Objectives and aims

Data security policy defines the aims, responsibilities and means of implementation of the Seinäjoki Joint Municipal Authority for Education (maintenance organisation) concerning data security. Data security is part of the quality system of the maintenance organisation.

The objective of data security work in the maintenance organisation is to safeguard the uninterrupted use of data systems and data networks that are important to the uses of the maintenance organisation, to prevent the unauthorised use of data and data systems, the unintentional or deliberate destruction or distortion of data, and to minimise damage caused. In addition to safeguarding operational data processing at normal times, preparations should be made to deal with threats that might result in the suspension of uses and to recover from such situations.

Through administrative, technical and other procedures, the data and data processing systems and services of the maintenance organisation can be kept appropriately protected, during both normal times and emergencies.

The aim of the maintenance organisation is to ensure that data security arrangements are at a good level, both nationally and internationally. The aim is also to ensure that the basic level of data security covers all the data processing of the maintenance organisation, taking into account the basic nature of the faculties and their possible need to boost data security.

Data security

In this document ‘data security’ means the safeguarding of data processing taking place automatically (ADP-based). In addition to this, data security processes concern all processing, transfer and storage of data in electronic, audio-visual, oral and written form.

Data security is built on the confidentiality, integrity and availability of data, and, to a certain extent, on access control and non-repudiation.

‘Confidentiality’ means that the data is only available to those who have been authorised to use it by agreed means and in an agreed timescale, and that such information is not revealed or otherwise made known to a third party.

‘Integrity’ means that the data and data systems are reliable, correct and up-to-date, and have not been changed or damaged as a result of equipment or software defects, natural events or unauthorised human action.

‘Availability’ means that, from an operational point of view and within an acceptable timescale, the data and data processing systems are available and useful to authorised users.

‘Access control’ means that the data and data system cannot be used without the relevant permission.

'Non-repudiation' means the creation of proof in order to ensure that no party involved in the processing or transfer of data can afterwards deny its part in it.

Data security work is the planning and implementation of procedures carried out in order to achieve data security. This work includes methods, tools and procedures for safeguarding data, resources directed at such work and the data security properties of its related equipment.

Data security covers all the maintenance organisation's automatic data security tasks, including archiving.

The assurance of maintenance organisation data security takes place on the basis of rules and recommendations concerning national and international data security, and in observance of guidelines and recommendations issued by government data security organs.

Responsibilities

The highest level of responsibility in data security rests with the Board of the maintenance organisation and with the Director of the maintenance organisation. The directors of the performance units are responsible for data security in their area of performance responsibility.

Together with the Senior Systems Analyst in charge of data security, the IT Manager is responsible for the development of data security as a whole, for the supervision of data security implementation and for the promotion of data security awareness in the maintenance organisation, within the framework of the resources and authority that he/she has been granted.

The practical implementation of data security within the faculties and in their data processing systems is guided and monitored by the data security manager appointed by each faculty.

Within the maintenance organisation, computer system administrators are appointed (persons responsible for maintenance). They appoint a person responsible for each data system or a part thereof.

Each administrator and user of maintenance organisation data systems or data networks is responsible for the implementation of data security. Each administrator or owner of maintenance organisation data systems and the data they contain is responsible for the protection of their data and data systems.

Data security monitoring and dealing with problems

Persons appointed as being responsible for data security have the relevant authority and duty to carry out a study of the data security of maintenance organisation data systems and to initiate action in order to eliminate data security weaknesses that they may observe.

Each user of maintenance organisation data processing systems is obliged to observe the user rules and data security instructions approved by the maintenance organisation. Users and administrators must inform the faculty management, data security manager and IT manager of any data security deficiencies, abuse of data security or suspected data security offence that they may observe. These persons will react to such occurrences in a separately defined way.

In order to guard against serious data security offences, the maintenance organisation will appoint a special group, which will decide on immediate measures required to deal with such offences.

The internal and public reporting of serious data security offences will be dealt with on a case-by-case basis through the central office of the maintenance organisation, either by the Director of the maintenance organisation, the IT Manager or by somebody authorised by him/her.

Implementing data security in practice

Achieving the objectives of data security is a constant process, which includes administrative, physical and technical solutions. On the basis of data security policy, a set of user rules and plans concerning data security will be drawn up for the maintenance organisation. Also in the maintenance organisation's operating units, more specific data security development plans and procedural guidelines concerning different data systems will be prepared.

In order to define the data security development needs and objectives in the maintenance organisation, the organisation's data security risks will be investigated. Such investigation too is a continual process. The aim of the investigation is to identify operational threats, to study the vulnerable points of data processing, to assess threat-related losses and to evaluate the costs of constructing data security to reduce risks. Data security risks will be studied at the level of the teaching, administrative and other systems and operating environments of the maintenance organisation. In addition, the special data security risks of individual departments will be studied.

In order to define the level of data security, the data material and data systems of the maintenance organisation will be classified according to a) the confidentiality of the material and b) the importance of the data systems. A data security level and its related data security procedures will be defined for each security class.

The operating rules that personnel need in their work will be available to them through an internet service and in written form. Students will be informed about data security and the rules and recommendation that concern them. Usually, the data security awareness of members of the maintenance organisation is increased by different forms of communication. The level of data security of the maintenance organisation's data processing and data systems will be evaluated through internal inspection, but also if necessary through external auditing. Data security deficiencies will be analysed with the system administrators and owners.