AIRTHINGS

Policy and strategy for information security

Airthings

AIRTHINGS

Norway: Wergelandsveien 7, 0167 Oslo, Norway, +47 468 46 155
USA: Airthings America Inc., 25N River Lane, Suite 406, Geneva, IL 60134, +1 630 631 1092

Administrative

Document-ID:	
Version:	1
Revision:	1
Summary of changes:	First version of policy
Date of change:	2021-06-29
Classification:	Open for all
Responsible:	Julian Piek (acting until appointment of CISO)
Approved by:	Øyvind Birkenes (CEO) 
Intended audience	The entire company and interested third parties.

Introduction

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) that is 1) based on ISO 27001 and 2) integrated into our overall risk management and corporate governance structure.

A fundamental part of our ISMS is our *policy for information security*. The purpose of this policy is to outline a strategy and define the principles, objectives, roles and responsibilities for information security in Airthings. Moreover, the policy will demonstrate the management team's commitment to information security.

Scope

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 have to comply with the requirements and guidelines for information security set out by this policy, as well as all other relevant documents approved by Airthings' management team.

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.

By meeting these two objectives Airthings creates a foundation for an adequate and balanced level of information security at all levels of the organization that is critical to achieve Airthings' purpose, vision, mission, and key goals.

- Our Purpose and Vision:
    - Empower the world to breath better.
    - Good for People, Planet, and Business
    - Be the global benchmark of air monitoring and control - setting the agenda on how air impacts our life and how to act on it.
- Our Mission:
    - Airthings is on a mission to ensure people around the world take control of their air quality through simple, sustainable and accessible technology solutions – making radon and air quality solutions an essential and universal element for every building or home
- Our key goals
    - Become a global leading air quality technology company
    - Reach NOK 1B in revenue by 2024, with 200m in ARR and +20% EBIT margin

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 (and only then).
- 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.

Related policies

See description of Airthings' ISMS below. The content of the ISMS has not yet been produced, but an outline is included as an attachment to this policy.

Information security strategy

To achieve our security objectives, Airthings needs to ensure that we always meet a minimum level of acceptable 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:

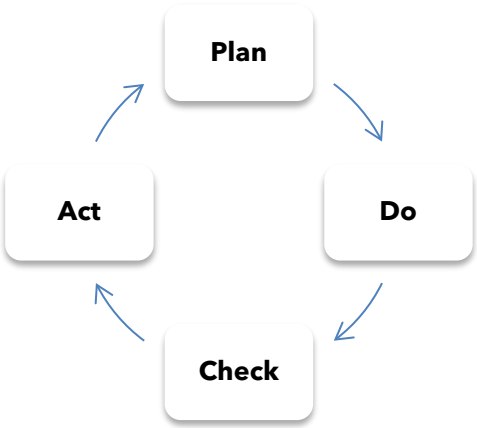

Figure 1: Process for continuous improvement

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 based on recognized standards, such as ISO 27001.

Responsibilities and resources

- The responsibility and authority for information security shall follow the ordinary line of responsibility in the organization.
- The Board approves the information security policy and 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 all relevant policies and is responsible for the ISMS and Airthings' information security risk. The execution of these responsibilities can be delegated to Airthings' CISO. 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 Chief information security officer (CISO) role shall develop, implement, and follow up the ISMS on behalf of the management. In Airthings this role is included in the COO role. 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 organisation.
    - facilitate communication between information security and business stakeholders.
    - report on information security issues to the organisation's senior executive and/or Board.
    - oversee the organisation'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 organisation.
    - manage a dedicated information and cyber security budget.
    - oversee information and cyber security awareness training.

- System owners are responsible for ensuring secure operation of their systems. This entails to:
    - have a documented overview of data flow and processing in the system.
    - be involved in the assessment of system criticality
    - monitor that all security requirements are met (together with the CISO)
    - have an overview of routines and contact points for relevant suppliers and customers
    - be responsible for creating and terminating users with access to the system.

- 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.

Norway: Wergelandsveien 7, 0167 Oslo, Norway, +47 468 46 155
USA: Airthings America Inc., 25N River Lane, Suite 406, Geneva, IL 60134, +1 630 631 1092

Airthings' information security management system

This document is not a complete draft at this point. The description of the ISMS should ultimately include the guiding principles for each of the areas mentioned below, but the actual details should be produced in separate documents. Both the principles and the documents will be developed as we gradually build and define our ISMS.

