Title	Version	Replaces	Org. location	Page # (of #)
Policy for Information and Data	1.2	1.1	N/A	1(4)

Owner	Changed by	Latest changed	Document type
CTO	Jörgen Olofsson	2022-11-08	Policy

Adopted by	Adopted on (Date)	Status	Replaced by
the Board of Directors	2022-12-01	Adopted	N/A

Policy for Information and Data

Background

What does this policy include?

This policy aims to describe Hemnet Group AB (publ) and its subsidiaries (the “Company", the “Group") approach in matters relating to the use and protection of data and information assets as well as ensuring the protection of personal privacy in accordance with applicable data protection legislation.

Who is affected by this policy?

All employees, hires and consultants at the Company who have in any way been trusted with and given access to Hemnet's data and information assets.

Why have we created this policy?

Much of Hemnet's value lies in the information and data that we have in our information systems, and as part of our business, we collect and process large amounts of data that can be directly or indirectly linked to an individual (personal data).

Information

Hemnet’s overall goal for information and data

Data is an important asset for our business, and we use our data to develop our business and our operations. The use of Hemnet’s data must always comply with applicable laws and take into account the interests of affected individuals’ personal privacy.

Using a risk-based approach, Hemnet will use relevant security measures to protect the business from any form of threat to information systems or data that may interfere with or adversely affect the Company’s business, the reputation or the individual's right to personal privacy. This includes risks that can affect the Company’s information systems and its integrity, confidentiality and accessibility of our data.

Focus

- Hemnet will use all reasonable measures we can to protect and manage our data in a manner that follows applicable data protection legislation as well as our stakeholders' requirements and reasonable expectations. Safeguards shall be designed to include, but not be limited to, availability, confidentiality and integrity.
- All safeguards should, as far as possible, be based on good practice (ex. ISO 27001/27701). When choosing and implementing protective measures, consideration should be given to the impact on the Company’s employees and visitors.
- Appropriate measures shall be taken to ensure the security of physical information assets. These assets include, but are not limited to, the company's offices, computers, networking equipment, and storage devices.

- The Company shall continuously and systematically work on analysing and evaluating the requirements, expectations and risks that exist in our information and data to ensure that the measures taken are relevant and effective. The evaluation shall be conducted in accordance with the guidelines established by the Company's senior executive management team.
- There should be relevant guidelines and procedures for the protection of personal data to ensure that the Company complies with applicable data protection legislation.
- From collection to deletion, the Company must ensure that the data is accurate and trustworthy.
- All information and data assets must be documented, and all assets must be assigned a classification to ensure that they are properly managed.
- In all development work and procurement, the protection of personal data and information security must always be part of the requirements.
- All employees who handle incidents related to information and data should have sufficient knowledge to determine if an incident includes personal information.
- All employees who handle personal data must have sufficient knowledge of the regulations governing personal data processing.
- The Company shall have relevant procedures to deal with all types of incidents arising from identified risks.
- For important information and data assets, there must be a continuity plan that ensures that the business can continue in the event of serious disruptions in accessibility.
- Hemnet shall assign access to information and IT resources only to the extent necessary to enable the execution of assigned tasks, in accordance with the principles of i enlighet med principen om minimum possible access.
- Any person assigned access, eg. in the form of account details, shall be aware that the assignment is personal and may not be made available to another party regardless of its relation to Hemnet or in any way transferred without the prior approval from the function that assigned the access.
- The Company should strive for a culture of high awareness of information security and protection of personal dataAll employees, regardless of form of employment, should be aware of the rules and guidelines that apply to data and information systems and understand the importance of responsible use of the Company's data and information assets.

Governance and management

Hemnet should have clear governance of the Company’s strategic decisions and investments. To ensure that the Company’s use of information, information systems and data is always in line with the business objectives, the senior executive management team shall be responsible for ensuring that there are clear roles with responsibilities and powers documented in accordance with the IT Governance Guidelines.

Exceptions to this policy

In those cases where exceptions are made to this policy, these must be approved by the Board of Directors. All exceptions must be documented, have a clear owner and have a limited time frame. There must be a clear plan, with the responsible person indicated, showing how the exception is to be addressed.

Responsibility

This policy is owned by the CTO, and the policy and all subsequent amendments must always be adopted by the Board of Directors.

Ultimately, the Board and senior executive management are always responsible for Hemnet's information and data being used and protected in an acceptable and legal manner. However, it is incumbent on every employee, partner or other person who has been entrusted with access to our data and information resources to ensure that the protection and use are done in accordance with the intentions of this policy.

Everyone with access to Hemnet's data and information resources has an obligation to report any detected violations in the protection of information and data.

Follow-up & review

This policy is to be followed up annually to ensure that it is implemented and firmly rooted in the business. In connection with this follow-up, a review of the policy should also be made to ensure that it remains relevant and effective. The audit shall be planned and carried out by Hemnet's HoIS and the results reported to senior executive management and the board.

Ensuring compliance with this policy

Updates to this policy

This policy is to be reviewed by the Company's CTO together with the Head of Information Security for content and correctness annually in accordance with Guidelines for Hemnet's Steering Documents.

Assessment of compliance

An assessment of compliance with this policy will be conducted yearly with regards to:

- Correct handling of incidents and that necessary measures have been taken
- That necessary measures have been taken to guarantee integrity, availability and confidentiality of our data
- Existence of continuity plans for important systems and that these are tested according to plan
- That all personnel have been given the necessary information and education to be an active part of The Company's information security work
- A summary of each incident that has occurred during the year, as well as what learning and measures have been taken from these

HOIS is responsible for doing the assessment and reports the result to the CTO.

Any case of non-compliance shall be reported to the Head of Legal.

Reporting to the Board of Directors

The CEO annually reports policy compliance to the Board of Directors. In relation to this policy, the following routines for reporting shall apply.

The Head of Information Security will produce a yearly report for the CTO. The report will account for:

- Exceptions made from the policy during the year
- Discoveries of non-compliance with the policy, including:
    - Measures taken to ensure compliance with the policy, or
    - Measures that are planned to be taken to ensure compliance with the policy
- A summary of assessment of compliance (see above)

Reporting channels for compliance issues

Hemnet's Code of Conduct indicates which reporting channels are to be used by employees who detect violations in compliance with Hemnet's steering documents. Each employee is asked to raise compliance issues with the person concerned in the matter in the first place where possible. If it is not suitable or possible, the employee should contact the immediate supervisor. If that is also not suitable or possible, employees are asked to contact their supervisor's supervisor, Hemnet's Chief People & Culture Officer or Hemnet's Head of Legal. Also, severe misconduct can be reported anonymously via the Company's whistleblower function available via https://report.whistleb.com/en/hemnet.

Violations of this policy

Violations of this policy will always be taken very seriously and may lead to disciplinary action, including dismissal. In addition, violation of relevant laws may mean that you (and/or the Company) are subject to legal sanctions.

Related documents

- Guidelines for Data Safety
- Guidelines for information security
- Guidelines for information classification
- Guidelines for responsible use
- Guidelines for responsibility and authority IT
- Guidelines for choice of suppliers
- Guidelines for Hemnet's Steering Documents.
- Code of Conduct