Information Security Policy

Information Security Overview

LeanIX GmbH and its subsidiaries (hereinafter jointly referred to as “LeanIX” or “Company”) are the trusted custodian of information provided to us by our customers, employees and partners and therefore, we shall ensure that due care is exercised in the protection of this information. We rely upon business information being secure, complete, accurate and available in order to meet our business goals.

“*We are committed to enhance confidence and add value to all our stakeholders and customers by protecting all our information assets (including customer data) from all threats.*”

Information security at LeanIX is driven by the following control objectives:

1. Protection of information against unauthorised access by maintaining its confidentiality;
2. Ensuring the integrity of information. Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations;
3. Ensuring the availability of information to those who are authorised and require it. Availability relates to information being available when required by the business process or customers now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities;
4. Meeting the Regulatory and legislative requirements;
5. Creation, maintenance, and testing of Business Continuity Plans;
6. Imparting information security awareness training to all staff;
7. Reporting and investigation of security breaches; and
8. Effective role definition for all employees to avoid conflict in duties and areas of responsibility.

The above mentioned objectives shall be generic to the whole company. Specific department level objectives are covered as part of Objectives & Key Results (OKRs). OKRs shall contain department and in some cases team level objectives, action plans which would describe how to achieve those objectives including due dates, responsible persons and measurement of achievement.

The departments and respective teams shall, to the extent possible and meaningful, derive their OKRs from the Management / Business OKRs to ensure alignment of their department including any Information Security related objectives with the overall business objectives.

Management Commitment

LeanIX Management shall provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS in accordance with the ISO 27001:2013 Standard. In addition, it will effectively demonstrate its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by providing guidance and direction on following:

1. Establishing an Information Security policy;
2. Ensuring that ISMS objectives and plans are established and are compatible with the strategic direction of the organization;
3. Ensuring the integration of the information security management system requirements into the organization's processes;
4. Assigning and communicating responsibilities and authorities for roles relevant to information security;
5. Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement.
6. Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS.
7. Deciding the criteria for accepting the risk and acceptable levels of risk.
8. Ensuring that internal ISMS audit are being conducted
9. Conducting management reviews of the ISMS.
10. Providing decisions on the risk acceptance, budgetary approvals and/ or any other request put forward by the Information Security team for the maintenance and enhancement of the ISMS.

Bonn 31 mei 2022

DocuSigned by:
Marc Zinnemers
1E292E796689411...

Place, Date, Signature:

Name: Marc Zinnemers
Designation: CFO, LeanIX