



Model Acceptable Use Policy for students

English translation of "Model Acceptable Use Policy voor studenten"

Author(s): Corporation between SURFibo en SURFnet

Version: 4.0




Date: 16 April 2013

SURFibo ("SURF Informatie Beveiligers Overleg") is a community of Practice of Information Security Officers, founded by the Platform ICT and Organization of SURF. SURFibo's mission is to give guidance to and actively stimulate information security within Higher Education in the Netherlands (universities, institutes for higher vocational education, and academic hospitals). SURFibo publishes guidelines and templates for direct use within the constituency and promotes corporation and exchange of best practices between associated Information Security Officers.

Version management:

Versie	Datum	Korte beschrijving aanpassingen
1.0	November 2005	First version
2.0	Augustus 2011	Adaptations regarding BYOD
3.0	November 2012	Complete revision to comply with new legislation as of May 2012: <ul style="list-style-type: none"> - Separate model-AUP's for students and employees - AUP's available in English - Separate guideline documents
4.0	April 2013	Update to safeguard basic principles Confidentiality, Privacy and (Intellectual) Property in new applications like Cloudcomputing and BYOD

Composed by:

Organisatie		Toelichting
ICTrecht		Arnoud Engelfriet, legal advice final editing version 3.0 www.ictrecht.nl
SURFnet		Rogier Spoor, coordination Evelijn Jeunink, legal advice www.surfnet.nl
SURFibo	SURF Informatie Beveiligers Overleg	Bart van den Heuvel, coordination Special thanks to members of the SURFibo Community of Practice for their contribution in workshops en as reviewers www.surfibo.nl
SCIRT		Special thanks to members of SCIRT Community of Practice for their contribution in workshops en as reviewers www.surfnet.nl/nl/Thema/beveiliging/scirt/Pages/scirt.aspx

Acknowledgement:

The Acceptable Use Policies for employees and students of <NAME_INSTITUTION> are based on model AUP's for Higher Education, a collaborative effort of SURFnet and SURFibo.



This publication is licensed under Creative Commons Attribution 3.0 Netherlands license.
www.creativecommons.org/licenses/by/3.0/nl/deed.en



Acceptable Use Policy for students studying at <NAME_INSTITUTION>

The <NAME_INSTITUTION> (hereinafter referred to as: the Institution) offers its own students and visiting students the opportunity to use the Internet for study purposes. An institution-related mailbox [and options for storing files and personal study information] will also be made available for personal use by students for study purposes.

Rules are attached to the use of these facilities to ensure the smooth course of events in the buildings and on the Institution's grounds.

Use of the facilities

Computer and network facilities (such as public computers, wireless and wired network connections, e-mail and Internet access, storage capacity, printers and electronic learning environments) will be made available to the student for the purpose of study to enable the student to carry out assignments, prepare reports and theses, keep a record of study progress, consult sources of reference and communicate with lecturers and fellow students, among other things.

Students may use their own equipment and applications on the Institution's facilities provided such use is in accordance with the rules set out in these Regulations. Changing the settings of equipment and applications made available by the Institution is only permitted with the separate consent of systems management. Connecting students' own network equipment for the purpose of sharing the connection with third parties on wired or wireless network connections is prohibited at all times[, except in student living accommodation].

[OPTIONAL EDUROAM] These Regulations also apply to guest access at other institutions, making use of credentials of one's own Institution (Eduroam).

Certain facilities will only be accessible with the aid of a username and [password|means of authentication, such as a smartcard or GSM]. These are person-related and are not permitted to be shared with other persons. Systems management may impose additional requirements on the quality of passwords and other security aspects[, as detailed in the Information Security Policy]. In the event of suspected misuse of a password [or means of authentication], systems management may block access to the relevant account with immediate effect.

Intellectual property and confidential information

The student will not infringe on intellectual property rights of the Institution or third parties and will respect applicable Licence agreements.

[Property rights on information from the Institution will be solely controlled by the Institution. The student will only be eligible for property rights on such information if those rights are explicitly granted by the Institution]

[Students are not permitted to download huge volumes of articles from the files in the digital library or systematically duplicate substantial sections of the files or databases in the digital library.]

