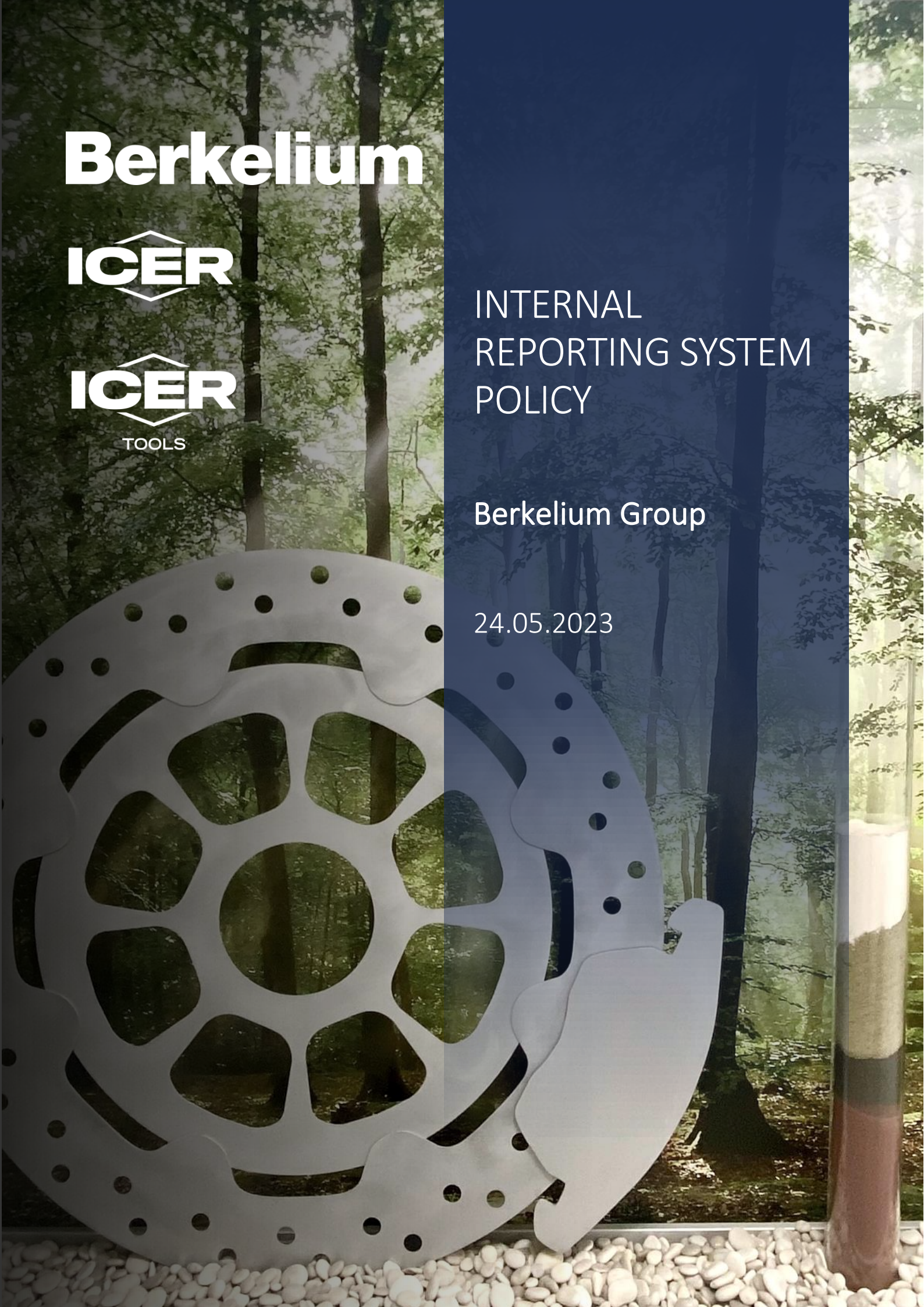

Berkelium

ICER

ICER TOOLS

INTERNAL REPORTING SYSTEM POLICY

Berkelium Group

24.05.2023

Berkelium
GROUP

Pamplona, 24 May 2023.

