INFORMATION SECURITY POLICY

PURPOSE AND SCOPE

This security policy describes the focus of Brim's management with regards to information protection and security in information processing. Brim's information assets must be protected from all threats, internal and external, intentionally or accidentally. Professional, coordinated practices are the key to success, as evidenced by the establishment of this security policy. The implementation and execution of the policy is important in order for the company's operations and services to be as secure as possible and the correct practices used.

Brim's security policy covers the security of the company's information assets and all information in any form and on any medium. The policy covers the conduct, handling and storage of data in any form and the work processes that pertain to services and activities at all of Brim's operating units.

The security policy also covers housing and equipment where information is handled or stored, as well as employees and contractors who have access to the company's information and Brim's operating units.

POLICY

Brim shall promote the security of valuable information through an organized procedure that supports continuous operation and minimizes operational risk.

GOALS

Brim's goals with the security policy are to:

- Ensure maximum security of valuable information as well as information systems owned or managed by the company.
- Protect valuable information from unauthorized access, improper use, disclosure or deletion of important and sensitive data.
- That tangible security is ensured at the company's operating units and premises.
- Establish and maintain an active awareness of information security among employees and the Board and those who gain access to valuable information in their work for the company.
- That there is continuous and systematic work within the company to promote improvements and to carry out regular risk assessments so that it is possible to assess whether improvements to the company's information security are needed.

APPROACHES TO GOALS

Brim's approaches to the above goals are to:

- Keep a record of the company's information assets and classify them according to importance in its operations.
- Regularly analyze, with a formal risk assessment, the value of information assets, their vulnerability and threats that may endanger them.

- Regularly analyze, with a formal risk assessment, access to the company's operating units and assets, their vulnerabilities and threats that could endanger them.
- Provide employees and service providers with training and education regarding information security and their responsibilities in this regard.
- Comply with all agreements the company is a party to and concern information security.
- Make plans for continuous operation, maintain them and test them as much as possible.
- Report and investigate deviations, violations or suspicions of information security vulnerabilities.
- Ensure that the risk due to the processing (handling) and storage of information is within defined risk limits.

RESPONSIBILITY

Responsibility for the implementation and maintenance of the security policy is divided as follows:

- Brim's Executive Board is responsible for its security policy and its review.
- Brim's Executive Board is responsible for the implementation of the security policy and to that aim applies appropriate procedures and work protocols.
- Brim's Executive Board is responsible for making agreements with contractors and suppliers to ensure that the policy is adhered to.
- Managing directors are responsible for the valuable information created in the relevant operating unit and that employees follow the rules and recommendations that apply to information security.
- Brim's management sets rules on the access of employees and contractors to the company's operating units.
- All Brim's employees are responsible for following the procedures and work protocols that ensure the implementation of the security policy is followed.
- Brim's employees shall guarantee that the implementation of rules on customers', contractors' and suppliers' access to the company's operating units is in such a way as to ensure that the implementation of the policy is followed.
- All Brim's employees must work in accordance with the security policy. They must report security breaches and vulnerabilities related to information security. Those who deliberately threaten the information security of Brim or its customers face court action or other appropriate legal action.

Approved by the Board of Directors of Brim hf. December 17, 2020.