Preamble:

**The RBO of 04.10.2016 differs from the
the "old" RBO of 07.02.2008 only through
editorial adjustments to the new faculty structure of the
structure of the university.
This means in particular that the obligations
obligations entered into in relation to the old RBO
continue to apply without restriction.**

Saarland University

Faculty of Mathematics and Computer Science (MI)

Computer Usage Regulations (RBO)

[As of: 04.10.2016]

More information:

1. Scope of application of the user regulations

The Computer Usage Regulations (RBO) regulate the use of the communication and data processing infrastructure (DP resources) of the Faculty MI (FakMI) by student and other users. The RBO is intended to enable the most secure, trouble-free, and unimpeded use of FakMI's communications and data processing infrastructure. The RBO regulates the usage relationship between the individual users among themselves and to FakMI and establishes the basic rules for the proper operation of the communication and data processing infrastructure.

2. Purpose of the facilities

The communication and data processing infrastructure of the FakMI is to be used within the scope of the tasks of the university in research, teaching and study.

The intended purpose includes, in particular, all exercises and practicals for courses, free practice for in-depth study, all work commissioned by the department, and the use of the communication facilities within the scope permitted in each case.

The individual purposes of use can be given priorities and restrictions by the operator.

Use for private and commercial purposes is excluded.

3. Admission of student users

Admission to computer use is requested at specified times from the offices announced by notice. The application is made by submitting a form for students with a major in computer science or mathematics and for students with a minor by entering their name in the list of participants of a course held at the FakMI. Admission is granted by assigning a user ID, taking into account available capacity. It may be subject to a limitation of resources and services and other conditions within the scope of the intended purpose of the facilities as set forth in Section 1. Approval is subject to the written acceptance of the RBO.

Other persons and institutions may be admitted to use or offer services for scientific purposes or to fulfill the tasks of the institutions of higher education of the Land, provided that the interests of the users specified in subsection 1 are not impaired thereby.

The representatives of the departments for computer operation (BfR) decide on the admission or refusal of admission.

4. Duties of the users

The user undertakes,

a) to use the provided equipment carefully, economically and in accordance with the intended purpose;

b) to keep the password of the user identification assigned to him secret and not to pass on information about other user identification that has become known to him and not to use it himself;

c) to take measures to protect against unauthorized use of his user ID. The system operator shall provide users with information on such measures;

d) to refrain from anything that disturbs the proper operation of the plant;

e) to behave in the working areas in such a way that other users are not disturbed;

f) to report any malfunctions, damage, faults and safety deficiencies in the facilities, equipment, data carriers and programs to the respective BfR without delay and not to take advantage of them;

g) to follow the instructions of the personnel of the plant operator on the premises of the plant operator and when using its equipment, data carriers and other facilities;

h) to respect the rights and person of other users;

i) not to feign false identities;

j) to disclose his/her identity when services request it;

k) to provide information about programs and methods used for control purposes to the respective BfR upon request and in justified cases, as well as to allow inspection;

l) to import and use licensed software only after consultation with the respective BfR;

m) not to copy or pass on software, documentation or data provided by FakMI or Saarland University to third parties, unless this is expressly permitted, nor to use them for purposes other than those permitted,

n) not to store personal data without a legal basis or without the consent of the persons concerned and to comply with the statutory provisions and other relevant regulations;

o) not to determine or use third-party user IDs

p) not to gain unauthorized access to other users' information and not to pass on, use or change other users' information that has become known without permission.

Reference is made to the relevant legislation (in particular concerning: copyright infringements (§§ 106ff. UrhG), spying out data (§ 202a StGB), data alteration (§303a StGB), computer sabotage (§ 303b StGB), computer fraud (§ 263a StGB), insult and slander (§§ 185ff, StGB), distribution of pornographic writings and distribution of pornographic performances by broadcasting, media and teleservices (§§ 184b, 184c StGB)).

(see also Annex 1)

q) In addition, reference is made to the regulations on the use of computer equipment (Annex 2), which supplement and concretize the obligations outlined here.

