GÖTEBORGS UNIVERSITET

Division of Buildings and Services
Leif Bouvin
031-789 58 98

CONTROL DOCUMENT
24-05-07 ref. no. A 13 349 / 07

Policy for IT security

Date of Publication	November 2014
Published	www.gu.se
Decision-maker	Vice-Chancellor
Date of decision	24-11-2014
Person responsible for document	Leif Bouvin
Period of validity	Until further notice
Summary	”Policy for IT security” at Göteborg University sets out the overall focus and goals, along with the overall responsibility and organisation, for IT security work.

Division of Buildings and Services
Karl Gustavsgatan 12 B, Box 100, SE 405 30 Göteborg
031 786 0000, 031 786 1142 (fax)
www.gu.se

GÖTEBORGS UNIVERSITET

November 2014

Policy for IT security

Work shall be actively carried out on IT security and risk analysis to enable the University to perform its functions within education, research and cooperation with the surrounding society effectively and at a high level of quality. The University shall be, and be perceived to be, a secure collaborative partner.

IT security work shall be focused on ensuring

- a high level of accessibility to information and services
- integrity of the information through protection against unintentional and intentional misrepresentation
- authorization checks based on classification of the sensitivity of the information
- traceability,
- confidentiality and the possibility of protected communication.

Every user is responsible to make sure that the current policy and regulations for IT security are applied and followed within their own area of responsibility.

The external functions that are connected to the University's IT resources shall comply with the University's regulations and policy for IT security.

Responsibility and organisation

The Vice-Chancellor has the overall responsibility for IT security. The responsibility from Vice-Chancellor follows the line organisation.

The Vice-Chancellor appoints persons to be IT-delivery owner with technical responsibility for security and operation of the University's common IT systems and communication networks.

The Dean, the Chief Librarian and the Head of Administration shall appoint IT-delivery owners? technical managers for security and operation of the IT system and communication network within their respective areas of responsibility.

Information responsibility

Information owner

All information must have an information owner. The information owner is the person who issues and/or approves a certain piece of information and who is responsible for ensuring that the information is correct and reliable, and for the way in which it is distributed. Information owner is responsible for:

- that information is assigned an a classification from the criteria: confidentiality, integrity, traceability and availability
- in cooperation with system manager create security requirements from the results in the information classification for how to handle the information. Security requirements should be stated in alignment with confidentiality, integrity, traceability and availability.
- in cooperation with system manager create rules for authorization based on information classification.

System- and operational responsibility

System owner

A system owner (official with responsibility for the system) must be appointed for each IT system. System owners are responsible for attending to the users' requirements and have overall responsibility for ensuring that the IT system supports the operations and goals. The system owner is responsible for:

- making sure that analysis of the technical security measures is made in alignment with confidentiality, integrity, traceability and availability and that vulnerabilities are managed.
- that the information owners rules for authorization is ensured,
- ensuring IT-delivery owners security requirements are met.

IT-delivery owner

For the technical administration an IT-delivery owner should be appointed. IT-delivery owner is responsible for

- making sure that analysis of the technical security measures is made in alignment with confidentiality, integrity, traceability and availability and that vulnerabilities are managed.
- that the information owners demands for security measures are technically realized.

Responsibility for authorization

Authorization Manager

Authorisation managers decide on allocation of access rights to the University's common and local systems, and are also responsible for following up access rights that have been allocated. Allocation and follow-up must comply with guidelines set by the system owner and IT-delivery owner.

Authorisation managers are heads of department, heads of division in Central Administration, heads of section for libraries within the University Library, heads of faculty offices, the director of national unit or equivalent.