The *Regulations of Digital Information Processing and Communication (I&C) at the Karlsruhe Institute of Technology (KIT) [I&C Regulations]* ("*Ordnung für die digitale Informationsverarbeitung und Kommunikation (IuK) am Karlsruher Institut für Technologie (KIT)*", abbreviated "*IuK-Ordnung*") have been published as "Amtliche Bekanntmachung 2013 No. 36" of the Karlsruhe Institute of Technology (KIT) and have now been translated into English.
Please be advised that the only legally binding version of the regulations is the above-mentioned German version of the *IuK-Ordnung*. The following English translation is solely meant as an information on the content of the *IuK-Ordnung*.

Regulations of Digital Information Processing and Communication (I&C) at the Karlsruhe Institute of Technology (KIT) [I&C Regulations]

Pursuant to Sec. 3, para. 3 and Sec. 10, para. 2, No.6 of the Act on the Karlsruhe Institute of Technology (KIT Act – KITG) of July 14, 2009 (Baden Württemberg Law Gazette, pp. 317), as last amended by Article 5 of the Act on the Introduction of an Incorporated Student Body and on Strengthening Advanced Academic Training (Incorporated Student Body Act – VerfStudG) dated July 10, 2012 (Baden-Württemberg Law Gazette, pp. 457, 464), the KIT Senate adopted as statutes the following Regulations of Digital Information Processing and Communication (I&C) at the Karlsruhe Institute of Technology (KIT).

Preamble

The Karlsruhe Institute of Technology (KIT) and its administrative units operate a cooperative system of information supply and processing (ISP). One part of this system is the infrastructure for digital information processing and communication (I&C infrastructure).
These Regulations outline the conditions under which the I&C services are provided and can be used at the KIT.
The Regulations

- are based on the legal duties of the KIT and its mandate to protect academic freedom;
- establish ground rules of proper operation of the I&C infrastructure;
- draw attention to the third-party rights to be protected (e.g. software licenses, conditions imposed by network operators, data protection aspects);
- oblige users to behave correctly and make economical use of the resources offered;
- explain measures potentially taken by the operator in cases of infringement of these Regulations and associated provisions.

Section 1 Definitions

(1) For the purposes of these Regulations, I&C infrastructure shall be any and all I&C systems, such as data processing systems (computers), communication systems (networks and their components) as well as other systems of digital information processing, software and their combinations, and the associated services (I&C services).
(2) Pursuant to these Regulations, the operator of the I&C infrastructure shall be the Steinbuch Centre for Computing (SCC) of the KIT together with other systems operators and service providers in the administrative units of the KIT within the framework of a cooperative supply system.
(3) The SCC is an institute of the KIT charged to perform services as per para. 2. The organization and administration of the SCC and the other systems operators and service providers shall be guided by the administrative regulations of the respective administrative unit.
(4) Pursuant to Sec. 28, State University and College Act (LHG), the competences and services of the KIT in the areas of information supply and processing shall be concentrated in an information center organized as a cooperative venture, the Media & ISP Service Center Karlsruhe (MICK). It shall be made up of the SCC as the central I&C service provider, the KIT Library, the KIT Archive, and the other installations of the KIT required for ISP systems, processes and services. The MICK shall jointly coordinate, plan, manage and operate systems, processes and services for the supply of information and literature, information processing, and communication. It shall be managed jointly by the Directors and Heads, respectively, of the institutions referred to in sentence 2 above, and shall be supervised and controlled by the Chief Information Officer (CIO) of the KIT.

Section 2 Data Protection and IT Security

(1) The provisions of the State Data Protection Act (LDSG), data protection provisions specific to certain areas (especially Federal Telecommunications Act [TKG], Federal Telemedia Act [TMG]) as amended, and the technical and administrative measures of data protection shall be observed.
(2) The importance of IT security to the KIT shall be explained in a Guideline on IT Security at the KIT. The IT security concept of the KIT based on that guideline shall describe the organization of IT security management as well as the technical measures for implementing the IT security architecture at KIT.

Section 3 Scope of Application and Supplementary Provisions

(1) These Regulations shall apply at the KIT to the I&C infrastructure provided by the SCC and the other administrative units.

(2) The I&C infrastructure referred to in para. 1 above may be used by the members and staff of the KIT in fulfilling their duties in research, teaching, studies, administration, education and advanced training, public relations and external relations, international cooperation, knowledge and technology transfer, and other duties outlined in Sec. 2, KITG. Use for private purposes shall be allowed only under a separate user permit.

(3) Under the preconditions of Sec. 20, para. 2, KITG together with Sec. 28, para. 1, LHG, use may be permitted also for other purposes and other persons and institutions. Details of use on a payment basis shall be settled in separate fee regulations.

(4) To ensure proper operation of the I&C infrastructure, the management of the SCC or the respective administrative unit may adopt other rules about matters of everyday operation (Rules of Use and Operation). In a supplementary fashion, the provisions of the administrative regulations of the respective institution shall apply.

(5) The use of the I&C infrastructure shall be ruled by user relations under public law.

Section 4 Permit of Use and Admission

(1) Members and staff of the KIT may be admitted to using the I&C infrastructure. Other users may be admitted as far as necessary for the KIT to fulfil its duties. No admission shall be required to I&C services for which anonymous access is provided.

(2) Admission shall be granted by a user permit. This permit may be issued either without special application on the grounds of membership, especially on matriculation or the establishment of a service or working association with the KIT, or by special application. The permit of use shall be issued by the responsible operator.