5. User rights

The user has the right,

a) to use the operating resources (computing time, storage, devices, networks, rooms and programs) made available to him by FakMI within the scope of the RBO;

b) to receive advice and support from the respective BfR to the extent possible;

c) to contact the respective BfR with suggestions and proposals;

d) to the elimination of occurring disturbances by the respective BfR within the possible scope.

6. Special services

The system operator can make supplementary arrangements for special services.

7. Violation procedure

Users may be temporarily or permanently restricted in their use of the DP resources or excluded if they

1. culpably violate the RBO, in particular the obligations listed under No. 5 (abusive behavior) or
2. misuse the communication and data processing infrastructure for criminal acts or
3. the Faculty MI or the Saarland University suffer disadvantages due to illegal user behavior.

The measures according to paragraph a) shall only be taken after a previous unsuccessful warning. The persons concerned shall be given the opportunity to comment. The decision on exclusion is made by the respective BfR.

8. Opposition

The Faculty Council decides on appeals against decisions of the respective BfR according to clauses 3 and 7.

9. Rights and duties of the faculty MI

a) FakMI maintains a user file on the granted user authorizations, which lists the user and mail identifiers as well as the name and matriculation number of the authorized users.

b) Insofar as this is necessary for troubleshooting, system administration and expansion, or for reasons of system security and the protection of user data, FakMI may temporarily restrict the use of its resources or temporarily block individual user IDs. If possible, the affected users are to be informed of this in advance.

If there are actual indications that a user is providing illegal content for use on FakMI's servers, FakMI may prevent further use until the legal situation has been sufficiently clarified.

c) In accordance with the following regulations, FakMI is entitled to document and evaluate the use of the data processing systems by the individual users, but only to the extent that this is required

1. to ensure proper system operation,
2. for resource planning and system administration,
3. to protect the personal data of other users,
4. for billing purposes,
5. for the detection and elimination of malfunctions, and
6. for clarification and prevention of illegal or improper use.

Under the conditions of paragraph c), FakMI is also entitled to inspect the user files in compliance with data secrecy, insofar as this is necessary for the elimination of current malfunctions or for the clarification and prevention of misuse, insofar as there are actual indications for this.

However, inspection of the message and e-mail mailboxes is only permissible to the extent that this is indispensable to eliminate current malfunctions in the messaging service. In any case, the inspection must be documented and the user concerned must be notified immediately after the purpose has been achieved.

In accordance with the statutory provisions, FakMI is obliged to maintain telecommunications and data secrecy.

10. Liability of the user

a) The user is liable for all disadvantages incurred by FakMI or Saarland University as a result of misuse or illegal use of the DP resources and the user authorization, or as a result of the user culpably failing to fulfill his or her obligations under these usage regulations.

b) The user is also liable for damages caused by third party use within the scope of the access and use options made available to him, if he is responsible for this third party use, in particular in the case of passing on his user ID to third parties.

c) The user shall indemnify FakMI and Saarland University against all claims if third parties assert claims for damages, injunctive relief, or otherwise against FakMI/ Saarland University due to the user's abusive or illegal conduct. FakMI/Universität des Saarlandes will notify the user of the dispute if third parties take legal action against FakMI/Universität des Saarlandes.

11. Liability of FakMI/University of the Saarland

a) FakMI does not guarantee that the system will run error-free and without interruption at any time. Possible data loss due to technical malfunctions as well as the knowledge of confidential data by unauthorized access of third parties cannot be excluded.

b) FakMI assumes no responsibility for the correctness of the programs provided.

programs made available. The university is also not liable for the content, in particular for the accuracy, completeness and timeliness of the information to which it merely provides access for use.

c) In all other respects, FakMI shall only be liable in the event of intent and gross negligence on the part of its employees, unless there has been a culpable breach of essential cardinal obligations. In this case, the liability of the university is limited to typical damages foreseeable at the time of the establishment of the user relationship, unless intentional or grossly negligent conduct is involved.

12. Entry into force

The RBO becomes effective immediately with the Dean's emergency decision dated 04.10.2016.

