POLICY FOR THE PROTECTION OF PERSONAL INFORMATION

1. THE OBJECTIVES

This policy constitutes the general framework concerning the behaviors expected of employees with regard to the handling of data, access to data, the use of information technologies, as well as actions on the governance and management of information.

This policy also emphasizes the importance of ensuring and preserving the confidentiality of personal information, respect for privacy and the ethical responsibility of anyone who holds information about others.

In addition, it indicates the procedures and general principles that Locweld employees must follow in order to give the utmost importance to the sensitive information to which they have access, the procedures for complaints and incidents, as well as the actions necessary in the support for information security requirements.

2. SCOPE OF APPLICATION

This policy applies to all Locweld employees who directly or indirectly have access to customer data, personal data from employees or candidates, or other company data defined as sensitive for the company.

All employees who are in the workplace or telework, including unionized employees, the office, subcontractors and managers are involved in the responsibility of this policy.

The scope also applies to the servers, databases and computer systems that process this data, including any device regularly used for e-mail, website access or other work-related tasks. Any user who interacts with the company's IT services is also subject to this policy.

3. DEFINITIONS AND CONCEPTS

- **Confidentiality:** a requirement that information is disclosed, processed and made available only to authorized persons or entities, according to established terms.

- **Right of access**: the right to use an information asset according to terms that vary according to the level of privilege granted.

- **Computer security incident:** any event likely to violate institutional computer security objectives and standards.

- **User:** all Locweld employees and any natural or legal person called upon to use information assets authorized by senior management.

- **Personal identifier:** an exclusive characteristic, unique and confidential information or a unique object held by the employee, making it possible to verify the identity of this person. It is a password or personal identification number predefined and informed only to the user.

- **Email Address:** Any address used in connection with any of the following accounts:
  - Locweld email account;
  - instant messaging account for specific purposes;

- **Informational asset**: any equipment connected or not to the network, software, system, data or information used for the hosting, processing, dissemination and exchange of information. Information assets also cover equipment, software, systems, data or information belonging to it and those that use or host assets of which the company is the owner, trustee or custodian.

- **Commercial activity:** Any regular activity as well as any isolated act which is commercial in nature.

- **Business contact information**: Any information allowing to get in touch or to facilitate contact with an individual in the context of his job, his business or his profession, such as his name, his position or his title, address or telephone or fax numbers of his workplace or his electronic address at work.

- **Record:** All elements of information, whatever their form and their medium, in particular correspondence, note, book, plan, map, drawing, diagram, illustration or graph, photograph, film, microform, sound recording or any reproduction of these elements of information.

- **Personal information**: Any information concerning an identifiable individual, namely:
  - race, nationality or ethnic origin.
  - religion.
  - age or marital status.
  - financial transactions.
  - numbers allowing the person to be identified (e.g. social insurance number or driver's license number).

- **Personal health information**: With respect to a living or deceased individual.
  - any information relating to his physical or mental health.
  - Any information relating to the donations of body parts or bodily substances made by him, or any information from the results of tests or examinations carried out on a part of the body or a body substance thereof.

Note: What is not generally considered personal information may include:

- Information that does not relate to an individual, either because the connection to that person is too vague or too distant (ex, a postal code applies to a large area with many residences).
- Anonymized information, provided that it is not possible to connect it to an identifiable person.
- Certain employee information such as name and job title.

- Business contact information of an individual that an organization collects, uses or discloses solely to contact them in the course of their employment, business or profession.

- **Depersonalization and anonymization of information**

  Personal information is "depersonalized" when this information "does not identify the person concerned directly". Information about a natural person is "anonymized" when it "does not allow, irreversibly, to directly or indirectly identify this person".

4. REGULATORY CONTEXT

This policy is based on the ACT RESPECTING THE PROTECTION OF PERSONAL INFORMATION IN THE PRIVATE SECTOR (LPRP), chapter P-39.1 as well as Law 25, ACT TO MODERNIZE LEGISLATIVE PROVISIONS IN THE MATTER OF THE PROTECTION OF PERSONAL INFORMATION, as well as the Act Personal Information Protection and Electronic Documents (PIPEDA) Act of Canada.

5. ACCESS CONTROL

Access to Locweld data is defined by position, responsibilities and permissions given by senior management. Access management exists to ensure that users can only access the resources they need to do their job.

5.1. IT access:

1. Each user will be identified by a unique user ID, so that everyone can be held accountable for their actions.

2. The use of shared identities is only authorized where they are appropriate, for example the team of inspectors.

3. User access records can be used as evidence in a security incident investigation.

5.2. User responsibilities :

1. All users must lock their screen whenever they leave their desk, to reduce the risk of unauthorized access.

2. All users must make sure not to leave any sensitive or confidential information around their workstation.

3. All users should keep their passwords confidential and not share them.

5.3. Access to physical documents (employee file):

1. All employees have a record of their career history. This file consists of several documents, the majority of which are considered strictly confidential. In order to preserve the employee's right to privacy, only duly authorized persons, given their professional duties, may consult the relevant documents contained in employee files.
2. It is forbidden to have access to these files, any person within the company for whom the consultation of the file is not necessary for the exercise of his functions and his responsibilities.
3. The employee is allowed to consult his file if the authorization is specified in the collective agreement or under the rules provided for in the Act respecting the protection of personal information in the private sector. To this end, the employee must make the request to HR and the consultation will be done in an office reserved for this purpose and with the presence of a member of the Human Resources team.

