KINEXON

ISP · Information Security Policy

Public

Table of Contents

KINEXON GmbH
Schellingstr. 35

80799 München

Tel.: +49 (0)89 / 200 61 65-0

info@kinexon.com

www.kinexon.com

This document has been validated for external publication and contains information that is the property of Kinexon GmbH. Reproduction is not permitted without the express written consent of the author. (info@kinexon.com).

If you have any questions, uncertainties or suggestions concerning this document, please send the problem description by mail to KINEXON GmbH. While the utmost care has been taken in preparing this document, KINEXON GmbH does not guarantee that it is absolutely free of errors.

Document information

Code	Version	Date	Author	Approved by	Confidentiality level
ISP · Information Security Policy	1.0	20/09/2021	J. Sanz	Executive Board	Public

Change history

Date	Version	Created by	Description of change
03/09/2021	0.1	J Sanz	Basic document outline
14/09/2021	1.0	J Sanz	Revision and comments by DPO

Table of contents

1 Purpose, scope and users

Top Management of Kinexon has approved the requirements included in this Policy concerning Information Security (IS) as an essential part of its strategy. The goal of this top-level Policy is to define the purpose, direction, principles and basic rules for IS management in Kinexon.

This Policy is applied to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

Users of this document are all employees of Kinexon, as well as relevant external parties.

2 Reference documents

- ISO/IEC 27001.
- Laws and regulations

3 Basic information security terminology

- **Confidentiality –** characteristic of the information by which it is available only to authorized persons or systems.
- **Integrity –** characteristic of the information by which it is changed only by authorized persons or systems.
- **Availability –** characteristic of the information by which it can be accessed by authorized persons when it is needed.
- **Information security (IS) –** preservation of confidentiality, integrity and availability of information.
- **Information Security Management System (ISMS) –** part of overall management processes that take care of planning, implementing, maintaining, reviewing and improving information security (IS).

4 GUIDELINES

4.1 Importance of Secure Data Processing & IS

Data processing plays a key role in the strategic planning of Kinexon as all essential operational functions and tasks are supported by Information Technology (IT).

Overall, it must be possible to compensate for a failure of IT systems without delay to prevent our business being impaired.

Since Kinexon's core competence lies in the development of innovative products, the protection of information against unauthorized access and unauthorized modification is of existential importance for the company.

4.2 Overall Goals

- The availability of all our data and our IT systems is to be secured in such a way that the downtimes to be expected in the event of a malfunction can be tolerated.
- Downtimes close to zero are to be strived for at Kinexon where technically possible. Redundancy must be built into all operationally important Kinexon systems and data structures. Malfunctions and irregularities in data and IT systems of Kinexon are only acceptable to a small extent and only in exceptional cases (integrity).
- Depending on the department of Kinexon, the requirements for confidentiality may have a higher level than legal compliance due to the sensitivity of the recorded data. High confidentiality requirements are to be applied to data generated by our development teams.
- The standard security measures of Kinexon must be implemented in an economically justifiable proportion to the value of the information and IT systems worthy of protection. Instances of damage with important consequences must be prevented through a risk-based evaluation process.
- All employees of Kinexon must comply with the list of legal requirements and contractual regulations. Negative financial and reputational consequences for Kinexon and its employees due to legal and contractual violations must be avoided.
- All employees and managers of Kinexon are aware of their responsibility in dealing with IT and support the security strategy to the best of their ability. Every employee is to be trained regularly on data protection and information security topics.
- The IT Security Officer of Kinexon, in collaboration with Management and Team Leaders, is responsible for reviewing these general ISMS objectives and setting new ones.

4.3 Specific Goals

1. Late or incorrect management decisions can have far-reaching consequences. It is therefore important for management of Kinexon to have access to accurate supervisory mechanisms when making important decisions. A high level of security in terms of availability and integrity must be ensured in Kinexon for this information.
2. Data protection laws and the interests of Kinexon employees require that the confidentiality of employee data be ensured. The data and IT applications of the human resources department of Kinexon are therefore also to be subject to a high level of confidentiality protection. The same applies to the data of our customers and business partners. Through the highest security standards, we aim to build strong trust with our customers and partners to collect, store and evaluate their data.
3. For the sales department of Kinexon, maintaining external communication with customers and business partners through access to the customer database is fundamental to ensure that business transactions are not delayed or endangered.
4. Failing to meet contractually agreed delivery deadlines can have far-reaching negative consequences for Kinexon. Inadequate availability or malfunctions of IT systems and data can play a significant role in such cases and can lead to reduced revenues. Maintaining communication and constant access to correct data for the sales staff is therefore of great importance for Kinexon.

5. The data generated by the research and development department of Kinexon is to have the highest confidentiality requirements as their loss or theft could lead to grave competitive disadvantages. Confidentiality is to be protected and unwanted manipulations are to be prevented by technical measures and a high level of competent attention from employees of Kinexon.
6. The availability and accuracy of systems is to be continuously monitored and safeguarded at Kinexon. Downtimes are only acceptable to the smallest degree, as they can lead directly or indirectly to reductions in revenue, for example through negative impacts on dependent processes.
7. The use of the Internet for information retrieval and communication is now a basic requirement for conducting our business. E-mail or chats (e.g., Teams, Skype) serve as a substitute or supplement to other office communication channels. Appropriate measures are to be taken to ensure that the risks of using the Internet are kept to a minimum. Private use of the Internet by employees of Kinexon is allowed under the circumstances defined in the contract and agreements signed by them, and to be reduced to a minimum extent.

