



Model Acceptable Use Policy for employees

English translation of "Model Acceptable Use Policy voor medewerkers"

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.



Acceptable Use Policy for employees of <NAME_INSTITUTION>

Model Regulations governing the use of ICT facilities and the Internet for the employees of SURF member institutions

This document serves as a model for drawing up regulations governing the use of ICT facilities and the Internet by employees working at institutions who are members of SURFnet.

Basis for the regulations

Many of the institution's employees need to use ICT facilities and the Internet to enable them to perform their work properly. However, there are risks involved in using ICT facilities and the Internet and this has created the need to establish rules of conduct. Against the background of these risks employees are expected to use ICT facilities and the Internet in a responsible manner.

In issuing these Regulations the institution, <NAME>, <DETAILS>, hereinafter to be referred to as the 'Institution', aims to set out rules concerning the required use of these operating assets. In doing so, the Institution seeks to ensure a proper balance between the responsible and safe use of ICT facilities and the Internet, and protection of the employee's privacy.

[IF using social media] The importance of using social media, such as Facebook, LinkedIn and Twitter, is growing but these media may also have repercussions for the Institution. For this reason the Institution also wishes to impose specific rules on the use of social media.

As an employer the Institution is entitled to stipulate rules relating to the performance of work and good order in the workplace, as provided for in legislation. In addition to legislation, these Regulations are also based on Article [123] of the Collective Labour Agreement [TITEL] [and on Article [123] of the Institution's Statute].

Given that the Regulations provide for the processing of personal data and/or the monitoring of employee conduct or performance, the Regulations are subject to the approval of the representative advisory body. The representative advisory body approved the contents of these Regulations on [DATE].

Article 1. Principles

1.1. The Regulations set out rules governing employee use of the operating assets ICT facilities and the Internet. The purpose of these rules is to provide for good order in respect of the following:

- systems and network security, including protection against damage or loss and misuse;
- preventing sexual harassment, discrimination and other offences;
- protecting privacy-sensitive information and personal data of the Institution and its employees, as well as that of students and their parents

- protecting the confidential information of the Institution and its employees, as well as that of students and their parents;
 - protecting the intellectual property rights of the Institution and third parties, including adherence to applicable license agreements;
 - preventing negative publicity;
 - controlling costs and capacity.
- 1.2. [OPTION - BROAD] Limited use of the Internet and ICT facilities for personal purposes is permitted, provided this does not interfere with day-to-day activities or the Institution's network.
- [OPTION - NARROW] Limited use of the Internet and ICT facilities for personal purposes is only permitted during breaks and/or to the extent such use is not detrimental to the performance of work.
- [OPTION – VERY STRINGENT] Use of the Internet and ICT facilities for personal purposes should be avoided as much as possible.
- [OPTIONAL for all of the above] Use of the Internet and ICT facilities for ancillary activities is prohibited at all times unless separate written consent has been obtained.
- 1.3. These Regulations apply to all those working for the Institution, including agency and temporary staff. These Regulations do not apply to students/guest students; separate Student Regulations have been drawn up for the latter. [OPTIONAL – VISTORS: These Regulations also apply to those visiting the Institution at the invitation of employees.]
- 1.4. [OPTIONAL EDUROAM] These Regulations also apply to guest access at other institutions, making use of credentials of one's own Institution (Eduroam).
- 1.5. In enforcing these Regulations, the Institution seeks to provide measures that keep access to privacy-sensitive information or personal employee data to a minimum. Where possible, information will only be monitored or filtered by the Institution on a computerised basis without the Institution providing itself or other persons access to the conduct of individuals.

Article 2. Intellectual property and confidential information

- 2.1. The employee is required to treat confidential information, privacy-sensitive information and personal data to which he or she has access at work as strictly confidential and take appropriate measures to safeguard confidentiality.
- 2.2. The employee respects the intellectual property rights of the Institution and third parties as well as applicable license agreements.