If the student gets access to confidential or privacy sensitive information in order to fulfill assignments for the Institution, the student is obliged to maintain confidentiality of this information at any time.

The student will pay special attention to implementing security measures as stated in this document if an assignment makes it necessary to transfer confidential information outside the control of the Institution, for example through sending it by e-mail or storing it on non-Institutional Cloud-services, external media or student owned devices (USB devices, Tablets, etc.)

If the Institution has issued specific instructions to safeguard confidentiality and the protection of intellectual property, the student is obliged to adhere to these instructions strictly.

Security policy for the Institution and the student

The Institution takes information security seriously. The Institution therefore maintains a stringent security policy and takes proper technical and organisational measures to protect the infrastructure against loss, theft, criminal activities, loss of confidentiality, privacy breaches and infringements on intellectual property rights.

It obviously is impossible to ensure one hundred per cent security. For this reason the Institution expects students to adopt a proactive approach and take serious measures to secure their own computer and other equipment, such as smartphones or tablets, properly. Students are at all times personally responsible for the use of their own equipment and for the data stored on the equipment.

[If students use their own equipment on the Institution's facilities, they should ensure the following security measures in particular:

- their equipment features an effective virus scanner and firewall;
- they should regularly make back-ups of all relevant data and store copies of Institution data securely;
- use passwords that are difficult to decipher and change these on a regular basis;
- keep the software settings on their equipment up-to-date;
- <ETC.>]

[Systems management will publish a list of security measures that will be updated regularly. Students must strictly comply with these measures.]

Personal use and disturbance

Limited personal use of the facilities is permitted. Use, whether personal or for study purposes, must not disturb good order in the Institution and must not cause disturbance to others, cause an infringement on the rights of the Institution or others, nor be detrimental to the integrity and security of the network.

Use causing interference and/or disturbance is always taken to mean the following:

- consulting Internet services that have a pornographic, racist, discriminatory, insulting or offensive content in public spaces or sending messages with such content;
- sending harassing/sexually harassing messages or messages that incite or could incite discrimination, hatred and/or violence;
- sending unsolicited messages to vast numbers of recipients, sending chain letters or sending malware, such as viruses, worms, Trojan horses and spyware.
- [using file sharing or streaming services (such as Internet radio or *TV-on-demand*) if the volume of data traffic imposes a threat to the integrity and safety of the computer or network facilities;]
- [downloading films, music, software and other copyright-protected material from any illegal source or if the student actually knows that this violates copyrights;]
- [distributing or uploading films, music, software and other copyright-protected material to or for third parties without the consent of the owners.]

No restrictions will be imposed on use by students using an Institution network facility in their living accommodation, except where required to ensure the integrity and security of the network, or to limit the effects of network congestion. If the Institution intervenes in order to limit the effects of network congestion, the same types of traffic will be treated equally. The other provisions set out in this Acceptable Use Policy apply in full to student users using an Institution network facility in their living accommodation.

Use of the computer and network facilities for the purpose of performing commercial activities is solely permitted if and to the extent the Institution has provided written consent to do so.

Monitoring by the Institution

Monitoring the use of facilities will only be carried to enforce the rules set out in these Regulations for the purpose of ensuring good order at the Institution and to monitor the integrity and security of the Institution's network and computer facilities. Use of the facilities for purposes designated as prohibited will be rendered impossible by means of technical solutions as far as possible.

To monitor compliance with the rules, information will be collected on a computerised basis (logged). Only the systems managers in charge will have access to the information, which will only be made available to the other systems managers and officers in charge in an anonymised format. They may decide to take further technical measures, such as blocking access to a certain service or limiting the options on the relevant equipment in order to use the network.

Switching off the network access options is a special measure that may be taken in the event of disturbance caused by students' own equipment. The student will receive an advance warning, if possible, offering him or her the opportunity to stop causing disturbance. If it is not possible to warn the student in advance of taking the measure due to the required urgency, the student will be notified of the measure as soon as possible.

