying the types of records provided, collected, created, or maintained in order to deliver the service, and specifying any applicable privacy legislation
- Stipulating the confidentiality of the information and the purposes for which it is to be used
- Identifying the organization(s) having custody and control of the records, including the responsibility and process for handling requests for access to information
- Ensuring that third parties and their employees having access to NeXafe, and information assets are aware of, and understand their responsibility to adhere to

NeXafe information handling and security policies, including maintaining the confidentiality of personal information

- Ensuring that NeXafe has access to information produced, developed, recorded, or acquired by third parties as a result of the contract, including timely access in response to requests for information, and specifying that third parties shall not deny access to, or retain custody of, personal information because of late or disputed payment for services
- Requiring third parties to report breaches of confidentiality and privacy to NeXafe Privacy Officer within 48 hours of knowing that the breach occurred
- Addressing disaster recovery and backup of any information assets and systems in the custody of the third party
- Addressing the disposition (e.g., destruction or return) of all NeXafe information assets (e.g., records, hardware, system documentation) upon termination of the contract
- Specifying any audit or enforcement measures that NeXafe will undertake to ensure that third parties comply with information handling and security provisions outlined in contractual agreements (for example, non-disclosure agreements, audit trails, regular review of third-party access requirements, inspection of third-party premises).

NeXafe ensures that all employees are aware of its privacy policies and procedures and understand the importance of maintaining the confidentiality of personal information.

Care shall be taken in the disposal or destruction of personal information to prevent unauthorized parties from obtaining access to the information.

8. Openness

Upon request, NeXafe makes available specific information about its policies and practices relating to the management of personal information, including:

- The means of gaining access to personal information held by NeXafe;
- Identification of personal information held by NeXafe, and a general account of its use;
- NeXafe Privacy Policy, guidelines and related procedures are posted and available on our website;
- Reference to the statement of NeXafe Privacy Policy on NeXafe website, if applicable.

To make an inquiry or lodge a complaint about NeXafe personal information handling policies and procedures, contact:

NeXafe Privacy Officer
customer.care@NeXafe.com

9. Individual Access

Upon request, NeXafe provides individuals with access to their personal information held by the company. Individuals have the right to challenge the accuracy and completeness of their personal information held by NeXafe, and to have it amended as appropriate.

All requests by individuals (e.g., customers, employees, contractors) to access their personal information held by NeXafe, or to correct or amend their personal information, should be directed to the designated Privacy Officer. Such requests should be in writing.

NeXafe responds to requests for access to personal information within 30 business days.

Responding to an individual's request for information is usually done at no or minimal cost to the individual. However, a fee for reasonable costs incurred may be charged when responding to more complex requests, provided the individual is informed in advance.

To safeguard personal information, NeXafe may request sufficient information from the individual to verify that person's identity.

Limitations to Individual Access

NeXafe provides individuals access to their personal information, subject to limited and specific exceptions. NeXafe will refuse access to personal information if:

- NeXafe has disclosed information to a government institution for law enforcement or national security reasons;
- It would reveal personal information about a third party unless there is consent or a life-threatening situation;
- Doing so could reasonably be expected to threaten the life or security of another individual;
- The disclosure would reveal confidential commercial information; or
- The information is protected by solicitor-client privilege.

If access to information is refused, NeXafe shall, in writing, inform the individual of the refusal, the reason(s) for the refusal, and any recourse the individual may have to challenge NeXafe decision.

Correction/Amendment of Personal Information

NeXafe corrects or amends personal information as required when an individual successfully demonstrates the inaccuracy or incompleteness of the information. Amendment may involve the correction, deletion, erasure, or addition to any personal information found to be inaccurate or incomplete.

Any unresolved differences as to accuracy or completeness shall be noted in the individual's file. Where appropriate, NeXafe shall inform any third parties having access to the personal information in question as to any amendments, or the existence of any unresolved differences between the individual and NeXafe.

10. Challenging Compliance

NeXafe investigates all complaints concerning compliance with its Privacy Policy, guidelines, and practices, and responds within 30 days of receipt of a complaint. If a complaint is found to be justified, NeXafe takes appropriate measures to resolve the complaint including, if necessary, amending its policies and procedures. Individuals shall be informed of the outcome of the investigation regarding their complaint.

Complainants may address inquiries or complaints concerning compliance with these policies or guidelines by contacting NeXafe's Privacy Officer as set out in this Policy under Openness. A complaint may also be addressed in writing to the Privacy Commissioner of Canada at 112 Kent Street, Ottawa, Ontario, K1A 1H3 -or- to the Office of the Information and Privacy Commissioner of Alberta, #410 - 9925 - 109th Street, Edmonton, AB, T5K 2J8, 780-422-6860, www.oipc.ab.ca.