Decision maker: The Vice-Chancellor Type of document: Guidelines Period of validity: Until further notice	Decision date: 23-12-04 Valid from: 2023-12-04
Replaced document(s):	

Guidelines for information security in procurement and purchasing

Table of contents

1. INTRODUCTION 3

2. THE PURPOSE OF THE DOCUMENT 3

3. ALLOCATION OF RESPONSIBILITY AND TASKS 4

4. INFORMATION SECURITY IN PROCUREMENTS AND PURCHASES 4

4.1 THE INFORMATION SECURITY PROCESS 5
4.2 CONFIDENTIAL AND SENSITIVE INFORMATION MANAGEMENT 5
4.3 PROCUREMENTS SUBJECT TO PROTECTIVE SECURITY 6

5. FOLLOW-UP 6

1. Introduction

Luleå University of Technology strives for a high level of information security in all its information processing. Through systematic work on information security, risks can be identified at an early stage to prevent information from falling into the wrong hands, or being distorted or destroyed. If this happens, it could lead to expensive and time-consuming measures following the conclusion of a contract or the acquisition of a product.

It is particularly important to identify confidential information early, for example, personal data, research data or other types of organisation-related information comprised by and affected by the procurement or the acquisition. Confidential or sensitive information and integrity-sensitive personal data may not be processed in, for example, cloud-based services[1] without the University having carried out a detailed risk assessment and taken necessary security measures. It is also important that decisions on the handling of and access to information are documented. Furthermore, the decisions must be taken by the authorised head in accordance with the *Vice-Chancellor's Decision and Delegation Procedures* for Luleå University of Technology.

Information security in the procurement and purchase process is specifically important upon the acquisition of services or products that will handle, process, store or transmit organisation-related information or data in any way. It is about securing that the procured service, product or IT system meets the requirements necessary to protect the information both within our organisation and with the supplier during the entire period of agreement.

2. The purpose of the document

The present guidelines are part of the University's Information Security Management System, ISMS, and their purpose is to ensure that University staff are well versed with and know how to comply with existing rules and regulations concerning procurement and purchases in an information secure manner. The document is essentially based on the guidelines for information security for procurement produced by the Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, MSB)[2].

The guidelines include a description of what information security is, an overview of responsibilities, and instructions on what to do in terms of information security prior to a procurement or purchase. Regardless of whether there is a procurement/purchase of a service, a product or an IT system, the systematic information security process must be followed, to obtain secure handling of information. A detailed description of the process is

[1] The term cloud-based services is an umbrella term for a large number of internet services that provide various types of IT solutions. It may involve software, data storage and other collaboration functions.
[2] MSB1177 – November 2018

available on the webpage section *Working procedures for information security in procurement and purchasing*[3].

3. Allocation of responsibility and tasks

The head of the organisational unit/equivalent, according to the Vice-Chancellor's decision and delegation procedures for the University, is responsible for securing that preconditions exist enabling the staff to follow the information security process in accordance with the model described in section 4.1 below. The information security work must be documented, approved and entered in the official register.

The individual member of staff or other person participating in the procurement process must follow current guidelines and be updated about how to manage information security when procuring or purchasing services, products or IT systems.

Besides providing support regarding the actual purchase/procurement, Professional Services provides support to identify information security requirements, IT security requirements and legal requirements that have an impact on the basic conditions for the purchase or procurement.

In good time before a purchase or procurement, contact should be made with the information security coordinator for support and advice.

4. Information security in procurements and purchases

To carry out a procurement, direct award or purchase in an information-secure manner involves identifying and setting out adequate requirements for the University's information to be handled in a secure manner both internally and by an external supplier. With this initial work, the University can prevent important information security requirements and other requirements from being overlooked only to appear later in the procurement or purchase process, or to appear after the conclusion of the University's agreements. Such situations may be both costly and time-consuming, but also risk the information security.

Information security requirements and, where applicable, IT security requirements are to be compiled in a specification of requirements, be very detailed and possible to evaluate. The requirements, formulated in connection with the individual procurement or purchase, are to be clearly defined, by specifying which requirements are mandatory ("must") and which are non-mandatory ("should").

[3] https://www.ltu.se/en/staff-web/services-and-support/security/information-security/information-security-in-procurement-and-purchasing

The supporting documents of a specification of requirements are to be based on the information classification, the self-evaluation and the risk assessment related to the information processing that the procurement/purchase is subject to or is to handle. It is above all the members of the relevant unit/equivalent for the present procurement or purchase process who should define which information is involved.

4.1 The information security process

An information classification is to be carried out based on the sensitivity and worth of protection of the information where the starting point is the three aspects confidentiality, integrity and availability. The information classification is to clarify the needs for protection of the information.

It is very important to identify the security requirements and legal requirements that will form the basis of the information security requirements to be set for the service, product or IT system (also known as self-evaluation).

After that, a risk assessment must be carried out to raise the awareness and knowledge of decision-makers and other responsible persons about threats, risks and vulnerability related to the relevant unit/equivalent with reference to procurement or purchase. This assessment adds to the basis for planning, implementation and training regarding the procured product or service.

A detailed description of how to carry out this work based on procedures and working practice is available on the webpage section *Working procedures for information security in procurement and purchasing*[4].

4.2 Confidential and sensitive information management

Confidential or sensitive information and integrity-sensitive personal data[5] cannot be processed without the University having carried out a detailed risk assessment and taken necessary security measures. Decisions on management and measures are to be taken by the responsible head and must be documented and registered.

[4] https://www.ltu.se/en/staff-web/services-and-support/security/information-security/information-security-in-procurement-and-purchasing
[5] GDPR

In cases where cloud-based services are purchased to serve as IT support to manage information, consideration must be given to legal risks related to personal data handled by suppliers outside EU/EEA or by countries being approved by the European Commission.[6]

4.3 Procurements subject to protective security

When the University intends to make a procurement involving information that is subject to protective security, there are special requirements, for example:

- Protection against offences that may threaten Sweden's national security
- Protection of secret information concerning Sweden's national security
- Protection against terrorism

In a procurement that is subject to protective security and includes a protective security agreement, a separate protective security assessment must in some cases be carried out and documented. Prior to the procurement process, the contracting authority, that is, Luleå University of Technology, must consult Swedish Security Service (Säkerhetspolisen), which is the supervisory authority of national security. An application for consultation with the Swedish Security Service must be submitted before the contracting authority publishes the procurement.

More information is available on the webpage section Working procedures for information security in procurement and purchasing[7].

5. Follow-up

The University is to check that the specified information security requirements are expedient and adequate and that the contracted party has implemented the agreed security measures. The follow-ups must be documented. This is important to maintain security of the procured product or service during the period of agreement.

[6] European Commission, Adequacy decisions: How the EU determines if a non-EU country has adequate level of data protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en,
US organisations: Participant Search (dataprivacyframework.gov)
[7] https://www.ltu.se/en/staff-web/services-and-support/security/information-security/information-security-in-procurement-and-purchasing