Privacy Policy

Adopted

October 23, 2012

Reviewed and adopted by the board of trustees: March 5, 2026

_____	_____
Signature of Authorised Trustee	*Signature of Authorised Trustee*
_____	_____
Name	*Name*
_____	_____
Date	*Date*

PRIVACY POLICY

The Board of Trustees is responsible for the good governance of the Boilermakers Lodge No. 191 Benefit and Pension Plans (together called "the Plans"). Privacy of Personal Information is the cornerstone of the Plans' administration procedures and policies. We understand the importance of protecting Personal Information. We are committed to collecting, using, and disclosing Personal Information responsibly and in compliance with all applicable legislation, and to being open and transparent about the way the Plans handle Personal Information .

HOW THE PLANS COLLECTS, USES AND DISCLOSES PERSONAL INFORMATION

WHAT INFORMATION DO WE KEEP?

We collect and store non-public Personal Information. Personal Information includes any factual or subjective Information, recorded or not, about an identifiable individual. This includes Information in any form, such as:

- Social Insurance Number
- income
- ethnic origin
- personal address
- opinions, evaluations, comments, medical records

Personal Information comes from a variety of sources such as the applications or other forms that you complete, from your employers, or from correspondence with you and service providers you have engaged to provide medical or other benefits. We collect only the information we need for the purpose of providing and servicing the benefit and pension plans administered on your behalf.

In order to provide certain benefits, we may be required by legislation (such as the *Pension Benefits Standards Act)* to collect and store your Social Insurance Number.

We do not sell your Personal Information.

WHY DO WE NEED THE INFORMATION?

We need to collect Personal Information to:

- determine your eligibility for benefits;
- administer and adjudicate your benefits;
- determine the cost and financially manage these programs; and
- meet regulatory or contractual requirements relating to the benefits and related services provided to you.

We will make sure you understand why we need the information by using clear, understandable language in describing the purpose.

The Trustees are aware of the sensitive nature of the Personal Information that Members have disclosed. The administration staff of the Plans are trained in the appropriate uses and protection of Personal Information . Together with the Trustees, those involved in the administration of the Plans

ensure that:

- Only necessary Personal Information is collected;
- Personal Information is obtained and shared only with consent when applicable and as indicated in this Privacy Policy, unless written notification from a member is received allowing other disclosure;
- Storage, retention, and destruction of Personal Information complies with all applicable legislation;
- The Plans' privacy protocols comply with all applicable privacy legislation and standards

of the applicable regulatory authorities, in particular, all applicable legislation dealing with privacy and health care records.

WE WILL OBTAIN YOUR PERMISSION

We collect, use or disclose your Personal Information with your permission. Your permission may be expressed in writing or be implied and you may give it to us verbally, electronically, or through your authorized representative. Your knowledge and consent are required for the collection, use, or disclosure of your Personal Information, except where inappropriate.

With reasonable notice, and subject to legal and contractual restrictions, you may withdraw your permission to collect, use and disclose your Personal Information at any time.

We will obtain your consent to collect or release medical information about you. Before we make information available to third parties, other than an agent or authorized service provider who needs it, we will tell you at the time we obtain your consent or before we make the information available, who those persons or organizations are, the kind of information we want to share with them and why.

Of course, you can choose not to provide us with some or all of your Personal Information . However, this choice may hinder our ability to adjudicate any claims you have for benefits to which you may be entitled.

HOW LONG DO WE KEEP INFORMATION?

We will keep your Personal Information as long as it is necessary, or as required by law. When Personal Information records are destroyed, we will use appropriate safeguards to prevent unauthorized parties from gaining access to the information during the process. Personal Information will be retained in accordance with the Plans' Document Policy.

THE PLAN WILL PROTECT YOUR PERSONAL INFORMATION

WE ARE RESPONSIBLE FOR YOUR INFORMATION

We are responsible for all Personal Information in our possession, including information transferred to a third-party service provider or agent, so that we can provide you with benefits and related services.

HOW WE PROTECT INFORMATION

Only the Plan Administrator's employees, the Trustees of the Plan, Plan sponsors, agents and authorized service providers who need the information in order to do their jobs may access your

Personal Information. Where possible, when we provide information to third parties such as actuaries, we attempt to eliminate any references that allow identification of the individuals. We require all employees, agents and authorized service providers to comply with this Privacy Policy.