- 2.3. [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.]
- 2.4. [The employee is 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.]
- 2.5. The employee will pay special attention to implementing security measures as stated in this document if work related activities make 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 employee is obliged to adhere to these instructions strictly.
- 2.6 This applies in particular to systems managers in respect of the special nature of their position. If they breach the duty of confidentiality, this will be deemed a gross dereliction of duty.

Article 3. Using computer and network facilities

- 3.1. Computer and network facilities are made available to the employee for work purposes. Consequently, use thereof relates to performance of the duties associated with the employee's job. Personal use of these facilities is only permitted as set out in Article 1.2
- 3.2. The employee is required to treat the login information he or she has been provided with due care at all times as well as any additional means of authentication, such as smartcards and tokens). Person-related passwords and additional means of authentication are not permitted to be shared. In the event of suspected misuse of a password, systems management may block access to the relevant account with immediate effect.
- 3.3. [The Institution may specify systems or applications for educational and other business purposes, such as an Electronic Learning Environment, an e-mail system, (mobile) applications (Apps), Cloud services or multimedia services. When sharing course material or conducting research the employee will use these systems only and will strictly comply with the restrictions and requirements imposed.]
- 3.4. Installing software on the organisation's computer and network facilities is not permitted without the separate consent of systems management. Connecting servers and active network components, such as access points and routers, is not permitted without the consent of systems management.
[IF BYOD does not apply] Connecting own client equipment, such as laptops, tablets and telephones, is not permitted without the separate consent of systems management. Systems management may attach rules to consent, such as the requirement to install virus scanners and password protection.

- [IF BYOD applies] Connecting own client equipment, such as laptops, tablets and telephones, is only permitted on the network/wireless network connections made available for that purpose. Systems management may attach rules to access to these connections, such as the requirement to install virus scanners and password protection.
- 3.5. [IF personal use applies – not stringent] Storing personal files or information on the Institution's systems is permitted provided this does not overload the storage space on these systems or disrupt good order in the workplace. However, the Institution is not obliged to produce back-up copies of such files or information or make available copies should the relevant systems be replaced or undergo repair.
- 3.6. Use of the computer and network facilities by the employee for the purpose of ancillary activities is solely permitted if and to the extent the Institution has provided written consent to do so.

Article 4. Use of e-mail and other ICT means of communication

- 4.1. The e-mail system, the corresponding mailbox and e-mail address are made available to the employee for work purposes. Consequently, use thereof relates to performance of the duties associated with the employee's job.
- 4.2. Personal use of these tools is only permitted as provided in Article 1.2
- 4.3. Use of ICT means of communication, whether personal or work-related, for the following purposes is prohibited:
- sending messages containing pornographic, racist, discriminatory, intimidating, insulting or offensive content;
 - sending messages containing sexual harassment content;
 - sending 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, Trojan horses or spyware.
- 4.4. [IF including personal use – stringent] The employee will not use the e-mail address provided by the Institution for personal messages, and will observe the limits set out in Article 1.2. The organisation will not block access to or specifically monitor other e-mail services.
- [IF including personal use – not stringent] The employee will preferably not use the e-mail address provided by the Institution for personal messages, and will observe the limits set out in Article 1.2. The organisation will not block access to or specifically monitor other e-mail services.
- 4.5. In the event of illness, unforeseen prolonged absence or gross negligence on the part of the employee, the Institution has the right to give the employee's replacement or supervisor access to the employees' files or mailbox, but only if business interests form a compelling reason for doing so [OPTION A, but only

after separate consent has been obtained from one of the employee's superiors/OPTION B: but only if it can be proven that it is impossible to obtain the employee's consent, or that the business interests are so substantial that they outweigh the need for consent.]. However, the latter is not permitted to access files marked personal, personal e-mail messages recognisable as such, or e-mail messages that have been sent to or from a [confidential adviser / company doctor / HR consultant]. If the employee has not marked files or e-mail messages as personal, the Institution may check the relevant information pertaining to the employee by engaging a confidential adviser to identify personal information and place it in a separate location prior to providing access to the employee's replacement or supervisor.