The **Berkelium Group**, which includes the companies Berkelium S.L., Icer Brakes S.A. and Icer Tools S.L., is committed to promoting a solid integrity infrastructure and to fostering a culture of reporting as a mechanism to prevent and detect threats of public interest in all entities of the Group. As a consequence of this commitment, the management body has agreed to **design, implement, maintain and improve** an Internal Reporting System in accordance with the provisions of Law 2/2023 of the 20th of February, regulating persons who report regulatory violations and the fight against corruption (hereinafter, the Law), in order to provide adequate protection to informants and strengthen the reporting culture in the companies that make up the **Berkelium Group**.

In order to ensure the management of the system, the management body of the parent company of the Group has appointed the Group Compliance Officer as Head of the Internal Reporting System, who shall perform his or her duties independently and autonomously from the other bodies of the **Berkelium Group**. This Officer shall ensure that the principles that form part of this policy are correctly implemented.

The companies that constitute the **Berkelium Group** accept and share this Internal Information System Policy, demonstrating their motivation, commitment and individual responsibility. The **Berkelium Group** pledges to comply with the principles of the system and to demand this commitment from all its employees and, as far as possible, from its employees.

1. GENERAL PRINCIPLES OF THE SYSTEM

The Internal Reporting System is governed by the following principles:

- Accessibility: The **Berkelium Group** has internal reporting channels that enable persons described in the Act to report breaches under the Act in a working or professional context in written form, verbally or both. The information on the reporting channels shall be clear, easily accessible and easy to use for persons who wish to report a violation. In addition, the functioning of the reporting channels shall be public.
- Confidentiality: Communications through the enabled reporting channels may be made anonymously, and at all times the reporting channel will be confidential and will have technical security guarantees. In the event that the informant decides to make the communication without remaining anonymous, his or her identity will be treated as confidential information. The processing of this information shall be limited to a small group of people, so that the identity of the informant and that of third parties affected may not be revealed, except in cases expressly provided for in the applicable regulations. The necessary technical and organisational measures shall be employed to ensure that the communications and investigations managed in the system are handled securely, confidentially and in compliance with the regulations on personal data protection.
- Efficiency: Communications made through the Internal Reporting System and authorised channels shall be processed as quickly and diligently as possible and always respecting the deadlines established in the Informant Protection Law and any other applicable regulations. As a general rule, receipt of the communication must be acknowledged within 7 calendar days and the period for responding to the investigation actions shall not exceed 3 months from the communication, except in cases of greater complexity, in which case the response period may be extended up to a maximum of 6 months.
- Objectivity: The information received through the reporting system shall be treated objectively, in compliance with the law, and the presumption of innocence of the persons affected by communications shall be maintained until the end of the investigation. The Compliance Officer in his or her capacity as Head of the System and the persons in charge of managing the information shall avoid any type of conflict of interest that may arise in all cases.

2. INFORMANT PROTECTION

Persons who report the possible existence of violations through the internal reporting system of the **Berkelium Group** in compliance with the requirements of Law 2/2023 of 20th of February, shall be guaranteed protection against possible retaliation provided by law.

The management bodies of the **Berkelium Group** expressly prohibit any act constituting retaliation, including threats and attempts of retaliation, arising from the communication made. Informants will be protected against acts or omissions prohibited by law, unfavourable treatment or disadvantage in the employment context because of their status as informants or because they have made the public disclosure.

This policy shall be reviewed periodically and amended as appropriate for continuous improvement, in which case, it shall be communicated to interested parties.

3. PUBLIC DISCLOSURE

In order to ensure the proper management and proper functioning of the internal information system, this system policy shall be duly disclosed in the organisation so that all employees and persons related to the **Berkelium Group** are aware of its principles and can be governed by them.

This policy shall be reviewed periodically and amended when relevant to the continuous improvement of this policy, in which case it shall be communicated to interested parties.