We have developed and are continuing to enhance security procedures to safeguard and protect Personal Information against loss, theft, unauthorized disclosure, copying, and unauthorized use or modification. We will maintain appropriate safeguards and security procedures that reflect the types of documents, including electronic or paper records, organizational measures, including security clearances and limiting access on a "need-to-know" basis, and technological measures such as the use of passwords and encryption. While we endeavour to protect all information, the most sensitive information, such as medical information, receives the highest level of protection.

For telephone inquiries to the Plan's Administration staff, the information provided varies based on the relationship of the person making the inquiry to the Plan Member (e.g. authorized service provider, Plan Member, or dependent). After the caller has been screened for appropriate identification, only information pertaining to the specific claim, treatment, or benefit in question is shared.

The Plans will not, under any circumstances, disclose medical history without specific written consent from the Plan member, unless required by law or provided to an authorized provider of the Plans for the purpose of determining eligibility for benefits.

When requests are received to disclose Personal Information that is not covered by the foregoing rules, the Plans will obtain the relevant person's permission prior to releasing such Personal Information .

Plan Members and others may withdraw their consent to the use or disclosure of Personal Information. The Plans will explain the ramifications of that decision.

YOUR RIGHT TO ACCESS YOUR PERSONAL INFORMATION

You have the right to ask whether we hold any Personal Information about you. You have the right to see that information, as provided by law. Where we have obtained medical information about you from a third party, we will release this information only with your permission.

You also have the right to know:

- how we collected your Personal Information;
- how we are using it; and
- to whom it may have been disclosed.

HOW TO REQUEST AN UPDATE OR CORRECTION

If you believe any of the information we have collected about you is incorrect or incomplete, you have the right to ask us to change it.

You may make a request to change the Plan's records about you by writing to the Privacy Officer. If you show that your Personal Information is inaccurate or incomplete, we will make the necessary changes, and where appropriate, we will contact any third parties with which this information has been shared.

HOW TO REGISTER COMPLAINTS

If you feel we have not dealt with your request to your satisfaction, you may register a privacy-related complaint by contacting the Plan's Privacy Officer. We will explain our complaint procedure to you and

investigate all complaints.

If a complaint is justified, the Trustees will take all appropriate steps to set the situation right, including, if necessary, changing our policies and practices. We will also let you know what other complaint procedures may be available to you.

We reserve the right to revise our privacy policy as needed. If changes are made, the new policy can be obtained by contacting the Plan's Privacy Officer.

If a breach is to be reported, the Plans will follow the protocol outlined in Schedule 1 - Mandatory Notice Requirements of PIPEDA.

PRIVACY STATEMENT

The Boilermakers Lodge No. 191 Benefit and Pension Plans (together called "the Plans"), their administrator Employee Benefit Plan Services Limited, and providers working with the Plans or administrator may collect, maintain, use and disclose Personal Information that is necessary for the administration of the Plans. Personal Information will be protected pursuant to the applicable legislation. The Plans may collect, maintain, use and disclose Personal Information with relevant persons or organizations (Trustees, institutions, investigative agencies, unions, insurers, re-insurers, auditors, legal counsel, actuaries, payroll/payment providers, Plan administrators, and regulatory authorities) in order to manage the Plans and entitlement to the benefits of the Plans, and may include information such as financial, health or benefits related information. Questions related to the Privacy Statement should be directed to the Privacy Officer.

FOR MORE INFORMATION

Please be assured that the Trustees and all Plan administration staff are committed to providing excellent service. Plan Members, dependants, and beneficiaries are invited to discuss the Privacy Policy with the Plans' Privacy Officers. If you have any questions or concerns about the Plans' Privacy Policy, please contact the Plans' Privacy Officer:

Ryan Laird

45 McIntosh Drive
Markham, Ontario L3R 8C7

Tel: 905-946-9700
Toll Free: 1-800-263-3564
Email: rlaird@mcateer.ca

REVIEW

This Policy is reviewed every two years or more frequently if necessary.

TRANSPARENCY

This Policy is available to Plan Members via the Plans' website www.boilermakers191benefits.org.

PRIVACY POLICY – SCHEDULE 1

MANDATORY NOTIFICATION REQUIREMENTS OF PIPEDA

Organizations subject to the federal Personal Information Protection and Electronic Documents Act ("PIPEDA") must notify affected individuals of a breach to the confidentiality of their personal Information that results in a real risk of significant harm to them.

PIPEDA regulations define significant harm as including "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."

The regulations require organizations to report to the Privacy Commissioner of Canada ("the Commissioner") all applicable breaches that result in a real risk of significant harm, and to maintain records of all breaches involving personal Information, including those that do not meet the real risk of significant harm threshold.

