Privacy and Personal Information Management Policy

1. PREAMBLE

The purpose of this privacy policy is to inform employees and former employees, candidates, customers and former customers, prospects, users of the website about:

- how their personal data is collected.
- their rights in relation to this data;
- the person responsible for the processing of the personal data collected and processed;
- the recipients of this personal data;
- the website's cookie policy.

2. APPLICATION

This policy applies to all STAS management and personnel.

They must refer to *the Privacy Guidelines* to enquire about its application.

3. PERSONAL INFORMATION

Personal information is any information which relates to a natural person and allows that person to be identified.

Personal information does not include information that cannot be attributed to or information that does not enable to identify a person, such as information of an aggregate nature that does not relate to an individual or anonymized information.

4. COLLECTION AND USE OF PERSONAL DATA

4.1. General principles

We act in accordance with the Act Respecting The Protection Of Personal Information In The Private Sector. Thus, personal information is:

- Processed lawfully, fairly and transparently with regard to the data subject;
- Collected for specified, explicit and legitimate purposes, and will not be further processed in a manner incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and kept up to date when in use. All reasonable steps shall be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Stored in a form allowing the identification of data subjects for no longer than is necessary in relation to the purposes for which they are processed;
- Processed in such a way as to ensure appropriate security of the data collected, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The processing is only licit if and to the extent that at least one of the following conditions is met:

- The data subject has consented to the processing of his or her personal data for one or more specific purposes and may withdraw that consent;
- The processing is necessary for the performance of a contract to which the data subject is a party or for the performance of pre-contractual measures taken at the request of the data subject;
- The processing is necessary for compliance with a legal obligation to which STAS is subject;

4.2. Data collected

The personal data collected in the course of our activity are as follows (non-exhaustive list):

- Identification data (first and last names, date of birth, social insurance number, etc.);
- Contact information (postal or email address, location or IP address);
- Emergency contacts
- Other information regarding status (gender, marital state, interests, etc.)
- Education and career (CV, certificates, diplomas, language, references, employment history)
- Employment data (photo, contracts, employee number, position, performance, salary and benefits, bank details, etc.)
- Financial data (bank account, history, credit score, etc.)
- Immigration data (citizenship, immigration status, special needs, etc.)

The collection and processing of this data serves the following purpose(s):

- *Meet our obligations and exercise our rights in connection with our customer, supplier and partner contracts;*
- *Exercise our legal obligations;*
- *Manage our human resources;*
- *Promote our products and services to our target customers.*

4.3. How data is collected

Personal information is communicated to us orally (meeting, telephone, trade show or corporate event, etc.), by email, telephone, text messages, fax or via social networks (Facebook and LinkedIn). Personal information is also collected through the interactivity that may be established between our website and the people who visit it.

4.4. Cookies

Our Services may use cookies and/or similar technologies such as beacons, tags, and scripts. Cookies are small text files that are stored on your device by the browser. Some cookies remain stored on your device until you delete them. Cookies make it easier for us to recognize your browser on your next visit. If this goes against your preferences, you can configure your browser so that it informs you of the installation of cookies and only allows it in certain cases. Disabling cookies may limit the functionality of our Services.

Our website may also use statistical and performance analysis services, such as Google Analytics. These services use cookies or other tracking technologies to help us analyze how users interact with and use our website, compile reports on related activities, and provide other services related to site activity and usage. The technologies used by these services may collect information such as your IP address, the time of your visit, whether you are a returning visitor, and any referring sites or applications. The information generated by these services will be transmitted and stored by the relevant service.

To learn how to opt out of Google analytics tracking, please click here.

4.5. Social media and other links

Our website may, from time to time, contain links to and from social media platforms or other third party websites. You may choose to communicate with STAS Inc. through a social media platform, such as Twitter, and when you do, we may collect additional information (including personal information), such as your screen name, through the social media platform.

Social media platforms and other websites may also collect information about you. We have no control over (and assume no responsibility for) the collection, use or disclosure practices of personal information from social media platforms or other third-party websites. Please review their privacy policies and practices, including data security practices, before using these social media platforms or other websites.

4.6. Persons with access to personal data

The categories of persons who have access to personal data are:

- Personal information collected in connection with recruitment is accessible only to management, human resources staff and IT personnel. They may also be accessible to staff members involved in the recruitment process.

- Personal information collected in the course of managing employee files is accessible only to management, human resources staff and IT personnel.

Personal information collected in the course of managing customer records is accessible to management, sales and marketing staff, project management personnel, engineering personnel and IT personnel.

Personal information collected in the course of managing vendor records is accessible only to management, procurement staff and IT.

5. DATA RETENTION AND SECURITY

STAS stores personal information in Quebec.