- 4.6. E-mail correspondence between members of the representative advisory body, from company doctors, HR consultants and all persons who may invoke statutory privilege will not be checked. This does not apply to computerised security control of e-mail traffic and the network.

Article 5. Internet use

- 5.1. The employee is given access to the Internet and the corresponding facilities for work purposes. Consequently, use thereof relates to performance of the duties associated with the employee's job.
- 5.2. Personal use of these facilities is only permitted as set out in Article 1.2
- 5.3. However, each time the employee uses the Internet, whether for personal or work-related purposes, the following is prohibited:
- visiting websites containing pornographic, racist, discriminatory, insulting or offensive material;
 - 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 employee 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.

Article 6. [IF using social media] Use of social media

- 6.1. [IF opting for stringent] The use of social media, such as Hyves, Facebook, Youtube, MSN, Skype, Omegle, Twitter or LinkedIn, for matters affecting the employee's performance or position as an employee of the Institution is only permitted with separate consent from the Institution.
- 6.2. [If opting for stringent]. The Institution may in such case stipulate specific rules concerning the manner of presentation or communication. If use concerns sharing knowledge with colleagues working in the professional field, the employee will in principle only state his or her name and job role. If it is

deemed desirable to state the organisation's name, the employee will state that he or she has done so in a personal capacity.

- 6.3. [IF taking a liberal stance] The Institution is supportive of the employee conducting open dialogue, sharing ideas and knowledge with colleagues in the professional field and third parties using social media, such as Hyves, Facebook, Youtube, MSN, Skype, Omegle, Twitter or LinkedIn).

[OPTION A] If the topics are work-related, employees must ensure that the profile and content reflects the professional image they would project textually and audiovisually to colleagues in the professional field and students.

[OPTION B] If the topics are work-related, the employee must always state the name of the Institution and his or her job role, and include a disclaimer stating that it is the employee's personal view, which does not necessarily reflect that of the Institution. The employee is nonetheless obliged to demonstrate good behaviour.

- 6.4. [IF desired] The employee will not add students as 'friends' or contacts on the social media referred to above, unless he or she maintains a separate profile for that purpose which is clearly linked to the Institution and on which the Institution may impose requirements on the manner of presentation, content and performance.
- 6.5. Board members, managers, supervisors and other persons responsible for promulgating policy or strategy have specific responsibility for the use of social media, even if the content is not directly related to their work. On the grounds of their position they should consider whether they should publish information in a personal capacity. They are fully aware that employees read what they write.
- 6.6. This article also applies if employees participate in social media using personal computers or Internet connections, but only in cases where their participation may affect their work.
- 6.7. If an employee creates a social media account relating directly to their work but in the employee's name, the employee and the Institution will seek an appropriate solution for transferring the employee's profile or the information or contacts contained in the profile on termination of employment.

Article 7. Monitoring and control

- 7.1. Monitoring the use of ICT facilities and the Internet will only be carried out for the purpose of enforcing the rules set out in these Regulations for the purposes referred to in Article 1. Use of the operating assets for purposes designated as prohibited will be rendered impossible by means of technical solutions as far as possible.
- 7.2. 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.

- 7.3. 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 e-mail and Internet use. Only if there are important reasons for doing so will the content be checked.
- 7.4. When performing a check at the level of traffic data or personal data 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.
- 7.5. The Institution may take specific monitoring measures, such as:
 - Monitoring to prevent negative publicity and sexual harassment, and as required for the purpose of system and network security will be carried out on the basis of filtering the content using key words. Suspect messages will automatically be returned to the sender.
 - Monitoring for cost and capacity control purposes will be restricted to checking the sources of the costs or the required capacity (such as the addresses of Internet radio stations and video sites) on the basis of traffic data. If significant costs are incurred by these websites or if they create considerable disturbance, they will be blocked or removed, without breaching the confidentiality of the communication content.
 - Monitoring the use of images will be carried out on the basis of third-party complaints or reports, or at random in the case of publicly accessible images.