Appendix 1 to the Computer Usage Regulations of the Faculty MI

University of the Saarland
Faculty MI - Mathematics and Computer Science

Important legal texts

[As of: 07.02.08]

Aim

This is a collection of excerpts from applicable German legal texts. It does not claim to be correct or complete.

Criminal Code

§202a Spying out data
(1) Any person who without authorization obtains for himself or another person access to data which is not intended for him and which is specially secured against unauthorized access by overcoming the access security shall be liable to a custodial sentence not exceeding three years or to a monetary penalty.
(2) Data within the meaning of subsection (1) shall only be data that is stored or transmitted electronically, magnetically or otherwise in a manner that is not directly perceptible.

§ 202b Data interception
Any person who, using technical means, obtains for himself or another person data not intended for him (Section 202a (2)) from a non-public data transmission or from the electromagnetic radiation of a data processing system without authorization shall be liable to a custodial sentence not exceeding two years or to a monetary penalty if the act is not punishable by more severe penalties under other provisions.

§ 202c Preparing the spying and interception of data
(1) Any person who prepares an offence under section 202a or section 202b by using
Passwords or other security codes which enable access to data (Section 202a (2)), or
1. computer programs whose purpose is the commission of such an act,
2. manufactures, obtains for himself or another, sells, gives to another, distributes or otherwise makes accessible, shall be punished by imprisonment not exceeding one year or by a fine.
(2) Section 149 (2) and (3) shall apply mutatis mutandis.

§ 303a Data modification
(1) Any person who unlawfully deletes, suppresses, renders unusable or modifies data (Section 202a (2)) shall be liable to a custodial sentence not exceeding two years or to a monetary penalty.
(2) The attempt shall be punishable.
(3) Section 202c shall apply mutatis mutandis to the preparation of an offence under subsection (1).

§303b Computer sabotage
(1) Any person who interferes with data processing that is of essential importance to another person's business, company or authority by

1. commits an act pursuant to Section 303a (1) or
2. destroys, damages, renders unusable, removes or alters a data processing system or a data carrier, shall be punished by imprisonment for not more than five years or by a fine.
(2) The attempt is punishable.

§185 Offense
The offense shall be punishable by imprisonment for a term not exceeding one year or by a fine, and if the offense is committed by means of an activity, by imprisonment for a term not exceeding two years or by a fine.

§186 Slander
Any person who, in relation to another person, alleges or disseminates a fact which is likely to bring him into contempt or to disparage him in public opinion shall, unless such fact is demonstrably true, be punished with imprisonment for not more than one year or a fine, and, if the offence is committed publicly or by dissemination of writings, with imprisonment for not more than two years or a fine.

§187 Defamation
Whoever, against his better knowledge, asserts or disseminates an untrue fact in relation to another, which is likely to make the latter contemptible or to degrade him in public opinion or to endanger his credit, shall be punished with imprisonment for a term not exceeding two years or a fine, and, if the offence is committed in public, at a meeting or by dissemination of writings, with imprisonment for a term not exceeding five years or a fine.

§263a Computer fraud

(1) Any person who, with the intention of obtaining an unlawful pecuniary advantage for himself or a third party, damages the property of another by influencing the result of a data processing operation by incorrect design of the program, by use of incorrect or incomplete data, by unauthorized use of data or otherwise by unauthorized interference with the operation shall be punished by imprisonment for not more than five years or by a fine.

Saarland Data Protection Act

§ 4 Permissibility of data processing; data avoidance and data economy
(1) The processing of personal data shall be permitted only if
a) this Act or another legal provision permits it, or
b) the data subject has consented.
Consent must be given in writing, unless another form is appropriate due to special circumstances. If the consent is to be given in writing together with other declarations, the data subject shall be specifically informed in writing of the declaration of consent. The data subject shall be informed in a suitable manner about the significance of the consent, in particular about the purpose for which the data will be used, and about any intended transfer to third parties; the data subject shall be informed of the legal consequences of refusing consent and of the right to revoke consent with effect for the future.
(2) .....

§ 6 Data secrecy
Those persons who have official access to personal data at public bodies or their contractors shall be prohibited from processing such data without authorization; this shall also apply after termination

of their activities. These persons shall be informed of the data protection regulations to be observed in their activities.

§ 19 Indispensability of the rights of the data subject
The rights listed in §§ 20 to 24 may neither be excluded nor limited by legal transaction.

§ 20 Information
(1) The data subject shall, upon request and free of charge, be provided with information by the controller regarding
1. the personal data stored about him/her,
2. the purpose and legal basis of the processing as well as
3. the origin of the data and the recipients of transfers, insofar as this is stored.
This shall not apply to data that is blocked because it may not be deleted due to statutory retention requirements or is stored exclusively for purposes of data backup or data protection control.
(2) The request shall specify the type of data about which information is to be provided. The data controller shall determine the procedure, in particular the form in which the information is to be provided, at its due discretion; if the data is stored in files, the data subject shall be granted access to the files upon request. Information from files or inspection of files shall be granted insofar as the data subject provides information that enables the data to be located with reasonable effort and insofar as nothing to the contrary results from Section 29 of the Saarland Administrative Procedure Act.
(3) The obligation to provide information or to grant inspection of records shall not apply insofar as
a) this would jeopardize the proper performance of the tasks of the responsible body,
b) this would endanger public security or otherwise be detrimental to the welfare of the Federation or a Land, or
c) the data or the fact of their storage must be kept secret in accordance with a legal provision or by their nature, namely because of the legitimate interests of a third party.
(4) A statement of reasons for the refusal to provide information or to inspect files shall not be required only if the purpose pursued by the refusal to provide information would be jeopardized by the communication of the reasons. In this case, the main reasons for the decision must be recorded. In any case, the data subject shall be informed that he or she may contact the State Commissioner for Data Protection.
(5) If the provision of information or the inspection of files relates to the origin of personal data from authorities of the Office for the Protection of the Constitution, the Public Prosecutor's Office and the police, from financial authorities, insofar as these store personal data for monitoring and auditing purposes in fulfillment of their statutory duties within the scope of the Fiscal Code, and from the authorities specified in Section 19 (3) of the Federal Data Protection Act, it shall only be permissible with the consent of these authorities. The same applies to the transfer of personal data to these authorities. Paragraphs 3 and 4 shall apply mutatis mutandis to the refusal of consent insofar as this Act applies to the aforementioned authorities.

§ 21 Correction, blocking and deletion
(1) Personal data shall be corrected if they are inaccurate. If personal data which is not processed automatically is to be corrected, it shall be indicated in a suitable manner at what time and for what reason this data was or has become inaccurate.
(2) Personal data shall be blocked if
a) their accuracy is disputed by the data subject and neither the accuracy nor the inaccuracy can be determined,

b) deletion in accordance with paragraph 3, sentence 2, is not possible and the data subject requests blocking,
c) the data subject requests blocking instead of deletion pursuant to paragraph 3 sentence 1 letter a,
d) if there is reason to believe that the deletion of the data will adversely affect the legitimate interests of the data subject,
e) they are stored only for purposes of data security or data protection control, or
f) they may not be deleted due to legal storage regulations.
In the cases referred to in sentence 1 letter d, the reasons shall be recorded. In the case of automated processes, blocking shall be ensured by technical measures; otherwise, a corresponding note shall be made. Blocked data may not be further processed beyond storage unless this is essential to remedy an existing evidentiary need or for other reasons that are in the overriding interest of the controller or a third party, or unless the data subject has consented.
(3) Personal data shall be deleted if
a) their storage is inadmissible or
b) their knowledge is no longer required by the Controller for the performance of its tasks.
If personal data are stored in files, the deletion pursuant to sentence 1 letter b shall only be carried out if the entire file is no longer required for the performance of the task; if deletion is not possible according to this, the data shall be blocked at the request of the data subject.
(4) Apart from the cases of paragraph 3, sentence 1, letter a, deletion shall be dispensed with insofar as the stored data are to be offered to an archive for transfer or are to be taken over by an archive on the basis of legal provisions.
(5) The bodies to which the data have been transmitted shall be informed without delay of the correction of incorrect data, the blocking of disputed data and the deletion or blocking of inadmissibly stored data. The information may be omitted if it would require considerable effort and there is no reason to fear adverse consequences for the data subject.

§ 22 Right of objection of the person concerned
Data subjects may also submit written objections to the controller against the processing of their personal data which is permitted by law, citing a special personal interest worthy of protection in individual cases. In these cases, the processing shall only remain permissible if an examination shows that the public interest in the processing prevails. Data subjects shall be informed in writing of the result of the review. If the objection is not met, the data subject shall be informed that he or she may contact the State Data Protection Commissioner. The right of objection does not exist if a legal provision obliges processing.

§ 23 Right of appeal of the person concerned
(1) Everyone shall have the right to apply directly to the State Commissioner for Data Protection if he or she believes that his or her rights have been violated in the processing of his or her personal data by a body subject to the control of the State Commissioner; this shall also apply to employees of public bodies.
(2) No one may be discriminated against or reprimanded for having turned to the State Commissioner for Data Protection.

§ 24 Damages
(1) If the data subject suffers damage as a result of automated processing of his/her personal data which is inadmissible or incorrect in accordance with the provisions on data protection, the data controller shall be obliged to compensate the data subject for such damage, regardless of whether the data subject is at fault. In serious cases, the data subject may also demand equitable

compensation in money for the damage that is not pecuniary damage. The party liable for compensation shall be liable to each person affected in accordance with sentences 1 and 2 for each damaging event up to an amount of 125,000 euros.
(2) Insofar as the unlawful or incorrect processing of personal data is not automated, the controller shall only be liable in the event of fault. The Controller shall not be liable if it proves that the circumstance as a result of which the damage occurred cannot be attributed to it.
(3) Sections 254, 839 (3) and 852 of the German Civil Code shall apply mutatis mutandis to the contributory negligence of the party concerned and to the limitation period for the claim for compensation.
(4) Further-reaching other claims for damages shall remain unaffected.

Penalty and fine provisions; transitional provisions

§ 35 Crimes
(1) Any person who, without authorization, discloses personal data protected by this Act in return for payment or with the intent to enrich himself or another or to harm another,
1. collects, stores, modifies, discloses, makes available for inspection or retrieval, deletes or uses,
2. retrieves, inspects, procures or causes to be passed on to himself or to others by false pretences,
shall be punished by imprisonment for not more than two years or by a fine. Attempt is punishable.
(2) Paragraph 1 shall apply only insofar as the act is not punishable under other provisions.

§ 36 Administrative offences

(1) It shall be an administrative offence for any person who, without authorization, discloses personal data protected by this Act which,

1. collects, stores, modifies, discloses, makes available for inspection or retrieval, deletes or uses,

2. retrieves, inspects or obtains such data or causes it to be disclosed to him/herself or to others by feigning false facts.

(2) The administrative offense may be punished by a fine of up to 50,000 euros.

Copyright Act

§15 General
(1) The author shall have the exclusive right to exploit his work in physical form; the right shall include in particular
1. the right of reproduction
2. the right of distribution
3. the right of exhibition.

§16 Reproduction right
(1) The reproduction right is the right to make copies of the work, regardless of the method and number of copies.

§17 Distribution right
(1) The right of distribution shall be the right to offer the original or copies of the work to the public or to put them into circulation.

(2) If the original or copies of the work have been put on the market by way of sale with the consent of the person authorized to distribute the work within the scope of this Act, their further distribution shall be permitted.

§23 Edits and redesigns

Adaptations or other transformations of the work may only be published or exploited with the consent of the author of the adapted or transformed work.

§24 Free use

1. an independent work created in free use of the work of another may be published and exploited without the consent of the author of the work used.
2. .....

§ 53 Duplications for private and other own use

(1) Individual reproductions of a work by a natural person for private use on any carrier

(1) Individual reproductions of a work by a natural person for private use on any medium shall be permitted, provided that they are not made directly or indirectly for commercial purposes and provided that the reproduction does not involve the use of an obviously unlawfully produced original or one that has been made available to the public. The person authorized to reproduce may also have the reproductions made by another person, provided that this is done free of charge or that the reproductions are made on paper or a similar medium by means of any photomechanical process or other process having a similar effect.

(2) It shall be permissible to make or have made individual copies of a work
produced

1. for the author's own scientific use, if and to the extent that the reproduction is required for this purpose and does not serve any commercial purposes,
2. for inclusion in one's own archive, if and to the extent that reproduction is required for this purpose and one's own work is used as a template for reproduction,
3. for the purpose of informing the public about current affairs, if the work is broadcast by radio
broadcast work is concerned,
4. for other personal use,

a) if it concerns small parts of a published work or individual contributions which have appeared in newspapers or magazines,

b) if the work has been out of print for at least two years.

In the case of sentence 1 no. 2, this shall only apply if in addition

1. the reproduction on paper or a similar carrier by means of any
photomechanical processes or other processes with a similar effect, or
2. an exclusively analogous use takes place or
3. the archive is active in the public interest and does not pursue any directly or indirectly
economic or profit-making purpose.

In the cases of sentence 1 nos. 3 and 4, this shall apply only if, in addition, one of the
conditions of sentence 2 No. 1 or 2 are fulfilled.

(3) It shall be permissible to make reproductions of small parts of a work, of works of small extent or of individual contributions which have appeared in newspapers or periodicals or which have been made publicly accessible, for the author's own use

1. to illustrate teaching in schools, in non-commercial institutions for initial and further training and in vocational training institutions in the number required for the participants in the lessons, or
2. for state examinations and examinations in schools, universities, in non-commercial institutions of training and further education as well as in vocational training in the required number to produce or

have produced, if and to the extent that the reproduction for this purpose is required. Reproduction of a work intended for educational use in schools shall always be permitted only with the consent of the rightholder.
(4) The reproduction of
a) graphic recordings of musical works,
b) of a book or periodical
if it is an essentially complete reproduction, shall, unless it is made by copying, always be permitted only with the consent of the rightholder or under the conditions of paragraph 2, sentence 1, No. 2, or for the rightholder's own use if it is a work that has been out of print for at least two years.
(5) Paragraph 1, paragraph 2, sentence 1, nos. 2 to 4, and paragraph 3, no. 2, shall not apply to database works whose elements are individually accessible by electronic means. Paragraph 2, first sentence, No. 1, and paragraph 3, No. 1, shall apply to such database works with the proviso that scientific use and use in teaching shall not be for commercial purposes.
(6) The copies may neither be distributed nor used for public reproduction. However, it is permissible to lend legally produced copies of newspapers and out-of-print works, as well as such works in which small damaged or lost parts have been replaced by copies.
(7) The recording of public lectures, performances or presentations of a work on visual or audio media, the execution of plans and designs for works of visual art and the reproduction of a work of architecture shall always be permitted only with the consent of the rightholder.

§106 Unauthorized exploitation of copyrighted works

(1) Any person who, in cases other than those permitted by law, reproduces, distributes or publicly reproduces a work or an adaptation or transformation of a work without the consent of the rightholder shall be liable to a custodial sentence not exceeding three years or to a monetary penalty.

(2) The attempt is punishable.

Special provisions for computer programs

§69a Subject of protection
(1) Computer programs within the meaning of this Act are programs in any form, including design material.
(2) The protection granted shall apply to all expressions of a computer program. Ideas and principles underlying an element of a computer program, including ideas and principles underlying interfaces, shall not be protected.
(3) Computer programs shall be protected if they constitute individual works in the sense that they are the result of the author's own intellectual creation.
No other criteria, in particular qualitative or aesthetic, shall be applied to determine their protectability.
(4) The provisions applicable to linguistic works shall apply to computer programs, unless otherwise provided in this Section.

§69b Authors in employment and service relationships
(1) If a computer program is created by an employee in the performance of his duties or in accordance with the instructions of his employer, the employer shall be exclusively entitled to exercise all proprietary rights in the computer program, unless otherwise agreed.
(2) Paragraph 1 shall apply mutatis mutandis to employment relationships.

§69c Actions requiring consent

The rightholder has the exclusive right to perform or create the following acts:

1. the permanent or temporary reproduction, in whole or in part, of a computer program by any means and in any form. To the extent that loading, displaying, running, transmitting or storing the computer program requires reproduction, such acts shall require the consent of the rightholder;
2. translation, editing, arrangement and other reworking of a computer program, as well as reproduction of the results obtained. The rights of those who edit the program shall remain unaffected;
3. any form of distribution of the original of a computer program or of copies thereof, including rental. If, with the consent of the rightholder, a copy of a computer program is put on the market in the territory of the European Communities or of another State party to the Agreement on the European Economic Area by way of sale, the distribution right shall be exhausted in respect of that copy, with the exception of the rental right.

§69d Exceptions to the actions requiring consent

(1) In the absence of special contractual provisions, the acts referred to in §69c Nos. 1 and 2 shall not require the consent of the rightholder if they are necessary for proper use of the computer program, including error correction, by any person entitled to use a copy of the program.

(2) The creation of a backup copy by a person authorized to use the Program may not be contractually prohibited if it is necessary for securing future use.

(3) The person entitled to use a copy of a program may, without the consent of the rightholder, observe, examine or test the operation of that program in order to determine the ideas and principles underlying a program element, if this is done by actions to load, display, run, transmit or store the program to which he is entitled.

§69e Decompilation

(1) The consent of the rightholder shall not be required if the reproduction of the code or the translation of the code form within the meaning of §69c Nos. 1 and 2 is indispensable to obtain the information necessary to establish the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

1. the acts are performed by the licensee or by another person authorized to use a copy of the program or on his behalf by a person authorized to do so;
2. the information necessary for establishing interoperability has not yet been made readily available to the persons referred to in No. 1 above;
3. the actions are limited to the parts of the original program necessary to establish interoperability.

(2) Information obtained in the course of actions referred to in paragraph 1 shall not be used

1. be used for purposes other than establishing interoperability of the independently created program,
2. be disclosed to third parties unless necessary for the interoperability of the independently created program,
3. used for the development, production or marketing of a program with substantially similar expression or for any other acts infringing the copyright.

(3) Paragraphs (1) and (2) shall be interpreted in such a way that their application shall neither interfere with the normal exploitation of the work nor unreasonably prejudice the legitimate interests of the rightholder.

§69f Infringements

(1) The rightholder may require the owner or possessor to destroy all copies unlawfully made, distributed or intended for unlawful distribution. [...]
(2) Paragraph 1 shall apply mutatis mutandis to means intended solely to facilitate the unauthorized removal or circumvention of technical program protection mechanisms.

§69g Application of other legal provisions; contract law

(1) [...]
(2) Contractual provisions that conflict with §69d (2) and (3) and §69e shall be null and void.

Appendix 2 to the Computer Usage Regulations of the Faculty MI

University of the Saarland
Faculty MI - Mathematics and Computer Science

Rules for the use of computing facilities

[As of 12/06/13]

On the self-understanding of these rules

This catalog represents an unfinished collection of rules for the use of computers and networks in the Computer Science Department. These rules supplement the RBO and provide guidance for use.

A) Respect of access / access rights

1. do not attempt to gain access to other license plates, especially `root', without authorization.

2. do not attempt to break passwords of other license plates. 3.

3. the system operator must be informed of any security deficiencies discovered. They must not be exploited.

4. do not attempt to read or copy electronic mail or explicitly protected data of other users without their consent.

5. copyright protected software may only be used in accordance with the license.

B) User responsibility

1. the user is responsible for all actions under his license plate.

2. the user is responsible for choosing a secure password and for protecting his data. (i.e.: as passwords do not use names, words found in dictionaries (German or English), birthdays, account, passport or similar numbers; use upper and lower case).

3. passwords must be kept secret.

4. never leave your workstation unattended.

C) Use of the computers

1. do not interfere with the work of other users.

2. do not make any unauthorized attempts to modify devices, programs or data. In particular, do not introduce or apply virus programs. 3.

3. do not make unauthorized copies of programs and data.

4. do not use the provided equipment for commercial or partisan purposes.

5. attempts to use unauthorized services are prohibited.

6. the generation of BitCoins is expressly prohibited.

D) Rules for the use of news and mail

1. do not send messages with hurtful, abusive or obscene content.

2. do not send messages with commercial content (e.g. advertising for companies); private `classifieds' are allowed.

3. the sender of messages must identify himself/herself perfectly. In particular, deception about the true sender is prohibited.

E) General notes

1. you leave your workplace as you found it.

2. in the workrooms, conversations must be held at a low volume.

3. respect the rights and the person of other users.

4. eating, drinking and smoking are expressly forbidden in the workrooms.

F) Other

1. in all cases of doubt, the system operator must be consulted.

Appendix 3 to the Computer Usage Regulations of the Faculty MI

University of the Saarland
Faculty MI - Mathematics and Computer Science

Prohibitions on handling computer equipment in the computer science department (FRI) student computer pools.

[Status: 16.02.2006 resp. 04.10.2016]

Expressly prohibited:

- Connecting hardware that is not part of the computer room equipment.
- Unplugging and plugging in connectors of any kind.*.
- Tampering with equipment (including opening it).
- Turning off/on or rebooting equipment.**.
- Operating emergency stop switches without a true emergency being present.
- Disassembly of furniture.
- Eating and drinking in the computer rooms.
- Unnecessarily disturbing or inconveniencing others present in the rooms.

* Exception: data electrants in the front row of benches in Room 012.
** Report emergencies to the appropriate FRI staff. If supervisor is present, report directly there, or email operator@studcs.uni-saarland.de with a brief description of the condition of the machine.

Appendix 4 to the Computer Usage Regulations of the Faculty MI

University of the Saarland
Faculty MI - Mathematics and Computer Science

Notes on system security

[As of 4/21/1995 or 4/03/2000 or 10/04/2016]

System security requires that every account in the system be protected as well as possible against unauthorized use. Each user must feel responsible for the security of his or her account. After all, once an intrusion has been made into a poorly secured account, not only can system resources be misused on behalf of that user, but all other users are also threatened by the burglar's new capabilities. This checklist is intended to give the user hints as to which measures he or she can take to improve system security:

- Report recognized safety deficiencies to the plant operator and do not exploit them
- Observe rules for handling passwords:
  - the password should be 8 characters long
  - the password should not be a word with a meaning
  - the password should not be a word from a dictionary
  - the password should not be derived from personal data
  - the password should not be formed from known abbreviations
  - the password should contain upper and lower case letters, numbers, punctuation marks
    Example: Choosing a sentence with a meaning that can be remembered. Take in turn the first letter of each word and the punctuation marks as the password.
  - the password must be kept secret
  - the password must be changed regularly (about every 3 months)
  - on different security clusters * different passwords are to be chosen
  - do not store passwords in plain text in the computer (in scripts, etc.)
  - die Nutzung des eigenen Accounts auch keinem "guten Freund" erlauben
- Log off (log out) at the end of the session.

- if possible lock the terminal or lock the room even if you are absent for a short time
- no world-write-access to the home directory and all own files
- no world-access to point-files like .login, .cshrc, .profile, etc.
- no world-exec-access to own programs (risk for the caller)
- world read access to own files only in exceptional cases
- no set-UID programs with world exec access
- no set-UID or set-GID scripts
- set umask to value 077
- check own files from time to time for plausibility (name, owner, access protection, date) using "ls -alc
- include only secure directories in the definition of the command search path (CSH variable path, SH variable PATH, environment variable PATH)
- add current directory (".") as the last directory in PATH or path
- no "+" in .rhosts file
- no host and user from other security cluster in .rhosts file
- no entry without user in the .rhosts file
- no "old" entries (hosts , users) in .rhosts file
- in .netrc file only entries for access to anonymous FTP, no passwords
- be careful when running programs from other user directories (unwanted side effect, trojan horse)
- do not give command "xhost +" or "xhost +computer name
- make password entries via xterm only in secure mode (option secure-keyboard or secureonpwd)
- form a security cluster, e.g. the educational computers or the systems of a chair.