TUAS Information Security Policy

Introduction

The information security policy expresses the position of the TUAS management on the objectives, responsibilities and implementation methods of information security at Turku University of Applied Sciences.

TUAS has stakeholders which set requirements, obligations, regulations and instructions regarding information security. These stakeholders include, for instance, clients, contractual partners and the legislator.

It is important to take information security threats into account since the everyday operations at TUAS rest on safe and secure functioning of the information systems and networks. In addition to securing information systems in normal times, precautions must be taken for handling threatening situations interrupting the operations and preparations made to ensure recovering from them.

TUAS proportions its information security policies to the gravity of threats, to the level of technological development, and to the costs.

Objectives and main goal

Objectives

Information security must be continuously developed to meet the constantly changing risks, requirements and environments. TUAS' information, data processing systems, information network and its services are appropriately protected in normal, fault, exceptional, and emergency conditions with the help of administrative, technical and other measures.

Main goal

The main goal of information security work at TUAS is to ensure the uninterrupted functioning of those information systems and networks crucial to TUAS' operations, to stop unauthorised use of information and information systems, to prevent intentional or unintentional destruction or distortion of information, and to minimise the caused damage.

Information security – concept and definition

Information security means securing all information processing. Information security work refers to planning, implementing, supervising, monitoring and guiding the measures to be realised in order to achieve information security. This work includes methods, tools and actions for protecting data, resources allocated to the work, and the information security properties of the equipment.

Information security is built on confidentiality, integrity and availability of information and also, where appropriate, on access control and non-repudiation.

Confidentiality means that the information is only available to those so entitled in an agreed manner and at an agreed time, and it will not be disclosed or otherwise put at the disposal of unauthorised persons.

Integrity means that the information and the information systems are reliable, accurate and current and have not been altered or damaged as a result of equipment or software flaws, natural disasters or unauthorised human action.

Availability means that the information and the information processing systems are available and usable to authorised users within an acceptable time considering the nature of operations.

Access control means that the data or the information systems cannot be used without permission.

Non-repudiation means creating evidence to ensure that no-one, who has processed or transferred data, can dispute their part in it afterwards.

Information security covers all information processing at TUAS, including archiving of various types of documents. Information security measures concern processing, storing, sharing and transferring information in electronic, spoken or written form.

Factors maintaining information security

The information security at TUAS is maintained according to national and international regulations concerning information security and abiding by both the government instructions and recommendations for information security and the information security requirements of CSC – IT Centre for Science.

Community subscriber

As a community subscriber TUAS has the responsibility to ensure the security of its operations, telecommunications, equipment, software and documentations. In its communications network, TUAS handles confidential messages, identification information, information concerning stakeholders and personal data.

Some of the personal data items handled at TUAS are sensitive. These include, for instance, data concerning students and their health assessments (Polytechnics Act 351/2003). Clear guidelines concerning data handling and sharing must be given to all stakeholders. In different educational areas at TUAS, real working life data, also including confidential data, such as patient, vehicle inspection and account data, and business secrets of the organisations acting as student traineeship posts or as the commissioners of theses, are handled. In its operations, TUAS follows the good practice on information management according what is mentioned in the Act on the Openness of Government Activities (621/1999) and the Personal Data Act (523/1999). Other key regulations concerning data protection are the Act on the Protection of Privacy in Electronic Communications (516/2004) and the Act on the Protection of Privacy in Working Life (759/2004).

Good maintenance

Information security work implements for its part the good maintenance of the information systems and networks. Good maintenance refers to maintenance which is methodical, responsible and professional and in which the good practice on information management regulated by the Act on the Openness of Government Activities and by the Decree on the Openness of Government Activities and on Good Practice in Information Management is taken into account.

Responsibilities

Vice Rector and TUAS Board

The Vice Rector leads the overall information security management at TUAS. The Vice Rector shares the highest responsibility with the Board of TUAS, which is in charge of implementing information security and creating the necessary preconditions.

Information security group

The Vice Rector appoints an information security group to ensure that all the actions and requirements relating to information security will be fully covered. The information security group represents the different views on information security at TUAS, reconciles information security actions with the security level, and manages information security actions.

The main tasks of the information security group include realising risk analyses, drawing an information security development plan and monitoring the implementation of the plan, organising an audit, and preparing a Board review.

