

Information Security Policy

Contact: Linus Lindström, Chief Information Officer, E-mail: linus.lindstrom@vasakronan.se

Introduction

Information is one of Vasakronan's most important assets and must be managed securely. Our information security work includes the measures we implement to protect our information and ensure that it meets requirements for confidentiality, accuracy, availability and traceability. The Information Security Policy aims to reduce the risk of data hacking, incorrect processing and other security threats. Secure processing of information not only enhances our own protection but also that of our customers.

Goals and purpose

The aim of information security work is to protect all of Vasakronan's information assets. Information security work is tasked with creating security for employees and customers and proactively prepare us to deal with any incidents.

Vasakronan applies a systematic, structured and risk-based approach to work with information security with the aim of offering balanced protection that ensures the right information is available to the right people at the right time and prevents unauthorised use of information.



Governing principles

Integrated work with information security

Information security must comprise a natural component of daily work throughout our operations and support us in reaching our business goals and maintaining a high level of trust. In the event of a need for more concrete and detailed regulations, supplementary instructions or procedures are to be implemented in the relevant function or department.

Risk-based work with information

The measures we take to protect our information must be based on risks identified in operations. Risk mitigation must be performed continuously and new assessments conducted at least annually. A prioritised risk scenario then serves as a basis for information security work moving forward.

Structured and proactive

Our work with information security must be well-organised, proactive and continuously improve – making it easy to do the right thing.

Balanced security measures

When choosing security measures to reduce risks to an acceptable level, we must balance these measures in terms of protection value, threat, risk level, operational impact and cost.

Access to information

Access to information must be based on the requirements of our work duties. Information is a key



component of our work and access to the right information at the right time is crucial to our operations. However, we maintain a high level of protection by limiting access to more information than we need. The type of information we have access to is guided by the categorisation of information into classes.

Incident reporting

Incidents and deviations must be reported immediately and according to the principle of better once too often than once too little. A structured process must be used for their management that enables us to proactively handle and prevent loss and damage.

Information security culture

We are to create a strong information security culture where all personnel have the awareness and knowledge needed to maintain security over time.

Roles and responsibility

All employees at Vasakronan are responsible for complying with this policy. Our integration of information security as a natural component of our work and offering entails that all employees have an important responsibility for information security at Vasakronan.

Company management is responsible for ensuring that work with information security at Vasakronan is conducted in accordance with legal requirements and the company's undertakings.

The CIO, who reports to the company's CFO, is responsible for information security at Vasakronan with the central role of leading, coordinating and monitoring information security work. The CIO ensures compliance with legal requirements, the internal policy documents for information security, the communication of policy to management, awareness raising activities and training.