GÖTEBORGS UNIVERSITET

June 2012

1 Regulations for the use of the University of Gothenburg's IT facilities

1.1 General

The University of Gothenburg's (GU's) IT facilities are owned by the University and are intended to be used in and for the University's function of providing education, research and administration in that connection, and also for cooperation with the surrounding society. The facilities may not be utilized for purposes through which the University's name, prestige and good reputation can be harmed.

IT facilities refer to computers, mobile phones, tablets, software, software licenses, communications network and all other peripheral equipment that is used in connection with communication and handling information in digital form.

1.2 Regulations for the use

1.2.1 Restrictions on the use of the University's IT facilities

The University's IT facilities may not be used to inappropriately or unethically distribute, store or convey information that

- contravenes applicable legislation, e.g. incitement to racial hatred, child pornography, illegal depiction of violent acts, slander, molestation, unauthorised access to computer systems or infringement of copyright
- without any connection with the users role at GU, can be regarded as political, ideological or religious propaganda
- contravenes the Personal Data Act's provisions on individual's personal integrity
- is personally insulting or offensive
- is intended to market products or services unconnected to the University
- contravenes agreements concerning IT facilities made by GU
- or in any other way disrupts GU's IT operation

Private use of the University's IT facilities is only permitted to a limited extent.

1.2.2 Responsibilities and authorisations

Before users are given access rights to GU's IT facilities, they must be informed of the current regulations for use and sign the "Agreement of responsible use of GU's IT facilities" or in some other way confirm that they are aware of the regulations.

It must always be possible to trace the identity of the user therefore it is not permitted to use someone else's authorisation or exploit faulty configurations, program errors or in any other way manipulate the IT facilities.

The authorisation allocated is time-limited and is linked to studies, employment, and participation in a project or commission. Users must themselves report circumstances that lead to cancellation of their access rights.

1.3 Regulations for the use of Internet and e-mail

1.3.1 General

GUNET/SUNET are fast networks and a computer connected to them is therefore constantly exposed to attempts to gain unauthorised access (hacking). Information that is sent or made accessible via the Internet can also be accessible by unauthorised persons. It is the responsibility of each user to protect GU's IT facilities against infringement and information against access by unauthorised persons.

Consequently,

- computers and computer systems must always be protected by a safely constructed password, see point 1.5, or other technical authorisation- and user identification
- computers owned/ leased by GU must have antivirus programs licensed by GU and other security systems recommended by GU installed. Definitions must be updated
- other computers connected to GU's IT facilities must have equivalent security systems installed in order to attain sufficient protection. Definitions must be updated
- all attached documents/files must be tested for viruses before they are opened or downloaded onto the user's computer
- the user must never download programs and files onto a computer that is connected to GU's IT facilities without analysing the security risk
- all attempts to gain unauthorised access to computer systems must be reported to the University IT-support or IT-support for students
- information meriting protection that is sent using e-mail or that is made accessible via the Internet must be protected on the basis of the result of the information classification carried out

If unsure regarding application of the above regulations contact University IT-support or IT-support for students.

1.3.2 Use of the Internet

It is forbidden to by GU computer or a computer of one's own use GU's IT-facilities to unlawfully download material protected by copyright without permission from the rights holder.

GU's web policy must be followed when publishing material on the web. If in doubt regarding publication of personal details contact GU's personal data representative before publication.

An employee, that within the scope of his employment, uses a social media or cloud service must, before usage, take up a definite position to risks in proportion to the information/ material, that can be connected to the usage of the media or service. That means e.g copyright, personal integrity and the content of the user agreement or other contract.

1.3.3 E-mail

All e-mails sent from addresses within GU represent the University. E-mails must contain correct information about the sender's name and address.

Before sending an e-mail the address must be checked carefully in order to ensure that the e-mail reaches the correct addressee.

1.3.4 E-mails handled by GU staff

E-mails are covered by the regulations for public documents. Registration of public documents, in the form of e-mails, must therefore take place according to the same regulations as ordinary paper documents.

It is the responsibility of every employee that incoming e-mail is handled and to ensure that in their absence it is received and if necessary dealt with.

All e-mails received and sent to/from GU must go via GU's e-mail servers. Employees who need to handle e-mail for the University when not directly connected to GU's IT facilities must gain access to GU's own web services or another connection approved by the technical officer. Automatic forwarding to external addresses of e-mail addressed to GU is not permitted. E-mail sent to GU must also be answered from a GU address.

1.4 Regulations for employees´ remote access in relation to GU's IT facilities

1.4.1 General

In order to maintain good security when using remote access, requirements are in place to ensure a high level of security throughout the communication process from user, equipment and program up to the IT service used.

To access some IT services users must themselves ascertain which regulations and instructions that the system owner and technical officer have put in place for the IT services and IT systems in question.

1.4.2 Remote access from a private computer

In order to maintain a high level of security even when working from a private computer connected to one of GU's IT facilities, the computer must have at least an equivalent level of security as computers owned by GU. The private computer equipment must have

- individual passwords, se point 1.5 below
- up-to-date anti virus software
- securely updated software

- connection approved by GU

For broadband connection additional protection against unauthorised access must be in place through the installation of a so-called firewall.

1.5 Regulations for passwords

The University's IT systems and each user must be protected by password and/or other technical authorisation- and user identification.

In order to make protection derived from a password function effectively, the following criteria must be met.

- User identity, password and authorisation allocated must be personal.
- Passwords must be kept secret and not lent to anyone else.
- A password must consist of at least 8 characters in a mixture of upper and lower case letters, numbers and a special character. It must not be related to personal details such as name or date of birth, consist of simple words or similar and nor must it consist of keys that are in groups.
- The password must be changed every 6th month or as soon as it becomes known to an outsider.
- The function to automatically lock the screen (power saving mode) after max. 10 minutes inactivity must always be switched on. Resumption of work at a work station consequently entails it being unlocked by means of a password.
- The user must always log out from the computer when leaving the computer without the user's supervision.

1.6 Consequences and actions when the regulations are violated

Any violations of these regulations can result in the user being completely or partially suspended from using the University's IT facilities. The decision is taken by the person responsible for the area in question.

In serious cases the technical officer may close down a mismanaged or misused IT facility with immediate effect.

Any violation of these regulations will be reported by the Head of Department/equivalent to

- the Vice-Chancellor, in the case of students. The Vice-Chancellor will decide if the matter is to be referred to a disciplinary committee. The disciplinary consequences entail a warning or temporary suspension from teaching and other activities at the University.
- the staff disciplinary committee in the case of employees. The consequences may be disciplinary responsibility or suspension.

Suspicion of crime can result in the police being notified.