Airthings' information security management system (ISMS) is based on ISO 27001 and integrated with Airthings' overall risk management and corporate governance processes. The purpose of this document is to describe the ISMS and how we work with information security.

The document:

- serves as the overarching basis for all work related to information security
- specifies all the elements, processes and underlying documentation that are part of the management system.
- distributes responsibilities among relevant parties
- demonstrates the management team's commitment to information security.

Scope

The scope of the ISMS is tailored to Airthings' size and the complexity and extent of information management in the company. It encompasses 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 ICT tools. The management system is valid both for how Airthings operate internally and for the products that we create and sell.

The management system applies to all of Airthings' locations and factories. The management system also applies to every employee partner, contract manufacturer, and consultant that processes information on behalf of Airthings. This means that all relevant parties have to comply with the requirements and guidelines for information security set out by the management system, as well as all other relevant documents approved by Airthings' management team.

Description of the management system

Airthings' ISMS shall ensure a risk-based, balanced and effective level of information security that protects both our own and our customers' valuable information assets. In this context, information security includes all information and supporting systems, including IT-systems, -services, and -components.

The documents and mechanisms that are part of the management system are categorized into a management level, an executive and operational level and a controlling level.

- The **management level** contains the overall requirement for information security (external and internal) as well as the way information security is organized in Airthings.
- The **executive and operational level** contains detailed guidelines, procedures, routines, and action plans. These documents describe how activities should be performed and how responsibilities are distributed. These documents are dynamic and can be revised when needed.
- The **controlling level** contains documentation on the control mechanisms that are used to check that the requirements are met, and guidelines are followed. This includes management's review, internal control and reports and evaluations from the handling of any unwanted security incidents.

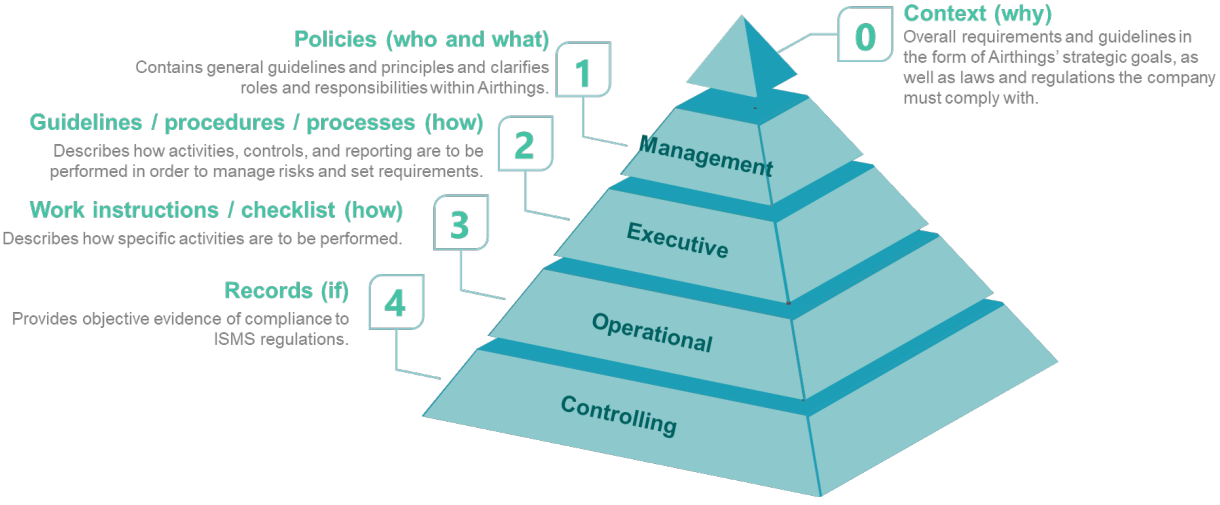

Figure 2: ISMS document hierarchy

Management level (policies and strategies)

External requirements

Relevant laws and regulations

Other external requirements (e.g. contracts and agreements)

Internal requirements

Airthings' business strategy

Policy for information security

AIRTHINGS

Executive and operational level (Guidelines, routines etc.)

Risk management

Information Management

Personnel security

Physical security

Operations security

Communication security (network)

System acquisition, development and maintenance

Supplier relationships

Continuity and incident management

Controlling level (Record etc.)

Internal control / Security Audits

Reporting of security events and weaknesses

The management's review of information security