BACKGROUND

The factors that are relevant in determining whether there is a real risk of significant harm to an individual include

a) the sensitivity of the personal Information involved,

b) the probability that the personal Information has been, is being or will be misused; and

c) any other prescribed factor. There are currently no other prescribed factors.

PIPEDA defines a "breach of security safeguards" as the loss or disclosure of personal Information or the unauthorized access to personal Information resulting from a breach of the organization's security safeguards or from its failure to establish such safeguards.

IMPACT ON THE PLAN/PLANS

In the event of an applicable breach, the Plan must:

- report the breach to the Commissioner if applicable (see Plan Notice to Commissioner below);
- notify the affected individuals; and
- notify government institutions or other organizations if the Plan believes that the other organizations may be able to reduce the risk of harm to the affected individuals.

PENALTIES

If the Plan fails to report applicable privacy breaches to the Commissioner, fails to notify affected individuals of breaches affecting their personal Information, or fails to maintain records of such breaches, it could be subject to fines of up to $100,000.

PLAN NOTICE TO COMMISSIONER

PIPEDA requires that a report to the Commissioner be made as soon as feasible after the Plan determines that a privacy breach that resulted in a real risk of significant harm has occurred. The regulations require that the report be in writing and be submitted via a secure means of communication, such as an encrypted email.

The Plan communication must contain at least the following:

- a description of the breach and its cause, if known;
- the date, or the period or approximate period, of the breach;
- a description of the personal Information involved to the extent that it is known;
- the number, or approximate number, of individuals affected by the breach;
- a description of the steps taken by the Plan to reduce the risk of harm to those individuals;

- a description of the steps taken by the Plan, or intended to be taken, to notify the affected individuals; and,
- the contact information of the Plan's Privacy Officer, who can answer the Commissioner's questions about the breach.

The regulations recognize that the full extent of a breach may not be known immediately. They permit but do not require the Plan to provide new Information to the Commissioner following the initial reporting of a breach.

NOTICE TO INDIVIDUALS

PIPEDA requires that notice of a breach resulting in a real risk of significant harm must normally be provided to affected individuals directly and as soon as feasible after the Plan determines that a breach has occurred. Notices must contain sufficient Information to allow an individual to understand the significance to them of the breach and to take steps, where possible, to reduce the risk of harm or mitigate such harm.

The regulations require that at least the following Information be included in such notices:

- a description of the breach;
- the date, or the period or approximate period, of the breach;
- a description of the Personal Information which was compromised to the extent that it is known;
- a description of the steps taken by the Plan to reduce the risk of harm to affected individuals;
- a description of the steps that affected individuals could take to reduce the risk of harm to them or mitigate such harm; and,
- the contact information of the Privacy Officer who will answer questions about the breach.

The regulations provide that notice may be given in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances. The form of notice should be documented so the Plan can address any future claim that no notice, or insufficient notice, was provided.

The regulations also provide that affected individuals may be notified indirectly if direct notice would likely cause further harm to the individual, would impose undue hardship on the Plan/Plans, or if the Plan does not have contact information for the affected individual. At the direction of the Board of Trustees, indirect notice shall be given through public communication or a similar measure that could reasonably be expected to reach the affected individuals, such as a workplace posting or a relevant website.

The method of notice will be determined by the Privacy Officer.

BREACH RECORD KEEPING

PIPEDA requires that the Plan maintain records of all breaches of its security safeguards, including those that do not meet the real risk of significant harm threshold, for 24 months from the date the Plan/Plans determined that a breach had occurred.

These records must be available to the Commissioner upon request and must contain sufficient Information for the Commissioner to determine whether the Plan complied with its notification and reporting obligations.

Records of breaches that did not satisfy the real risk of significant harm threshold should indicate how that determination was made.

Notwithstanding that a breach is not reportable, it will be reported to the Privacy Officer as part of the breach record-keeping protocol.

Breach records are destroyed after 24 months unless the matter is the subject of known litigation.

Depending on the Information breach, the Plan may pay the cost of credit monitoring for affected individuals if the confidentiality of their financial Information is breached. Different steps may be required if the confidentiality of personal medical Information is breached. The Board of Trustees will make the determination on a case-by-case basis.

ENCRYPTED DATA

It is the policy of the Plan administrator to send confidential data in an encrypted format. However, many Members, union officers, and other stakeholders may not. Breaches involving encrypted data are not exempt from the notification and reporting requirements of PIPEDA.

The use of high-quality encryption may reduce the risk of harm to below the real risk of significant harm threshold, so no notification or reporting would be required. In such circumstances, the Plan must maintain a record of the breach for 24 months.