Information security officer

TUAS has an information security officer appointed by the Rector or according what has been determined in TUAS' operational rules. The designated information security officer is responsible for monitoring and reporting on information security, for supervising the implementation of information security, for carrying out development projects, and for the promotion of information security awareness. The designated information security officer acts within the boundaries of the resources allocated and the authority granted to him with the help of the information security group and serves as the chairperson of the group.

Information security contact persons

The designated information security contact persons lead and control the implementation of information security in their respective units or campuses and within their respective information processing systems.

Supervisors

Supervisors are responsible for ensuring that their own staff members are aware of information security requirements and regulations and that they obey those. The supervisors are in charge of introducing new employees and substitutes to the information security principles of their respective units. The supervisors themselves deal with minor and unintentional breaches of information

security. All serious breaches of information security must be reported to the information security officer at TUAS.

Administrators and users of information systems and networks

All persons who handle information of TUAS, maintain or use TUAS's information systems or networks are ultimately responsible for implementing information security for their own part.

Owners of information systems and information

The owner of an information system, for instance, holds the responsibilities of a data controller mentioned in Personal Data Act and is in charge of the information security of his/her own respective information system including: reporting, security classification, maintenance of the user right register, user rights, usage, confirmations, support, training, maintenance, development, and planning of continuity and being prepared for emergency situations. Training is arranged on a regular basis in order to ensure that everyone knows their responsibilities.

TUAS units

All the units of TUAS shall make provision for the implementation of information security in their own action plans.

Subcontracting and outsourcing

The responsibilities and requirements concerning information security at TUAS are also extended to all subcontractors and to the suppliers of outsourced services.

Means of implementation

The basis for implementing information security is this written information security policy approved by the TUAS management.

The policy will be disseminated in the Internet and intranet to reach each and every TUAS staff member, student and person using the information systems of TUAS.

Charting of risks

The obtaining of the information security goals is a continuous process based on administrative, physical and technical solutions. In order to define the development needs and goals for the TUAS information security, the information security group charts the information security risks regularly. The objective of the charting is to identify potential threats to operations, to chart the vulnerable points in information processing, to assess the losses in the event of a threat materialising, and to assess the costs of information security measures in order to minimise risks.

Information security plan

On the basis of the information security principles and the charting of risks, the information security group formulates an information security plan which is revised regularly.

The information security principles are included in the enterprise architecture of TUAS, and that way they will be taken into account, for instance, when purchasing information systems.

Classifying documentation and information systems

In order to define the level of information security, the information security group together with the help of experts assesses and classifies TUAS' information material and information systems according to the confidentiality and importance of them. Each security class will be assigned the required information security level and information security measures accordingly.

Information system owners

The Vice Rector appoints a sole owner for each information system or part of it. The owner of an information system has the responsibility concerning introduction to the information system under his/her responsibility.

IT Services

IT Services is responsible for the basic technical aspects of information security. One of the fields of expertise of IT Services is information security. IT Services takes actively part in planning information security and implementing information security work. IT Services maintains their information security skills which are at the disposal of each TUAS unit. IT Services provides expertise and consulting services relating to information security. Information security training is organised in cooperation with the persons responsible for personnel training.

Documents

Documents stipulating how information security is to be achieved are approved and made available to the relevant target groups.

Informing

Informing on information security matters outside TUAS and within TUAS on a general level is under the responsibility of the TUAS information security officer. The designated information security contact persons within the units will also participate in internal informing at their units.

The information security group informs the students and staff of TUAS about information security and about the rules and instructions concerning them.

Monitoring of information security and handling of problem situations

Monitoring information security

The persons appointed responsible for information security have the authority and the duty assigned by TUAS to chart the information security at TUAS and to take action in order to minimise the observed risks.

All persons using the TUAS information systems are bound by the approved rules for the use of the systems and by the information security guidelines.

Handling problem situations and reporting on them

Users and administrators must report any observed information security flaws, misuse pertaining to information security or any suspected breach of information security to the information security contact person at their unit, or directly to the TUAS information security officer.

The TUAS information security officer reports to the TUAS management and, if necessary, to the TUAS Executive Board on any serious breach of information security or any suspicion of it.

This information security policy is effective as of the date of approval.

In Turku, 18 December 2012

Juha Kettunen

Rector