



Information Security Policy

XIT-POL-007

Policy

- PUBLIC-

Author	Jan Pavel
Version	1.3
Status	Final
Reviewed by	Tomas Kucera
Approved by	Tomas Kucera
Responsible	Jan Pavel
Valid from	9.6.2010
Scope	Whole company

Abstract

This document declares the policy of information security management.

Keywords

Policy, information, security, ISMS, ISO 27001

Modification History

Version	Date	By	Reason
0.1	16-FEB-2010	Jan PAVEL	First draft
1.0	24-MAR-2010	Jan PAVEL	Review after translation, finalization
1.1	29-APR-2010	Jan PAVEL	Minor update after QMS internal audit
1.2	13-JUL-2010	Jan PAVEL	Correction of a typo in the ISO directive number (27000 → 27001)
1.3	13-JUL-2010	Jan PAVEL	Correction of a typo in the ISO directive number (27000 → 27001) in the KTree metadata

Table of Contents

1.	Information Security Policy	4
1.1	Asset Management	4
1.2	Risk Management	4
1.3	Continuity Plans	4
1.4	Declaration of Applicability of the ISMS	4
1.5	Safety Measures, Responsible Persons	5
1.6	Ongoing Evaluation and Continuous Improvement.....	5

1. Information Security Policy

The management of xlTee k.s. recognizes the importance of a standardized management system, and its impact on the level of services provided and overall company performance. For this reason, it has been decided to implement an integrated management system that includes quality management, service management and information security. Moreover, the management established separate policies setting out the following objectives, principles and guidelines to ensure continuing fulfilment or exceeding of customer expectations and the realization of values expressed in the company's mission statement. The policies of the integrated management system are reflected in the system of long-term goals that support the fulfilment of the company's strategy.

The management is committed to complying with internal rules, standards and legislation governing the integrated management system and to ensuring ongoing financial resources needed to observe the respective policies. The management requires that the employees:

- know the principles of the policies governing quality, services and information security and all related internal organizational documents and directives,
- respect the principles of the policies governing quality, services and information security in their actions, activities and within their scope and comply with the requirements established by the management system documentation,
- collaborate and act pro-actively in implementing, improving and developing the management system.

In the field of information security management, the following principles defining the basic framework for the provision of customer service and dealing with suppliers were established by the management.

1.1 Asset Management

- The company implemented a methodology describing the procedures, methods and tools used for classification and registration of assets, determination of personal responsibilities, and evaluation of the importance of such assets for the services provided.
- Any assets that have an impact on the level and availability of services provided are registered. Such assets are assigned responsible persons as well as security risks.

1.2 Risk Management

- The company implemented a methodology for describing the procedures, methods and tools used to identify, quantify and record risks, especially security risks, as well as to determine their relevance to services and to establish criteria for their acceptance.
- Any risks that affect the level and availability of services provided are identified and evaluated according to this methodology. Depending on the probability of risk and its impact on the services, specific preventive actions are taken and recovery plans are established and maintained.

1.3 Continuity Plans

- The company has approved and implemented a strategy of continuity of services and a plan ensuring continuity of services, which helps to ensure the required availability of the services. Security plans and working practices are updated in regular fixed intervals.

1.4 Declaration of Applicability of the ISMS

- The company issued and updates a document describing the specific security objectives and measures.

1.5 Safety Measures, Responsible Persons

- For all the risks exceeding the level of risk acceptance, security measures are proposed, implemented, evaluated and updated.
- The management determined different people responsible for organizing security measures and implementing technical measures. Responsible persons monitor one another.

1.6 Ongoing Evaluation and Continuous Improvement

- All the security problems and incidents are continuously recorded and evaluated, with a view to preventing errors and deterioration in quality of services.
- Regular assessments are carried out (assessment of the risks, residual risks and the levels of acceptable risk), as well as internal safety audits and management reviews with a view to assessing ideas for change and identifying areas for improvement.