Division of Buildings and Services	**CONTROL DOCUMENT**
Leif Bouvin	24-05-07 ref. no. A 13 349/ 07
031-786 58 98	

Appendix, ”Definition of roles and terms”, to policy for IT security

Date of Publication	June 2007
Published	www.gu.se
Decision-maker	Vice-Chancellor
Date of decision	11-06-2007
Person responsible for document	Leif Bouvin
Period of validity	Until further notice
Summary	The appendix, ”Definition of roles and terms” provides definitions of roles and terms that are used in policies, regulations and guidelines for IT security as well as in other control documents concerning IT.

May 2007

Definition of roles and terms

An employee can, primarily with regard to smaller systems, occupy several of the roles below. In order to prevent irregularities, the combination of roles that grants authorisation for a transaction and at the same time authorisation to conceal the transaction by, for example, deleting a log, is not permitted.

E.g. a personnel administrator who is authorised to perform transactions in the personnel administration system may not simultaneously be technical manager or system administrator for the same system.

The principal connection between the roles below is set out in ”Basic outline of roles and responsibilities”, page 5.

Authorisation administrator

Authorisation administrators are appointed by authorisation managers and are responsible for registration and deregistration of access rights in accordance with the decisions of the authorisation manager. The administrator is also responsible that decisions on allocation of authorisation are filed according to the stipulated filing requirements.

Authorisation manager

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

Authorisation managers are:

- head of department
- head of division in Central Administration
- head of section for libraries within the University Library
- head of faculty office and equivalent.

Information owner

The information owner is the person who issues and/or approves a certain piece of information and who has responsibility that the information is correct and reliable and for the way in which it is distributed.

All information must have an information owner.

The following table gives examples of who is considered an information owner in different cases, unless decided otherwise.

Category	Owner (unless indicated otherwise)
Approved documents	The person who approves the document
Data in information systems	The system owner
All other information	The issuer

Isolated network

An isolated network has no connections whatsoever with the Internet or other networks. It must not be possible for any IT systems outside the isolated network to communicate with IT systems in an isolated network.

IT infrastructure

Basic university-wide configuration of servers, clients, operating systems, networks, work stations, printers, software, databases etc.

IT facilities

IT facilities refer to computers, software, licences and all other peripheral equipment that are used in connection with handling information in digital form.

IT system

IT system refers to equipment and software that handle, i.e. gather, process, store and distribute information and exchange data between functional units using data transfer and in accordance with technical protocols.

IT service

Functions that users utilize and that are based on IT infrastructure and IT systems specific to activities.

Protected network

In a protected network both incoming and outgoing traffic is regulated, which means that there are regulations for how IT services in the protected network are permitted to communicate with IT services outside the protected network.

The restriction lies in the infrastructure and is not a part of the IT service's authentication process as is the case with, for instance a login procedure. Firewalls are examples of how to create protected networks.

System

System is defined in IT security documents as a broader term which contains not just the IT system but also the manual routines and human resources that go together with an IT system.

System administrator

Is responsible that the stipulated security requirements are applied in the technical administration and operation of IT systems. System administrators are not permitted to be users of the administrative system for which they are system administrator.

E.g. a personnel administrator who is authorised to perform transactions in the personnel administration system may not simultaneously be system administrator for the system in question.

System manager

Is responsible for system management based on the system owner's directives with respect to application, the users' requirements and needs. The system manager must have in-depth knowledge about the operations that the system is to support, as well as overall knowledge about the technology that is applied in the system.

System owner

A system owner (official with responsibility for the system) must be appointed for each IT system. System owners are to attend to the users' requirements and have overall responsibility that the IT system supports the operations and the goals. It is the responsibility of system owners that

- analysis of security requirements are carried out with respect to information content and operational requirements. The security requirements must be indicated with the focus on availability, integrity, confidentiality and traceability
- guidelines for allocation of access rights are drawn up
- technical officers' security requirements are met.

E.g. the director of personnel and organisation development is the system owner for the personnel administration system and a head of a research team can be system owner for the team's research database.

Technical officer

An official with technical responsibility is to be appointed to ensure technical reliability. It is the responsibility of the technical officer that

- analyses of technical security are carried out with respect to availability, integrity, confidentiality and traceability and that deficiencies revealed are rectified.
- system owners' security requirements are met technically.

For example, the head of the department for information technology, the IT manager at the Sahlgrenska Academy, faculty and University Library respectively.

Technical manager

Is responsible for the technical administration of the system based on the technical manager's directives. The technical manager must have a good knowledge of the system's design, data management and technical security format, as well as overall knowledge of the operations that the system supports.

User

Person who is allocated access rights to use Göteborg University's IT facilities and whom it must be possible to identify.

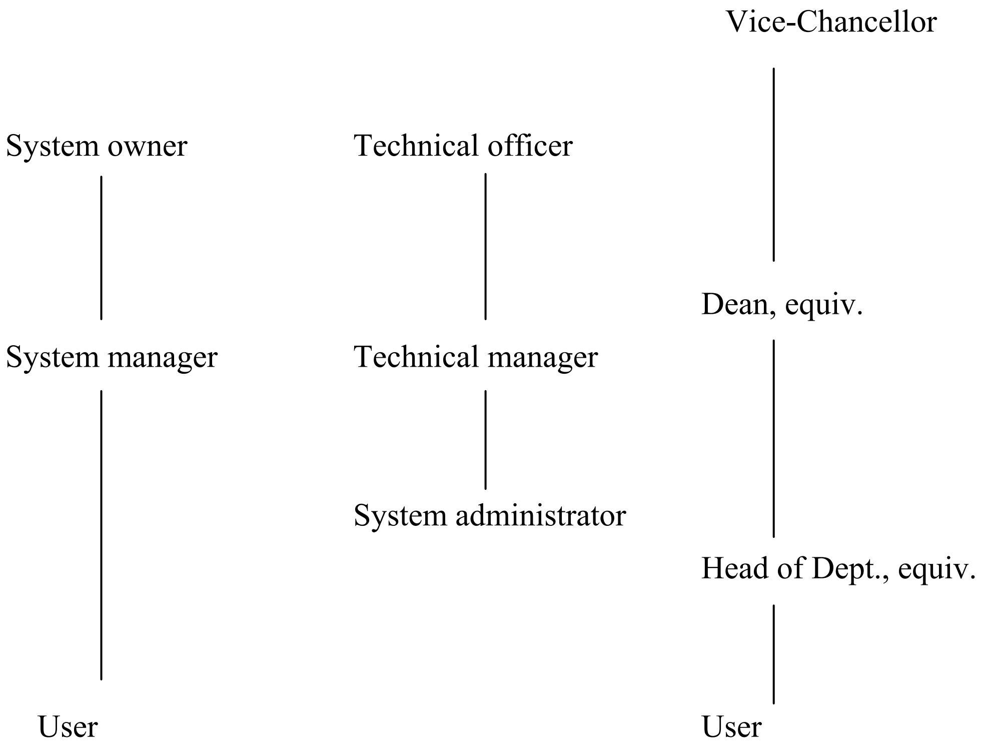
Basic outline of roles and responsibilities

System- and operational organisation

(System and operational-/technical responsibility)

Line organisation

(Overall responsibility for IT security)



Note

In the system- and operational organisation, an employee can, primarily with regard to smaller systems, occupy several of the roles above.

Technical managers are appointed at University-wide level and faculty or equivalent level respectively.

The lowest level at which system owners are appointed is head of department or equivalent.