Umeå University, 901 87 Umeå
Vice-Chancellor

Note: The English version did not exist at the time of the decision

Plan

Reg. No.: 100-3305-10
Date: 8 February 2011
Unit responsible: IT unit
Validity: Until further notice

IT security plan at Umeå University

By IT security is meant security in the use of the University’s IT resources.

Goal

IT security at Umeå University shall:

- secure the University’s use of the communications network and IT systems without unnecessary disruptions and with the functions intended and high accessibility.

- prevent disruptions in the communications network and IT systems from causing serious consequences for the University’s employees and students and the general public.

- secure the information that is transmitted, stored or dealt with in the communications network and IT systems so that it is protected against accidental, unauthorised or forbidden transformation, destruction, accessibility or copying.

- secure the communications network and IT systems so that they are protected against intrusion, forbidden usage, theft or damage.

Liability

Please see the Information security policy for Umeå University.

Support, coordination and control

The Universitety shall have centrally financed resources for support, coordination and control regarding IT security.

The IT Director is responsible for:

- the overall coordination of all IT security work at the University.

- the design and revision of regulations and instructions.

- the preparation of It security questions for the Board and the Vice-Chancellor.

- the coordination of IT security for the central IT resources.

Regulations and guidelines

Fixed regulations and guidelines must exist for computer security in the the communications network and IT systems that are of special importance to the University, and for such protective measures as are of special significance for the IT security at the University.

Protective measures

In all security work, the protection of life, health and personal integrity is of the highest value. The levels of security and measures of protection for the IT security at the University must be designed so that the goals for IT security can be attained at reasonable cost and without more complication of daily operations than is necessary.

The formulation of security levels and protective measures must be based on the current and anticipated threat situation, and on the consequences of disruptions for the University or its employees and students as well as the general public. Consideration shall be taken to direct as well indirect consequences.

Assessments of the threat situation and the consequences of disruptions shall be made systematically using established methods.

In order to be connected to SUNET, the IT security at the University must meet SUNET's regulations.

Protective measures for IT security shall be based on established standards.

Information and education

The knowledge and security-consciousness of the IT staff and the users is decisive for IT security. The staff and users must be given the information and education necessary for maintaining the IT security intended.

The IT Director is responsible for the production and updating of basic information and educational materials about IT security.

The operations manager is responsible for employees and students within her/his own unit receiving information and education on IT security.

The systems owners are responsible for the production of information and educational materials as well as the initiation of the supplying of information and education to users.

Users

Before being given access to the University's IT resources, each user shall attest that he or she has informed him- or herself of the University's *Regulations for the use of Umeå University's IT resources.*

The Regulations shall include:

- conditions for the use of the IT resources.
- users' liability and obligations.
- current regulations for the use of the IT resources.

Systems administrator

By systems administrator is meant the person having a higher degree of authorisation than ordinary users in the IT systems and communications network. The Systems administrator is normally responsible for the running and security, or has a position as assistant in the running and management of IT systems and networks.

The Systems administrator is appointed and assigned her or his rights and obligations via a written order by the Director of operations. In this order, it shall be stated which systems or equivalent are designated by the rights.

Everyone who is active as a systems operator at the University must have signed a special liability agreement. This liability agreement must include:

- reference to the information in the regulations for users.
- information on the responsibility and obligations of systems administrators.
- information on current regulations for the operation and management of the networks and IT systems.
- information on regulations and routines for measures in the case of incidents.

Operation

The person responsible for the operation of the communications networks or IT systems shall normally also be assigned the responsibility for IT security in operation and also supervise the accessibility of competent staff to the extent necessary so that the intended degree of IT security can be maintained.

Planning in case of disruption

The persons responsible for IT security for:

- central IT resources,
- IT systems of major significance for education or research,
- IT systems of major economic significance for the University,
- IT systems of significance for security in general at the University,

shall carry out planning for systems or resources in case of disruption.

Procurement and development

When carrying out procurement and development of IT systems and IT services, the demands of security must always be observed. The demand for IT security shall be included in the specifications and the contract.

Outsourcing

When a third party carries out assignments for the University in which IT services or IT systems constitute an important part, the University shall ensure in the contract that the third party maintains an IT security that meets the demands of the University.