Information security policy

Background, purpose and scope

This policy, accompanying standards and related procedures is comprised to give Voi Technology AB guiding principles for IT security and information security, as well as defining roles and responsibilities within the area. This policy is fully supported by the CEO and the Executive leadership team (E-team), who acknowledge the value of information security and privacy, as a core component of the business. This information security policy applies to all managers, consultants and employees within Voi Technology. Information security and IT security management in Voi Technology shall strive to efficiently contribute to the business goals and ensure that security related risks are kept at an acceptable level.

Information security principles

Information security shall be designed and implemented in a way that enables it to protect Voi Technology operations, employees and customers by defining appropriate information security controls. Controls should be based on applicable legislation, customer and staff requirements, industry best practice and complementing risk assessments.

- To protect confidentiality, integrity and availability of information, industry best practice expertise shall be applied. Such best practice could include an information security management system based on the ISO 27001 standard.
- Information security shall be evaluated in the annual company-wide risk assessment.
- Business critical assets shall be identified, information security classification shall be performed to ensure that an appropriate level of security controls are applied for processing of critical assets.
- Business continuity planning shall be performed to ensure that serious disturbances and incidents can be managed in an effective way.
- Premises and technical facilities shall be protected by appropriate physical security measures.
- Relevant information security controls shall be designed and implemented when considering acquisitions related to IT.
- Information security awareness training shall be provided to all employees.
- Information security is considered to be part of every employee's responsibility.
- To continuously improving Information Security and the company’s security posture, existing Objectives are reviewed and followed up, while new ones are defined.

The goal of these activities is to ensure that an appropriate level of security is applied for the full life cycle of the IT-components.

IT security principles

IT security is an integral part of information security and shall ensure appropriate protection of IT systems and IT infrastructure.

- The responsibility for all information security efforts has been appointed to the Information Security Officer, who can delegate different tasks to the Information Security Specialist and is supported by the VP Software Engineering.
- An inventory of applications and infrastructural components shall provide an overview of the IT landscape, appointed product owner and other information needed to enable effective IT security governance. The inventory shall indicate which systems or applications that are business critical or handle critical data.
- Access controls shall be implemented to ensure that only intended users have access to IT systems and information, based on business needs. Annual reviews should be conducted on all access rights, privileged access rights should be reviewed in regular intervals.
- Identity lifecycle management shall be performed to ensure that user IDs and corresponding access rights are kept up to date.
- Systems (i.e. virtual servers) shall be protected against DDoS (Distributed Denial-of-Service) attacks, malicious code, apply access controls, patch management, logging functions, backup routines and other appropriate security measures.
- All solutions for remote work or remote access to company assets should be subject to a risk assessment to ensure sufficient security controls have been implemented.
- Critical data assets should be encrypted at-rest and in transit.
- Incident reporting should follow the established IT and Information Security/GDPR Incident Response procedure.
- Appropriate IT security and information security measures shall be defined and applied when sourcing agreements are established. Compliance to Service Level Agreements (SLA) and Data Protection Agreement (DPA) shall be monitored by respective product owner.
- Security incidents shall be logged internally at the company’s incident logging system, followed up by a postmortem and remediations are taken and followed up regularly.

Related policies

- Standards

- Procedures