The STAS.com site is hosted by:

	Nubee
	245 Riverin Street, Chicoutimi, Quebec, G7H 4R6
	Sylvain Gauthier (sylvain.gauthier@nubee.ca, 418-615-3521)

Once we have collected personal information, it may be transferred to and stored in computer or cloud systems located outside Quebec or Canada, and in jurisdictions (Canada and/or the United States) where the privacy laws may differ from those in your jurisdiction and offer lesser guarantees regarding the protection of your personal information.

We take appropriate security measures to try to ensure the security and confidentiality of personal information. These measures are reasonable given the sensitivity of the information involved, the

purposes for which it will be used, the quantity and distribution of the information and the medium in which it is stored.

We do our best to protect personal information as soon as we collect it, but no data transmission over the Internet or any other public communication network can be guaranteed to be completely secure. If you suspect an unauthorized use or breach of security that compromises the security, confidentiality or integrity of your personal information, please contact the Privacy Officer.

6. COMMUNICATION OF PERSONAL INFORMATION

Except as provided in this Policy or in accordance with applicable laws, including the Act respecting the protection of personal information in the private sector, we do not disclose, in any way whatsoever, personal information to third parties other than our service providers and affiliates, and their directors, respective officers, employees, agents, consultants, advisors or other representatives for whom it is necessary to have access to personal information in order to provide or improve our website or Services to you. We do not sell, trade or rent personal information.

In accordance with applicable laws, including the Act respecting the protection of personal information in the private sector, we may be required to disclose personal information to certain third parties, including:

- to any service provider who necessarily needs certain personal information in the course of providing services to STAS, including in connection with the uses of personal information described in this Policy. We will only disclose personal information that is reasonably necessary to enable them to perform their duties;
- to government authorities and law enforcement agencies where required by applicable law. We may disclose personal information if we are required to do so, among other things, to comply with any applicable legal obligation, including if disclosure is required to comply with a subpoena, warrant, court order or court rules relating to the production of records;
- For the purpose of collecting a debt owed;
- to a body responsible under the Act for preventing, detecting or repressing crime or statutory offences, which so requires in the exercise of its functions, if the information is necessary for the prosecution of an offence under an Act applicable in Québec, in particular;
- if we transfer or intend to transfer control of our business, including the Website and Services, to a third party acquirer of all or substantially all of our assets, including our rights and obligations in relation to our Website and Services, to a third party. The third party may continue to retain and use the personal information provided. We will act reasonably, including by contractual means, to ensure that the third party agrees to be bound by, among other things, this Policy or by a contractual agreement stipulating measures substantially similar to those we employ to protect the confidentiality and security of personal information and to comply in the same manner with applicable privacy laws;
- to the acquirer, successor or assignee in connection with any merger, acquisition, debt financing, sale of assets or similar transaction, as well as in the event of insolvency, bankruptcy or receivership involving the transfer of personal information as a business asset to one or more third parties. In such circumstances, we will make every effort to ensure that the amalgamating, consolidated or amalgamated entity agrees to also be bound by this Policy or by a contractual agreement stipulating measures substantially similar to those we employ to protect the confidentiality of personal information and to similarly comply with applicable privacy laws; and if required or permitted by law.

When you disclose personal information or interact publicly with other users on the Website or Services, that personal information may be viewed by all users. We are not responsible for the use that these users may make of personal information that you voluntarily and publicly disclose to other users. We therefore invite you to exercise caution in your exchanges and to communicate only the personal information absolutely necessary, if any, to other users with whom you may interact on the website or the Services.

7. LIFE CYCLE AND DESTRUCTION OF PERSONAL INFORMATION

7.1. General principles

We retain and use personal information for as long as reasonably necessary for the purposes for which the personal information was collected.

In general, documents containing personal information are destroyed, regardless of their medium, as soon as the purpose for which they were collected is fulfilled, **unless:**

- a law or regulation provides for a retention period;
- a retention schedule provides for a retention period;
- the documents are project files, which **must not** be destroyed. Indeed, STAS inc. is called upon to refer to project files to make corrections to said project or to carry out similar projects.

7.2. Personal Information Retention Schedule (Paper and Electronic)

STAS Inc. must retain:

- Candidates' files for at least three (3) years following the rejection of their application;
- Former employees' records for at least three (3) years following the end of their employment, except:
    - Claims files under the *Act respecting industrial accidents and occupational diseases*, which must be kept permanently given the risk of recurrence and relapse;
    - Records of employment for at least six (6) years;
- Information used to carry out a pay equity plan or to evaluate the maintenance of pay equity in the company for at least six (6) years;
- Tax records and supporting documents for at least seven (7) years.

7.3. Destruction of personal information in paper form

Personal information in paper format is destroyed in two (2) ways:

- Cross-cut shredder: This means should be preferred for the immediate destruction of documents containing "highly confidential" information;
- Shredding by an external service provider (Coderre).

7.4. Destruction of personal information in electronic format

Personal information stored in electronic format is destroyed by deletion.

