ISO 27001

10 KEY REQUIREMENTS

1 INFORMATION SECURITY TEAM

In order to ensure information security, the organisation needs to create a management structure that starts and manages the implementation of information security.

2 PROTECTED ASSETS

Ensuring information security, it is important to define the protected assets, for example in the information systems portfolio all the information systems the company uses, and where the information security risks potentially occur.

3 INFORMATION SECURITY IMPLEMENTATION PLAN

Information security implementation plan defines the steps and follow-up of the practical implementation of the information security work.

4 ANNUAL CLOCK

Maintaining information security has to be a part of the organisation's continuous operations. For example, with annual clock it is possible to ensure that inforation security is up to date at all times by designing future information security maintenance measures.

5 POLICIES

Information security-, privacy- and risk management policy are prepared separately, in which the information security policy is a requirement for the standard. Policies have to be available for stakeholders when needed.

6 GUIDELINES FOR INFORMATION SECURITY

Information security guidelines are prepared for the company's employees, so the whole personnel know how to act information securely. Guidelines for information management is an internal document, that are prepared only for the information security team for more precise guiding in potential information security vulnerabilities.

7 CONTINGENCY PLAN

Contingency plan is prepared so the organisation can define how it ensures information security in all situations. Contingency plan defines for example, how to ensure information security in abnormal situations.

8 INFORMATION SECURITY PROCESSES

Information security processes ensure that information security is secured in the organisation's operations. Processes can be illustrated, for example, visually with swim-lane process diagram, and ensure that they work correctly in each information security situation.

9 INFORMATION SECURITY RISK MANAGEMENT

In the risk management, organisation's information security risks, their significance and probabilities are recorded. It is possible to count an effectiveness figure for risks, that show the unbearable risks for the operation.

10 INFORMATION SECURITY ABNORMALITIES

Potentially identified vulnerabilities and cyber attacks are recorded in information security abnormalities, that work as a "log" to inform what happened and when.

ARTER OY 2018
TEXT AND GRAPHICS:
NOORA LEHTINEN / ARTER OY
EN:
VENLA TULPPALA / ARTER OY