

INFORMATION SECURITY POLICY

PURPOSE

According to the Act on Personal Data Protection and Processing of Personal Data no. 90/2018, Hefring ehf., herewithin „Hefring“, must ensure adequate security of all personal data. This Information Security Policy describes the company's emphasis on the importance of that obligation. The company's personal data must be protected from all threats, both internal and external, regardless of whether the threats are intentional or negligent. With this policy, employees, customers and others can trust Hefring intention to safeguard the security of personal data, including for confidentiality, fairness and availability.

SCOPE

This Information Security Policy covers the handling and storage of all personal data in the custody of Hefring. It covers the internal operations of the company and the services that Hefring provides to its customers on shared or specific equipment, as well as all internal systems, software and hardware owned and/or under full control of Hefring. It also covers premises where personal data is processed, employees and contractual parties who have access to the pertinent data.

OBJECTIVE

Hefring's objective with this policy is to:

- Make sure all personal data is correct and accessible to those who have access rights.

- Guarantee the confidentiality of personal data and that confidentiality is maintained in accordance with applicable laws and regulations.
- Protect all personal data against damage, destruction or disclosure, regardless of whether it is due to intent or negligence.
- Oversee that all personal data that goes through Hefring's system reaches the correct recipient, undamaged and on time.
- Make sure that the risks involved in processing personal data are within defined risk limits.
- Comply with all laws, regulations and rules concerning the processing of personal data.
- Comply with all agreements to which the company is a party off and which concern the protection of personal data.
- Report and investigate all deviations, breaches or suspicions of information security vulnerabilities.
- Constantly work on and improve information security.

WAYS TO THE OBJECTIVE

Hefring's approaches to the above objectives are to:

- Keep records of information assets where personal data can be found, whether in electronic form or on paper, and classify it according to the nature and importance of confidentiality.
- Regularly analyze, through a formal risk assessment, the risks that the processing of personal data may entail for individuals.
- Manage the risk of processing personal information within defined limits by operating an information security management system.
- Perform an impact assessment on privacy if it is likely that a particular type of processing could pose a significant risk to the freedom and/or rights of individuals, such as when it comes to implementing new systems that host or otherwise process personal data.

- Maintain a quality manual with procedures and procedures for processing personal data.
- Have all Hefring employees receive regular training and education regarding the security of personal information and the responsibility that rests on them.
- Make sure all employees comply with applicable laws and regulations.

RESPONSIBILITY

- Hefring's board of directors is responsible for this Information Security Policy.
- Hefring's CEO is responsible for the implementation and the day-to-day management of the policy.
- Hefring's Data Protection Officer shall ensure that staff receive appropriate training on the security of personal information.
- All Hefring employees must work in accordance with the Information Security Policy. They should report security breaches and vulnerabilities related to information security. Those who deliberately threaten Hefring's information security face litigation or other appropriate legal action.

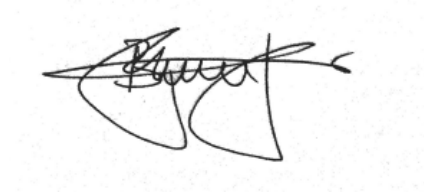
AUDIT

This policy should be reviewed annually and more frequently if necessary to ensure that it is in line with Hefring's objectives.

Signature page follows.

APPROVAL

Approved by Hefring ehf's Board of Directors on 14.02.2023.

A handwritten signature in black ink, appearing to be "Björn Jónsson", written over a light blue grid background.

Björn Jónsson

Chief Operating Officer,

Chairman of the BoDs and Secretary of the meeting