8. RIGHTS (ACCESS, RECTIFICATION, DELETION AND FORGETFULNESS), HOW TO EXERCISE THEM AND FROM WHOM

In order to exercise each of your rights, please make a request to cprp@stas.com

All requests must be made in writing and must contain:

- The title of the document you wish to consult, correct, delete or forget and a brief description that will allow it to be located;
- The period covered;
- Personal information that will identify you or a combination of several pieces of information to do so.
- Your first and last name and contact information (email, telephone number and mailing address) so that we can contact you if clarification is required.

A request may be considered only if it is made in writing by a person proving his identity as the person concerned, as the representative, heir or successor of the latter, as liquidator of the succession, as beneficiary of life insurance or death benefit or as holder of parental authority even if the minor child is deceased. If you are applying on behalf of someone else, you must provide:

- a consent form or power of attorney;
- or the mandate signed by that person, if you are a notary or lawyer.

All requests are processed diligently and at the latest within 30 days of the date of receipt of the request.

8.1. Right of access to personal information

Every individual has the right to be informed that a company holds personal information about him or her and to obtain disclosure of that information

8.2. Right to rectification or deletion of personal information

This gives you the right to request the correction of personal information about you, if this information is inaccurate, incomplete or ambiguous. You may also request its deletion if its collection, disclosure or retention is not authorized by law.

8.3. Right to be forgotten

The right to require that we cease disseminating personal information or that any hyperlink attached to the name of the person concerned allowing access to the information by technological means be deindexed or re-indexed, subject to certain conditions.

9. PRIVACY INCIDENT

A "privacy incident" refers to the following situations:

1. Unauthorized access by law to personal information ;
2. Unauthorised Use of Personal Information by Law ;
3. Unauthorized disclosure of personal information ;
4. The loss of personal information or any other breach of the protection of such information.

When a member of management or staff has reason to believe that a confidentiality incident has occurred, they must notify the Privacy Officer at cprp@stas.com. To do this, they can use the declaration form (see Appendix).

The appropriate management or staff member and the Privacy Officer must jointly:

- assess the risk of prejudice being caused to an individual whose personal information is affected by a confidentiality incident, taking into account, in particular, the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that it will be used for harmful purposes that could cause prejudice;

- take reasonable steps to reduce the risk of prejudice and prevent similar incidents from occurring.

If the incident poses a risk of serious prejudice, the Chief Privacy Officer shall, in a timely manner, advise:

- the *Commission d'accès à l'information*. The model opinion is available on the Commission's website:

  https://www.cai.gouv.qc.ca/documents/CAI_FO_avis_incident_confidentialite.pdf

- any person whose personal information is affected by the incident ;

- any person or organization likely to reduce this risk, by disclosing only the personal information necessary for that purpose without the consent of the person concerned. In the latter case, the person responsible for the protection of personal information must record the communication.

Notwithstanding the preceding paragraph, a person whose personal information is involved in the incident need not be notified so long as it would be likely to interfere with an investigation by a person or body responsible under the law for preventing, detecting or suppressing crime or statutory offences.

The Privacy Officer must record any confidentiality incident in a log.

10. COMPLAINT PROCESS

Any complaint relating to the management of personal information must be addressed in writing to the Privacy Officer.

It must state the facts and reasons in support of it. In addition, any document relevant to its analysis must be appended to it.

The Privacy Officer must deal with the complaint diligently and provide a written response to the complainant.

11. PRIVACY OFFICER

The person in charge of the protection of personal information is the Human Resources Department, it is possible to reach it at the following email address: cprp@stas.com

The person responsible for the processing of personal data is the Information Systems Department. They can be reached at the following email address: cprp@stas.com

12. ENTRY INTO FORCE

This policy is effective as of September 22, 2023.

Non-Compliance to the Protection of Personal Information Incident Reporting Form	
Date of incident	
Date the organization became aware of the incident	
Summary description of the incident (Attach any relevant documents to the Privacy Incident Registry)	
Description of the personal information involved in the breach	
Identification of the person(s) involved in the incident	
Description of the factors that lead the organization to conclude whether or not there is a risk of serious prejudice to the individuals concerned (the sensitivity of the personal information concerned, the potential misuse of the information, the anticipated consequences of using the information, and the likelihood that it will be used for harmful purposes)	
If there is a risk of serious prejudice, has an opinion been sent to the Commission? If yes: - On what date? - Append the notice to the Privacy Incident Registry	
If there is a risk of serious prejudice, has notice been sent to the person(s) involved in the incident? If yes: - On what date? - Append the notice to the Privacy Incident Registry	

If there is a risk of serious prejudice, has notice been sent to any person or body likely to reduce that risk? If yes: - On what date? - Attach the notification to the Register of Privacy Incidents; - Attach the record of the communication to the Register of confidentiality incidents;	
Description of the measures taken by the organization following the incident to reduce the risk of prejudice	

Person who discovered the incident:

Date:

Signature:

Privacy Officer

Date:

Signature: