HSG IT User Regulations

of 1 March 2016

Pursuant to Art. 35(2) of the University Statutes of 25 October 2010[1]

the Senate Committee hereby issues

the following User Regulations:

Whereas

daily work in teaching, research, executive education and consultancy at the University of St.Gallen (HSG) is increasingly based on information and communication technologies (IT); the utilisation of the IT services provided by the department responsible for IT (hereinafter called IT Services) is subject to various general legal and organisational conditions, compliance with which is crucial for secure, stable and efficient IT operations at the HSG; the following HSG IT User Regulations summarise the relevant provisions, as follows:[2]

1 Authorisation of access to the systems

HSG members receive an HSG user name and a related password for access to the HSG's network (HSGnet) after enrolment (students) or on employment (employees).

At the request submitted to IT Services by the IT administrator of an organisational unit, guests can also be provided with an HSG user name. Their access to the HSG's IT systems may be limited in terms of content and/or time. Different HSG user names and passwords may be assigned for different services.

Authorisation of access to the HSGnet shall expire on exmatriculation (students), on the termination of the employment contract (employees), on the lapse of the reason for access (guests) or on expiry of the period of validity (authorisation limited in terms of time). Special provisions, for instance for professors emeriti/emeritæ, shall be reserved.

2 Hardware

2.1 HSG appliances

If an IT workstation is funded by the core university or an institute, IT Services shall make available the necessary HSG terminal devices (desktops, laptops, etc.). The terminal devices available at any given time shall be subject to the separate regulation in respect of IT workstations at the HSG.

---

[1] Consolidated Statute Book of the Canton of St.Gallen, No. 217.15.

[2] Supplementary and more detailed rules and directives in respect of the utilisation of IT services are filed in the HSG intranet.

Every member of staff shall be obliged to treat their appliances with care. Besides the avoidance of physical damage to appliances, due care shall also include compliance with the criteria relevant to security in accordance with Point 3.9 below.
After termination of the employment contract, HSG appliances shall be returned to IT Services.

2.2 Private appliances and IT infrastructure not operated by IT Services

External or internal access to the HSG's network by means of private terminal devices may jeopardise the proper operation of the network. Therefore particular attention shall be paid to such appliances always including an updated virus protection and running on an updated operating system.

IT Services advises members of staff of institutes and the Administration with regard to questions of virus protection and the updating of appliance operating systems. IT Services shall reserve the right to limit external access to critical resources of the HSG network by technical means.

The following points shall also have to be taken into consideration:

a. The operation of terminal devices capable of wireless communication (ICT devices) in the protected network areas shall basically be reserved to IT Services. The operation of a private ICT device in a protected network area can be requested from IT Services through the competent IT administrator.
b. External stationary network connections through channels other than those made available by IT Services shall be inadmissible.
c. The operation of WLAN access points within the entire HSG network shall be exclusively reserved for IT Services.
d. The operation of servers shall basically be reserved for IT Services. In justified exceptions, the operation of servers by organisational units of the HSG shall be exceptionally admissible. IT Services shall define the minimum requirements to be satisfied. Permission shall be granted against written evidence of the satisfaction of such minimum requirements by the Head of IT Services.
e. IT Services shall be authorised to disconnect servers and other ICT terminal devices from the network if the network is disrupted by their operation or if there is danger ahead.

2.3 Theft and loss

Insurance protection for a terminal device in the ownership of the HSG shall be guaranteed by the University. This insurance shall cover unexpected and sudden damage or destruction caused by external influences and theft. It shall not cover damage owing to warlike events, terrorism, etc. It shall not in any case cover mobile telephones and smartphones. Each claim in the event of damage shall be subject to an excess.

3 Data and information

3.1 Software

The software licensed by the HSG is centrally installed on the HSG's hardware. If users use software not licensed by the HSG, they shall have to obtain the requisite licence.

Private utilisation of the software shall be possible within the framework laid down in the relevant licensing provisions. Software that has been installed on a private appliance not made available by IT Services shall have to be permanently deleted from the appliance after exmatriculation or the termination of the employment contract unless further utilisation has been expressly permitted.

IT Services advises members of staff of the institutes and the Administration with regard to questions concerning software licensing.

3.2 Content and dissemination of information

Any contents, news and messages which are transmitted through the HSG's infrastructure or are stored on the HSG's IT systems must not violate any statutory provisions. Users shall have to comply with any supplementary precepts laid down by the HSG.

Particular attention shall have to be paid to restraints and prohibitions that arise from the Swiss Criminal Code (SR 311.0) and the provisions concerning data protection (particularly the Federal and Cantonal Data Protection Acts [SR 235.1 and Consolidated Statute Book of the Canton of St.Gallen, No. 142.1, respectively]) and the protection of the legal personality (particularly Art. 28, Swiss Civil Code, SR 210).

Users shall be responsible for any contents that they transmit and store. They shall satisfy any claims by any third parties that are based on any inappropriate use of the HSGnet themselves. If legal action should be taken against the University or the Canton of St.Gallen on account of such inappropriate use, they shall be entitled to have recourse to the user that has caused such action. They shall be entitled to take legal action against such user in accordance with the Civil Procedure Act.

3.3 Website

The HSG's website is divided up into a publicly accessible part (internet) and a part not accessible by the general public (intranet).

The graphic design of the websites of the HSG and its organisational units is in the responsibility of the Communication Department, which shall issue the necessary design precepts and recommendations. The responsibility for the content of the website is shared by the content officers designated by the HSG's organisational units.

Internal HSG information that is of a general nature and is aimed at a wider circle of users shall be disseminated exclusively through the intranet. In the HSG's intranet and internet pages, care shall be taken that no copyright is violated, for instance through the use of photos that are not licensed or not freely usable.

3.4 Social media

If the social media platforms officially used by the HSG are put to commercial use, the University's own precepts shall have to be complied with.

3.5 Mass e-mails

The term "mass mails" shall denote the dispatch of identically worded e-mails to an indeterminate internal and/or external circle of addressees. In this context, it shall be immaterial if such e-mails are dispatched in several batches or in their entirety.

Permission for the dispatch of mass e-mails shall have to be requested from the Legal Office, which shall take its bearings from the applicable anti-spam legislation.

3.6 Third-party rights

Users of the HSG's IT systems, particularly the web and cooperation platforms, shall take into consideration the rights of third parties, notably such rights as arise from the protection of the legal personality and from legislation concerning copyright and data protection.

Material protected by copyright must not be made available on the HSG's IT systems without the copyright holders' consent.

Within the scope of the applicable statutory provisions, users shall be entitled to copy any copyright-protected materials stored in the generally accessible areas of the HSG's IT systems (e.g. intranet, internet, cooperation platforms, etc.) for their own private use (cf. Arts. 19 and 20 of the Copyright Act, SR 231.1). Any further dissemination, even on a non-commercial basis, shall be subject to the copyright holders' consent. If there are any utilisation and licence provisions, they shall have to be complied with in any case.

3.7 Modification of information

The departments responsible for communication, student affairs and human resources, as well as IT Services, shall ensure a minimum degree of order in such areas as are accessible to all users (particularly intranet, internet and official social media channels). They are entitled to modify any published contents with the authors' consent or to delete such contents – irrespective of whether they satisfy content requirements pursuant to Point 3.2 or not. In particular, this also concerns storage locations intended for data exchange on which data are deleted after a certain period of time without any further enquiry.

3.8 Data storage

Business data and non-public research data shall be stored on the HSG's central systems[3] as a matter of principle unless otherwise specified by agreement. This guarantees the availability and security of the data. Users shall take care to ensure that data are stored in locations with appropriately defined access rights. This shall be applicable to confidential and secret data, in particular.

If business data have to be temporarily stored on local appliances, users shall ensure appropriate data security, for instance by means of encryption or backup copies. Members of staff are themselves responsible for the backup of local data. IT Services advise HSG members of staff with regard to questions concerning the backup of local data.

[3] These systems also include the online storage facilities in Switzerland made available by the provider of the Swiss universities, SWITCH.

Data storage in the public cloud shall not be a substitute for data storage on the HSG's central IT systems. The use of public cloud storage facilities shall only be admissible as long as the HSG's precepts are complied with. Confidential and secret business data must not be stored in the cloud under any circumstances.

Examples of secret data (not exhaustive):

a. Specially protected personal data (religious, ideological and political views and activities; health, privacy and race; proceedings and measures of social security; proceedings and sanctions under criminal law and of a disciplinary nature).
b. Personality profiles (compilation of data allowing for an assessment of the personality of a private individual).
c. Data which if abused place a person at a substantial disadvantage.
d. Data which have to be kept secret on account of contractual agreements or statutory provisions.

Examples of confidential data (not exhaustive):

a. Personal data (information referring to a certain or identifiable person, for instance credit card number or dates of birth).
b. Data which if abused place a person at a disadvantage.
c. Data of financial relevance.
d. Data that need to be archived.

If any business data should not be required any longer, they shall be offered to the University Archive prior to deletion. The University Archive shall assess their archival value and ensure the long-term archiving of such data.

3.9 Security

For HSG appliances, IT Services provide and maintain an updated virus protection. Virus protection for private appliances shall be incumbent on users (cf. also Point 2.2).

The backup of business data stored on both HSG appliances and personal appliances shall be incumbent on users. When HSG data are stored on private appliances, it is imperative that the latter be provided with a PIN or with password protection. IT Services makes available centrally managed storage facilities in the form of network drives and cooperation platforms for this purpose. Any data stored there are backed up regularly and can be restored if need be.

User names and passwords (hereinafter called access data) shall have to be changed regularly and must not be passed on to any third parties. Users shall take suitable measures to ensure that their access data cannot be used by other persons or systems. When users leave their IT workstation, they shall lock their desktops or notebooks. Computers that are connected to the non-public network shall have to be equipped with an activated password-protected screen saver. If users are absent for lengthy periods of time, office premises with IT facilities shall have to be locked in the evenings.

Users shall undertake and warrant that they will exercise due care when working with IT facilities and that they will refrain from carrying out any actions or manipulations that might disrupt other users or compromise the operation or security of the IT systems of the HSG or external systems. The utilisation of tools and methods for unauthorised and abusive penetration into IT systems is prohibited.

3.10 Data protection in general

General information about data protection on the HSG's website is available at http://www.unisg.ch/datenschutz. Details about data protection inside the HSGnet in the technical work with data, the so-called logfiles, can be found in Appendix B of this document.

3.11 Privacy clause in the AAI context

The SWITCH-AAI service[4] provides participating institutions with mutual access to digital resources. To be able to use these resources, it is necessary to process selected personal data such as names, e-mail addresses, institution of origin and organisational affiliation.

The users of the HSG's IT systems agree with the data processing required in the AAI context. In particular, this consent also includes the use of cookies, as well as the digital exchange, buffering and storage of person-related authorisation attributes. The users' consent to the digital exchange of these authorisation attributes is translated into practice by technical means.

4 Purpose of use

The HSG's IT infrastructure is basically made available for the purposes of studying, teaching, research, executive education and administration. Any commercial utilisation outside employment by the HSG shall be prohibited. Private utilisation shall be admissible but shall have to be limited to a minimum.

Any improper use of IT facilities shall not be tolerated. In general, any utilisation of the HSG's IT systems shall be deemed improper if it

- contravenes applicable law,
- violates these user guidelines or
- violates any third party's rights.

Specific improper actions in the IT context include, in particular:

a. the use of contents that are pornographic, glorify violence or are racist in accordance with the Swiss Criminal Code (SR 311.0)
   (exception: research projects with prior consent by the superior or the dean; for students, the contact point is the faculty member in charge of the relevant course);
b. access to e-mails or computers of third parties without their consent;
c. cracking passwords and other access authorisation tools;
d. violation of copyright and data protection laws.

The right to use IT facilities shall lapse directly on termination of the employment contract or of studies.

5 Surveillance of the HSGnet and exclusion from use

5.1 Surveillance of the HSGnet

[4] Cf. https://www.switch.ch/aai/

IT Services shall monitor compliance with these provisions within the framework of applicable law (particularly the legislation concerning data protection and the protection of the legal personality). On suspicion of an infringement of these provisions, the Management of IT Services in coordination with the Legal Office shall take appropriate measures in compliance with statutory provisions in order to prevent any further violations, secure any evidence, restore the systems to their original condition and guarantee the security and operability of the systems.

In accordance with Appendix A, access to other persons' business e-mails is permissible in certain cases. When evaluating logfiles, IT Services shall take Appendix B into consideration.

5.2 Exclusion from use

Users who violate the provisions or utilise the system in another improper manner may be excluded from the use of the HSGnet. If there is a serious suspicion of improper use, the Management of IT Services in coordination with the Legal Office shall be entitled to block access authorisation to the HSGnet temporarily without advance warning. The initiation of steps under civil and/or criminal law by the University Management shall be reserved.

5.3 Exclusion procedure

Users who have been excluded for precautionary reasons and whose user account has been closed shall have to report to IT Services. After the situation has been clarified, the Management of IT Services may either reopen the user account without any formalities or submit a request concerning the further course of action to the Executive Director. The President may order the definitive closure of a user account.

Such an order may be appealed against before the Senate Committee (Art. 41 of the University Act, Consolidated Statute Book of the Canton of St.Gallen, No. 217.11).

In addition, administrative legal procedures shall be governed by the University Act (Consolidated Statute Book of the Canton of St.Gallen, No. 217.11) and the Administrative Procedure Act (Consolidated Statute Book of the Canton of St.Gallen, No. 951.1).

The communication and information required for the continuation of studies shall be guaranteed until the exclusion procedure has been completed.

6 Final provisions

The HSG IT User Regulations were issued on 1 March 2016 and became effective as of that date. They replace the HSGnet User Regulations of 12 April 2005.

On behalf of the Senate Committee:

The President:
Prof. Dr. Thomas Bieger

The General Counsel:
lic.iur. Hildegard Kölliker

Appendix A: Access to e-mails by third parties

1 Principle

If the private use of e-mails and the internet is not prohibited at the HSG, it must basically be assumed that private e-mails do in fact exist.

2 Private e-mails

Private e-mails must not be accessed even in cases of representation by third parties unless the owner of the mailbox gives his or her consent or there is an order from the prosecution authorities.

3 Business e-mails

E-mails with unequivocally business contents may be accessed by substitutes in the mailbox owner's absence.

Appendix B: Evaluation of logfiles

1 Generation of logfiles

The HSG uses various technical protection measures against improper use of and technical damage to its IT systems, for instance virus scanners, firewalls and network monitoring systems. In this context, the systems generate so-called logfiles (records) of the most important activities that are carried out.

2 Anonymous evaluation

Anonymous evaluations of logfiles by IT Services are permissible at any time and without prior notification. They are conducted for statistical evaluation in accordance with system-specific criteria (examples: used bandwidth, biggest downloads, number of e-mails sent).

3 Pseudonymous evaluation

Pseudonymous evaluations of logfiles may be conducted by order of the University Management on a random basis but not permanently. HSG members have to be given advance notice of the period of the pseudonymous evaluations in a suitable form. Pseudonymous evaluations are conducted for the purpose of logfile evaluations in accordance with pseudonymised, identifiable persons (example: number of e-mails sent by an institute of an administrative unit during the evaluation period). The identity of the persons involved in a pseudonymous evaluation must not be easy to establish.

4 Person-related evaluation

If anonymous and/or pseudonymous evaluations reveal, or arouse suspicion of, cases of improper use, logfiles can be evaluated on a personal basis. If the suspicion of improper use is not corroborated, the person-related evaluation of the logfiles is discontinued forthwith.
If a criminal offence is discovered or suspected, the relevant logfiles are stored separately. In such cases, the University Management reserves the right to lodge a complaint against the person concerned. The HSG treats the results of any possible investigations in confidence. In cases of person-related evaluations of logfiles, the persons concerned have to be informed about this after the event.