Article 8. Procedure for specific investigations

- 8.1. A specific investigation applies if the traffic data or other personal data concerning a specific employee is recorded as part of an investigation based on a strong suspicion that the relevant employee has breached these Regulations.
- 8.2. A specific investigation will be conducted only after the director of the relevant faculty has commissioned the investigation in writing. The Executive Board will receive a copy of the order commissioning the investigation and a document containing the results of the investigation. If no further measures are required as a result of the investigation, the document will be destroyed.
- 8.3. Contrary to the above paragraph, a specific investigation will be conducted into the security or integrity of peripheral equipment by the systems manager on the basis of concrete evidence. No separate consent is required from the body referred to in paragraph 2. The results of the investigation will only be shared with the employee for the purpose of improving the security or integrity of the peripheral equipment. In the event of recurrence, the procedure set out in paragraph 2 will be followed.
- 8.4. 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,

the Institution may subsequently examine the content of the communication or saved files. This requires written consent from the Executive Board, which consent will state why it was granted. [OPTION: The Institution will make every effort to maintain confidentiality of the identity of the persons examining the information, a record of which will be made in the name of the director.]

- 8.5. The Institution may take specific person-related monitoring measures, such as:
 - Monitoring the leakage of confidential information on the basis of random checks on keywords. Suspect messages will be singled out for further investigation in consultation with the Board.
 - Monitoring violation of the prohibition set out in Article 4 (3) by allowing two people to open e-mail messages and view the contents on the basis of complaints or random checks. These two people are bound to maintain confidentiality of the contents.
- 8.6. The employee 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 employee will be given the opportunity to explain the findings. Informing the employee may only be postponed if this would actually be detrimental to the investigation.
- 8.7. Systems managers will only provide access to employee accounts or computers if the employee has given consent to do so. Access without the employee'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 employee will be informed at a later stage.

Article 9. Employee's privacy rights

- 9.1. The employee 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.
- 9.2. The employee 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.
- 9.3. The employee 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.
- 9.4. The Board will not give the employee any instructions or orders concerning privacy-sensitive information and personal data conflicting with these Regulations.

Article 10. Consequences of violation

- 10.1. [OPTION A: separate measures]. The Board may take disciplinary measures in the event an employee acts in contravention of these Regulations or the prevailing statutory regulations, depending on the nature and seriousness of the violation. This includes a warning, a reprimand, a transfer, suspension and termination of the employment contract. The Board may furthermore decide to restrict access to certain ICT facilities, temporarily or otherwise.
- [OPTION B: refer to prevailing measures]. The Board may take disciplinary measures as set out in the Institution's Disciplinary Measures Regulations in the event an employee acts in contravention of these Regulations or the prevailing statutory regulations, depending on the nature and seriousness of the violation.
- 10.2. [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 employee the opportunity to state his or her views.
- 10.3. [OPTION C: call to account but no disciplinary action]. If it has been established that employees have failed to comply with the Regulations, they will be called to account for their conduct by their supervisor as soon as possible. They will be given access to the information that has been recorded about them and will have the opportunity to respond to the findings. The employee and the supervisor will make agreements for the future and on possible disciplinary measures in the event the agreements are breached. These agreements may be more stringent than the provisions set out in these Regulations. Access to e-mail or the Internet may also be restricted or completely blocked.
- 10.4 [DEPENDING ON CHOSEN OPTION: Contrary to the above | In addition 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 until such time as the cause has been removed. Disciplinary measures may be taken in the event of recurrence of the cause.

Article 11. Final provisions

- 11.1. These Regulations will be evaluated each year by the Board [OPTION and other parties, such as the representative advisory body]. The next evaluation will take place in [MONTH, YEAR].
- 11.2. The organisation may amend these Regulations [IF applicable with the consent of the representative advisory body] if circumstances so dictate. The employees will be informed of any proposed amendments prior to implementation. The Board will consider employee feedback before implementing the amendments.
- 11.3. In cases not provided for by these Regulations, the Executive Board will decide.

