Policy and strategy for information security Airthings

November 10th 2024

Scope

In Airthings we see information security as a fundamental part of our business. To ensure a process of continuous improvement, we have an information security management system (ISMS) based on ISO-27001 and integrated into our overall risk management and corporate governance structure.

Airthings' policy for information security applies to all information processing in Airthings, both internally and where Airthings is the responsible party externally. This includes all processing, storage, and communication of information (orally, on paper and digitally), as well as all use of information communication technology (ICT) tools. The policy for information security is valid both for how Airthings operate internally and for the products that we create and sell.

The policy applies to all of Airthings' locations and offices. The policy also applies to every employee, partner, contract manufacturer, and consultant that processes information on behalf of Airthings. This means that all relevant parties are expected to comply with the requirements and guidelines for information security set out by this policy.

Objectives and key outcomes

In Airthings we are dependent on the processing of information to deliver our services and products. It is vital that our customers, partners, suppliers, investors, the public and employees are confident that this processing is performed in a secure manner.

Externally, we therefore promise our customers that we will ensure that their data is protected, reliable, and available when and where they need it, that we will focus on sustainable and secure growth, and that we will comply with all relevant local and international regulations. This security promise entails that Airthings needs to be equipped to address the potential security challenges ensuing from the services we provide.

Internally, we also need to ensure a secure foundation for normal operations and future growth by preventing and limiting the consequences of potential security incidents.

To work systematically towards our security objectives, Airthings shall ensure the availability, confidentiality and integrity of our information, systems, and infrastructure. This implies:

- **Ensuring availability:** Relevant information and systems are available to those who need it when it is needed.
- **Guaranteeing confidentiality:** Only people and employees with the right to access and/or with relevant need can access the systems and information.
- **Maintaining integrity:** Information that Airthings is responsible for is only produced and modified by employees or external parties that are authorized to do so. Unintended changes to information shall not occur, and information is always correct, complete and up to date.

Information security strategy

To achieve our security objectives, Airthings needs to ensure that we always meet an adequate level of security, and that we are able to handle and adjust to the ever-changing security risk landscape. In order to achieve this, we need to see information security management as an ongoing process that is based on the principles of continuous improvement.

An example of this process is that we will always strive to improve our security by performing periodical risk assessments (plan), implementing relevant security measures (do), checking that the security measures have the intended effect (check) and maintaining and improving the security measures (act). This process is also the basis for our ISMS, where the system is first established and implemented before it is subjected to a regular review whereupon the relevant content is updated and improved.

Principles

- Airthings shall at all times have a risk-based and cost-effective approach to security management, where we prioritize the security measures that are most important to realize our security- and business objectives.

- The information security in Airthings needs to be adapted to the current risk landscape. We shall therefore perform periodic risk assessments, whereupon necessary risk reducing measures shall be implemented as a part of a process of continuous improvement.

- Airthings aims to follow the principle of least privilege, which implies that any user, program or process should have the bare minimum privileges necessary to perform its function.

- Leaders at all levels shall systematically manage, control and follow up information security in their unit.

- Larger security incidents shall be reported immediately, and information security risks shall – as a minimum – be reported to both the management team and the company's board of directors on an annual basis.

- Our ISMS shall ensure that Airthings achieves the security objectives set out in this policy. To evaluate the effect of the management system, and ensure continuous improvement, the ISMS shall be evaluated and reported on regularly.

- Our ISMS shall be integrated with Airthings' overall risk management and corporate governance processes.

- Information security is satisfactory when the level, scope and orientation of Airthings' security measures are based on risk assessments, and the above-mentioned security objectives are met.
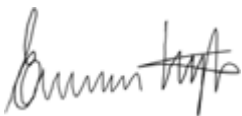
Compliance

- Airthings shall at all times be compliant with relevant laws and regulations in the field of information security.

- Airthings' information security management shall be certified according to recognized standards, such as ISO 27001.

Responsibilities and resources

- The Board has an overall responsibility for information security risk. The Board will periodically receive reporting on information security risk and related issues for Airthings.

- The CEO has the ultimate responsibility for information security risk. The CEO approves this Information Security Policy and is responsible for the ISMS and Airthings' information security risk. The execution of these responsibilities can be delegated to Airthings' Cybersecurity Manager (CSM)

- The CEO is responsible for defining clear roles, responsibilities and reporting lines in the organization, and will ensure that:
  - the guidelines set out in the ISMS are followed in the organization
  - the achievement of the security objectives is reported on periodically
  - risk assessments and security audits are performed periodically

- The Cybersecurity Manager (CSM) role shall develop, implement, and follow up the ISMS on behalf of the management. Among other things, this entails to:
  - ensure compliance with information security policies, standards, regulations and legislation.
  - ensure the alignment of information security and business objectives within the organization.
  - facilitate communication between information security and business stakeholders. o report on information security issues to the organization's senior executive and/or Board.
  - oversee the organization's information and cyber security incidents response activities
  - contribute to business continuity and disaster recovery planning.
  - ensure that a consistent vendor management process is applied across the organization.
  - oversee information and cyber security awareness training.

- All management at all levels, and each and every employee, have a responsibility for information security that is dependent on, and adapted to, their role. The most important part of this is being familiar with, and following, all relevant guidelines and routines from the ISMS.

Oslo, November 10th, 2024

Emma Tryti

CEO Airthings ASA