6. ACCESS TO CONFIDENTIAL AND RESTRICTED INFORMATION

Access to data classified as "confidential" or "restricted" regardless of its form or content, must be limited to authorized persons whose professional responsibilities require it, as determined by management or by a procedure provided for this purpose.

7. INFORMATION ACCESS COMMISSION AND CONFIDENTIALITY INCIDENT MANAGEMENT

Taking into account the importance of this policy for the protection of sensitive and personal information, and for the security of company data, an **intervention committee** has been established to create the access to the commission of access to information, to ensure the implementation of procedures and procedures in the event of a confidentiality incident occurring.

The information intervention committee is composed as follows:

Head of Committee and Data Protection (PRP) :
Pierre Lavoie (President & Chief Financial Officer)
Tel : 450-659-9661
info@locweld.com

Committee members: Operations chief
IT Director
HR Coordinateur
Controller

7.1. Responsibility of the PRP manager:

- Approve the personal information policies and practices that Locweld has established;
- Participate in the committee and manage the actions necessary for the protection of personal information;
- Participates in privacy impact analysis and harm assessment of a privacy incident.
- Define the necessary communications and the commitment of committee members to ensure the application of this policy;

7.2. Responsibility of the committee :

- Meet occasionally to update this policy.
- Define the measures to be taken if procedures need to be improved.
- Consider the sensitivity of the information concerned, the apprehended consequences of its use and the likelihood that it will be used for harmful purposes.
- Ensure that requests for personal information are used for the intended purpose. “Personal information may only be used within the company for the purposes for which it was collected, unless the person concerned consents (art.110 paragraph 12, LPRDE)”.
- In the event of an incident, take the necessary measures to put an end to the risks and damages.
- Keep a record of confidentiality incidents and highlight the measures taken to prevent new similar incidents from occurring.

7.3. Security incidents:

For the application of the law, a confidentiality incident is:

- Access not authorized by law to personal information.
- The unauthorized use of personal information by law.
- Disclosure of personal information not authorized by law.
- The loss of personal information or any other breach of the protection of such information that could cause harm.

7.4. Procedure in case of incident:

Privacy incidents or any damage to personal information which is in the possession of an organization must be declared to the Committee on Access to Information (CAI).

The committee will carry out an in-depth examination of the situation and will issue a report containing the details of the incident and the measures necessary to end data leakage. Measures to avoid repetition of incidents will then be determined by the head of the committee.

The head of the committee is responsible for reporting any confidentiality incident to the Committee on Access to Information in a timely manner.

8. DATA GOVERNANCE

8.1. Consent to use data

The purposes for which personal information is collected and the methods used to collect them are set out below to ensure the transparency of the collection and to respond to requests for information:

When collecting personal information:

- Consent must be requested, in simple and clear terms, for each of the purposes for which the information is collected.
- Written consent must be obtained separately from any other information communicated to an individual.
- The means of collection must be clearly defined.
- The possibility that the information will be communicated outside Quebec must be clearly indicated, if applicable.

8.2. Consent Exceptions :

Law 25 provides that an organization can use personal information to another end without having to obtain the consent of the person concerned in the following cases alone:

- When its use is for purposes compatible with those for which it was collected and it serves the data subject;
- When personal intelligence is necessary to conclude a commercial transaction;
- When the personal information is used for research purposes or to produce statistics;
- When personal information is commercial (name, title, functions, business address, email address and telephone number);
- The cases where the personal information is necessary to carry out a mandate or fulfill a contract for services carried out by a third party also constitute exceptions. However, this exception has certain condition:
    - The third party must have a written mandate that details their responsibilities with respect to the personal information and the security measures in place to ensure its protection
    - A written agreement must require the third party that he advises the person responsible for the protection of personal information of the organization responsible for collecting information from any violation or attempted violation of confidentiality.

8.3. Technological confidentiality

The confidentiality parameters of any technology or technological solution used by Locweld is set by default at the strictest level with regard to personal information.

8.4. Destruction of personal information

It is compulsory to destroy personal information when the purposes for which it has been collected are accomplished. If there is a legitimate reason to keep the information, it must be made anonymous, except for employee's files which must be kept according to the legal deadline. A period may be extended in the event of an ongoing dispute.

8.5. Right to be forgotten:

Locweld must accommodate people who wish to exercise their right to stop the dissemination of personal information or to de-index or re-index a hyperlink attached to their name allowing access to this information.

The masculine gender is used in this policy as the neutral gender. The use of the masculine gender is intended to lighten the text and make it easier to comprehend.