Definitions of information security policy

Administrative and organizational information security

Administrative means to improve information security such as organization, definition of tasks and responsibilities as well as guiding, training and monitoring the personnel.

Availability

The attribute that information, an information system or a service is available for access and use at desired time and required manner to those entitled to use it.

Baseline security

Minimal steps taken to ensure the flawless functioning of information processing and action procedures under normal circumstances. (An information security level, where the owner of the system is prepared to take routine action in case of accidents and interruptions occurring under normal circumstances.)

Classification of data

1) Separation of information into classes according to classification keys set by the owner of the information. A classification key can be e.g. the confidentiality of information or its relevancy to the functioning of the organization.
2) The vulnerability of information to unauthorized handling and revealing as well as the loss or nuisance caused to the society or the state by these serve as the basis of security classification in state administration. A classification key for information may be e.g. their need for protection, their ownership or their real time accuracy demand.

Classified information, security classification

Dividing confidential documents and information into classes based on confidentiality. State administration security classification is defined in national security auditing criteria (KATAKRI).

Note! All information handled at TUT is not subjected to national security auditing criteria. This information is handled using TUT internal security criteria.

Computer security; facilities security

The actions to implement information security pertaining to the usability, functionality, definition of configurations and access control of information processing and telecommunications hardware and facilities along with actions pertaining to availability of spare parts and accessories.

Confidential information

Information meant to be accessed by only a certain person or persons. According to state security classification, the term confidential corresponds to security class III.

Confidentiality

Keeping information confidential and keeping the rights to information and telecommunications from endangerment and deliberate breaches of security.

Data security

Steps taken towards information security in order to maintain the usability, integrity and confidentiality of documents, files and other data by means of data cataloging and classification along with guided administration, handling, storage and disposal of information storage.

Telecommunications security

1) State where information security has been implemented where telecommunications hardware, telecommunications systems and the information transferred therein is concerned.
2) Legislation, norms and steps taken to ensure secure telecommunications. Such steps are, among others, maintenance of hardware and data links and their configurations, network administration, access control, data link use control and monitoring, logging and resolving problem situations, securing and encrypting communications and testing and approving telecommunications software.

Exceptional situation

A situation facing the organization that can also occur under normal circumstances. Such situations include fire, electrical or air conditioning malfunction, a devastating crime, strike or loss of key personnel.

Extraordinary circumstances

A serious threat to the sustenance of the Finnish people, the economic life, justice system, basic rights of citizens, the territorial integrity or the independence of the country brought on by the international situation or a catastrophe.

According to Emergency Powers Act (1080/1991, changed 198/2000) possible extraordinary circumstances include, among others

- an armed assault against Finland, war and aftermath of war
- a serious breach against the territorial integrity and a threat of war
- a war between foreign powers that presents a threat to Finland
- a serious financial threat to Finland due to import complications or a catastrophe

Information security

1) State where information, information systems and services receive appropriate protection in such a way that threats against their

confidentiality, integrity and usability do not cause significant damage to society and it members.
2) Legislation and other norms along with steps that are taken to ensure information security under normal as well as exceptional circumstances.

It is customary to separate implementation of information security to eight segments of action: administrative, personnel, physical, telecommunications, hardware, software, data and usage security.

Information security incident

Intentional or unintentional event or circumstance, due of which the usability of the information within the organization's responsibility is not on planned level or the integrity or confidentiality of said information has been compromised.

Information security manual/documentation

University's common, units' internal and service or system wide guidelines to secure information processing.

Information security norm

A decree or an order by the authorities, which is geared towards securing the confidentiality, integrity and usability of information or information processing by seeking to combat threats targeting the aforementioned or regulating information security development work or organizations conducting said work.

Information security plan

A plan to implement and maintain baseline security under normal circumstances. The plan covers the goals, administration, tasks and procedures of the information security work within the organization. Vital information systems are named and steps taken for their recovery are defined.

Information security planning

A planning process containing, among others, threat analysis, definition of baseline security and planning for recovery readiness and extraordinary conditions. This process will result in information security plans, decrees and guidelines.

Information security policy

Same as information security strategy. Information security principles. An organization-wide vision on goals, principles and implementation of information security approved by the management.

Integrity

1) The genuineness, absence of alteration, absence of internal conflict, adequacy, status of being up-to-date, accuracy and usability of information or information systems.

2) The attribute that information or a message has not been altered without authorization, and that eventual changes can be verified from the logging chain.

IT security

Information security pertaining to the information technology of the organization, such as telecommunications, hardware, software and their use.

Operations security

The means of improving information security that pertain to use of information technology, usage environment, information processing and its continuity along with those pertaining to support, maintenance, development and service functions.

Personal security

Personnel security pertaining to personnel and to students where applicable.

Personnel security

Controlling information security risks pertaining to personnel with regards to job applicability, job descriptions, temporary handling of duties, and rights to access and use information, protection, security training and monitoring.

Physical security

Protection of persons, hardware, data, mail, facilities and stores against destruction and accidents. Physical security consists of among others supervision of traffic and facilities, guarding, defense against fire, water, electricity, air conditioning and burglary damage as well as the security of couriers and mail containing information.

Security

State, in which known threats do not present mentionable risk and they can be controlled.

Software security

Actions to improve information security upon operating systems and other software such as software recognition, isolation, access control and backup methods, monitoring and hunting actions, logging and quality control along with actions pertaining to software maintenance and updating.

Total security

The University's security consists of nine areas: security of operations, security at work, environmental security, rescue functions, preparedness planning, information security, personnel security, security of facilities and crime security.