4.4 Information Security Management

- A structured Information Security Management System (ISMS) and a Security Organization has been set up in Kinexon to achieve our Information Security Objectives. An IT Security Officer has been appointed at Kinexon who reports directly to the General Manager in charge of Administration, who will always be independent of the IT management.
- The IT Security Officer and the IT Administrators in Kinexon are to be provided with sufficient financial and time resources by Kinexon Management to receive regular training and information to achieve our Information Security Goals
- A Data Protection Officer (DPO) has been appointed at Kinexon to ensure compliance with all applicable data protection regulations. The DPO is also to be attributed sufficient resources for the fulfilment of data protection duties and is to be required to undergo regular training.
- The IT Security Officer is to be involved in all projects at an early stage to take security-relevant aspects into account as early as the planning phase. The same is to apply to the DPO in cases where personal data are to be processed.
- All IT users at Kinexon must follow the instructions of the IT Security Officer and IT Administrators in security-relevant questions and are to provide sufficient support to fulfil security goals.

4.5 Technical & Organisational Measures

1. For every IS Asset in Kinexon (processes, information, IT applications, IT systems and hardware, buildings, premises and facilities, etc.) at least one responsible person has been appointed who determines the respective protection requirements and assigns access authorizations.
2. Substitutes must be set up for all responsible functions in Kinexon. It must be ensured by means of instructions and sufficient documentation that they can fulfil their tasks.
3. Buildings, facilities and premises of Kinexon are protected by adequate access controls. Access to IT systems at Kinexon is protected by appropriate access controls and access to data by a restrictive authorization concept.
4. Computer virus protection programs are used on all necessary IT systems of Kinexon. All Internet access is protected by suitable firewalls in Kinexon. All protection programs are configured and administered at Kinexon to provide effective protection and prevent manipulation. In addition, IT users at Kinexon support these security measures by working in a security-conscious manner and immediately inform the appropriate authorities in the event of any anomalies.
5. Loss of data can never be completely excluded. Comprehensive data backups, as defined in our backup policy, therefore ensure that IT operations can be resumed at short notice if parts of the operational data stock are lost or incorrect. Information at Kinexon is uniformly marked and stored in such a way that it can be found easily.
6. In order to limit or prevent major damage as a result of emergencies, security incidents at Kinexon must be reacted to quickly and consistently. Measures for emergencies are compiled in our incident response plan. Our goal is to maintain critical business processes even in the event of a system failure and to restore the availability of the failed systems as quickly as possible within an acceptable timespan.

7. If IT services are outsourced to external parties, concrete security requirements are to be specified by Kinexon in Service Level Agreements (SLA). Standardized SLAs are only to be agreed upon if they meet our requirements, particularly regarding our right to control processing activities. For extensive or complex outsourcing projects, an independent detailed security concept with concrete specifications and corresponding measures is to be prepared.
8. IT users at Kinexon are to regularly take part in training courses on the correct use of IT services and the associated technical and organizational measures. Kinexon Management is to support the needs-based training and further education of employees. P&C, in collaboration with IT Security Officer and the DPO, will implement such trainings.

4.6 IS Objectives and its measurement

Objectives for individual IS controls or groups of IS controls are proposed by the IT Security Officer at Kinexon and approved by one of the Managing Directors of Kinexon. All the objectives must be reviewed at least once a year.

Kinexon will measure the fulfillment of all the objectives. The IT Security Officer at Kinexon, in collaboration with Management and Team Leaders, is responsible for setting the methods for measuring the achievement of the objectives – the measurements will be performed at least once a year and the IT Security Officer at Kinexon will analyze and evaluate the results and report them to Management as input materials for the **Management Review Report**. The IT Security Officer at Kinexon is responsible for recording details about measurement methods, periodicities and results in the **MRR-A · Measurement Report** (part of the Management Review Report).

5 Responsibilities

Responsibilities for the ISMS of Kinexon are the following:

- Kinexon Top Management is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring all necessary resources are available.
- The Kinexon IT Security Officer is responsible for operational coordination of the ISMS as well as for reporting about the performance of the ISMS.
- The Kinexon IT Security Officer along with the Top Management of Kinexon must review the ISMS at least once a year or each time a significant change occurs and prepare minutes from that meeting (e.g., when presenting the **Management Review Report**). The purpose of the **Management Review Report** is to establish the suitability, adequacy and effectiveness of the ISMS at Kinexon.
- The protection of the integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset.
- All security incidents or weaknesses detected at Kinexon must be reported to Kinexon IT Security Officer .
- The Kinexon IT Security Officer according to the agreements established with customers and suppliers, and in accordance with the legislation in force, will define which information related to information security (IS) will be communicated to which interested party of Kinexon (both internal and external), by whom and when.
- The Kinexon IT Security Officer along with P&C Manager and the DPO for Kinexon will implement IS training and awareness programs for employees at Kinexon (**IS Training and Awareness Plan**).
- P&C Manager of Kinexon is responsible for adopting and implementing the **IS Training and Awareness Plan**, with the support of the IT Security Officer for Kinexon, which applies to all persons who have a role in IS Management in Kinexon.

6 Support for ISMS implementation

By approving this IS Policy, Top Management of Kinexon declares that ISMS implementation and its continual improvement will be supported with adequate resources in order to achieve all objectives set in this IS Policy, as well as satisfy all identified requirements. The ISMS is to be a continuously improved process leading to an ever increasing level of security for Kinexon's information. As such, processes should be setup in such as way that they can be measured and upgraded later on if necessary. Input from stakeholders on suggestions for improvement should also be welcomed

7 IS Policy communication

The Kinexon IT Security Officer in collaboration with P&C has to ensure that all employees at Kinexon, as well as appropriate external parties are familiar with this IS Policy.