If there is reason to believe that the rules have been violated, monitoring may be performed at the level of individual traffic data relating to use of the facilities. Only if there are important reasons for doing so will the content be checked.

When performing a check at the level of traffic data or content, the Institution will fully abide by the Data Protection Act and other relevant laws and regulations. The Institution will specifically protect the data recorded during the check against unauthorised access while persons having access to the data will be bound by contract to maintain confidentiality thereof.

Procedure for specific investigations

A specific investigation applies if the traffic data or other personal data concerning a specific student is recorded as part of an investigation based on a strong suspicion that the relevant student has breached these Regulations.

A specific investigation will be conducted only after the director of the relevant faculty has commissioned the investigation in writing, consent for which will be granted stating reasons. The Executive Board will receive a copy of the order commissioning the investigation and a document containing the results of the investigation.

A specific investigation will initially be limited to traffic data relating to use of the facilities. If further evidence comes to light as a result of the specific investigation, after having obtained separate consent the Institution may subsequently examine the content of the communication or saved files. If no further measures are required as a result of the investigation, the document will be destroyed.

Contrary to the above, a specific investigation into the security or integrity of peripheral equipment is permitted to be conducted by systems management on the basis of concrete evidence, without requiring separate consent. The results of the investigation will only be shared with the student for the purpose of improving the security or integrity of the peripheral equipment. In the event of recurrence, the procedure set out in the previous paragraph will be followed.

The student will be informed by the director in writing of the reason for conducting the investigation, the procedure and the results as soon as possible. The student will be given the opportunity to explain the findings. Informing the student may only be postponed if this would actually be detrimental to the investigation.

Systems managers will only provide access to student accounts or computers if the student has given consent to do so. Access without the student's consent is only permitted in urgent cases or if there is a clear suspicion that these Regulations have been violated, as detailed in this Article. In such case the student will be informed at a later stage.

Student privacy rights

The student may request the Board for a complete overview of his or her personal data as processed by the Institution for the purpose of these Regulations. A request of this nature will be complied with within four weeks.

The student may request the Board to improve, add to, remove or protect his or her personal data if they are factually incorrect, incomplete for the purpose in mind or irrelevant, or conflict with statutory provisions. A request of this nature will be complied with within four weeks. A refusal will be accompanied by reasons. A request that has been granted will be carried out as soon as possible.

The student may also lodge an objection against the processing of his or her personal data on the grounds of serious personal circumstances. The Board will decide whether the objection is justified within four weeks of receipt. If the Board deems the objection justified, it will stop processing the data with immediate effect.

Consequences of violation

The Board may take disciplinary measures in the event a student acts in contravention of these Regulations or the prevailing statutory regulations, depending on the nature and seriousness of the violation.

[OPTION A: separate measures]. This includes a warning, reprimand, temporarily blocking or limiting the facilities (for a maximum period of one year) and in extreme cases termination of the student's enrolment.

[OPTION B: reference], as set out in detail in the Institution's Disciplinary Measures Regulations.

[COMPULSORY for A or B] Disciplinary measures, except for a warning, may not be taken solely on the basis of computerised processing of personal data, such as a finding generated by an automatic filter or block. In addition, no disciplinary measures will be taken without giving the student the opportunity to state his or her views.

Contrary to the above, it is possible for the Institution to temporarily block the relevant facility in the event disturbance is detected by the computer or otherwise. The block will be maintained for a maximum period of one week or shorter if the cause has been removed to the satisfaction of systems management. If systems management establishes after one week that no improvement has been made, systems management may decide to prolong the block. Disciplinary measures may be taken in the event of recurrence of the cause.

Concluding provisions

These regulations may be amended by the Board. Amendments will only be implemented at the start of the academic year, except in urgent cases or if external circumstances dictate that the Institution should do so earlier.

Amendments will only be implemented after a prior opinion has been sought from the Institution's representative advisory body. The Board will consider student feedback before implementing the amendments.

In cases not provided for by these Regulations, the Executive Board will decide.