(3) The operator may make the issuance of a permit of use dependent on proof of specific knowledge about the use of the I&C infrastructure. To ensure orderly operation with a minimum of failures, the permit of use may be attached to use-related conditions. The permit of use shall apply only to work and purposes connected with the use applied for, and may be issued for a limited period of time.

(4) When an application for admission is filed, it should contain this information:

1. Operator to whom the application for a permit of use is addressed to.
2. I&C services for which the permit of use is applied for.
3. Applicant: Name, accessibility, status – for students also matriculation number – and, if applicable, membership with an administrative unit or a recipient of services (client) different from the applicant, and other data required for cost allocation reasons.
4. Information about the purpose of use, especially where the applicant, within the framework of the permit, intends to process personal data with the I&C infrastructure by a process established by the applicant.
5. Acceptance of these regulations and of the supplementary provisions adopted pursuant to Section 3 as a basis of user relations.

(5) Other information may be collected only inasmuch as this is necessary for a decision about the application (Sec. 13, LDSG). At the latest six months after termination of the use applied for, the personal data collected together with the application shall be anonymized or destroyed (Sec. 23, LDSG) unless longer storage of the data is required under storage provisions not specific to the area in question.

(6) The permit of use may be denied, revoked or limited *ex post facto* either entirely or in part, especially if

1. no proper application has been submitted or the information in the application is not, or no longer, correct;
2. the preconditions for proper use of the I&C infrastructure do not, or no longer, exist;
3. the person entitled to use has been excluded from use pursuant to Sec. 6;
4. the existing I&C Infrastructure is unsuitable for the use applied for, or has been reserved for special purposes;
5. the capacity of the resources whose use is applied for is not sufficient for the planned use because of pre-existing loads;
6. the use must meet special data protection requirements and no factual reason for the planned use can be seen;
7. it is to be expected that the use applied for would inadmissibly impair other justified projects;
8. the planned project of the user does not concur with the duties of the KIT or the purposes of admission;
9. the export conditions of countries manufacturing computers or programs prohibit access or use by members of specific states named;
10. in the case of use against payment, the defined payment for use is not made at the proper point in time.

(7) The permit of use shall expire

1. with the notice of cancellation by the user;
2. upon expiry of a limited period of use;
3. with a change in status of the user, especially the end of KIT membership, unless otherwise agreed upon;
4. by revocation.

Section 5 Rights and Duties of Users

(1) The persons entitled to use (users) shall have the right to use the I&C infrastructure within the framework of the permit and subject to these Regulations. In addition, the regulations and provisions adopted in Sec. 3, para. 3 and 4, shall apply. Transactions with other operators, in addition, shall be subject to their supplementary guidelines for use and access unless these contradict the present I&C Regulations. Any other use shall require separate permits.

(2) The user shall be restrained from passing on rights of use. Users shall be obliged

1. to observe both the provisions of these Regulations and the limits of the permit of use and, in particular, pay attention to the purposes of use;
2. to contribute to a proper use of the I&C infrastructure, in particular refrain from upsetting proper operation of in-house and outside I&C infrastructures;
3. to handle carefully the I&C and other infrastructures;
4. to make responsible and economical use of the I&C infrastructure;
5. to use only the rights of use granted them;
6. to make sure that no other persons learn about the authentication keys, e.g. password, PIN, certificate, private key, and make provisions to prevent unauthorized persons from having access to the I&C infrastructure;
7. to neither determine nor disclose other authentication keys;
8. to seek no unauthorized access to information of other users and not pass on, use or modify any disclosed information of other users without authorization;
9. in using software and information, documentations and other data, to observe legal regulations, especially about copyright and trademark protection, and observe the licensing conditions under which software and documentations are made available;
10. to neither copy nor pass on to third parties software, documentations and data unless this is expressly allowed, or to use such items for purposes other than those authorized;
11. to comply with the instructions by personnel, and observe existing housekeeping rules, on the premises of the operator;
12. to produce the permit for use for use on request, and identify themselves;
13. without the express consent of the operator, not to interfere in the I&C infrastructure, especially introduce no private systems into the I&C infrastructure of the KIT without a specific user permit;
14. in well-founded individual cases, especially reasonable suspicion of misuse, to provide the operator on request with information about proper use;
15. to agree with the operator and the Data Protection Officer on the processing of personal data in a procedure within the meaning of Sec. 4, para. 4, No. 4 of these Regulations and, irrespective of the user's obligations under data protection laws, to take into account the data protection and data security provisions established by the operator;
16. to secure their data and programs in such a way that any loss will not entail damage to them;
17. to inform about changes in status.

(3) Any use shall by inadmissible which is likely to violate personal rights of others, impair the security of the I&C infrastructure, damage the reputation of the KIT in the public, or violate applicable legal provisions. Special reference is made to the following criminal offences:

1. clandestine spying out of data (Sec. 202a, Federal Criminal Code [StGB]);
2. data modification (Sec. 303a, StGB) and computer sabotage (Sec. 303b, StGB);
3. computer fraud (Sec. 263a, StGB);
4. dissemination of obscene presentations (Sec. 184, StGB), especially the possession of pornographic representations involving children (Sec. 184, para. 5, StGB);
5. dissemination of propagandistic publications of unconstitutional organizations (Sec. 86, StGB) and stirring up hatred against national, ethnic, racial or religious groups (Sec. 130, StGB);
6. tortious acts, such as insult or defamation (Sec. 185 ff., StGB);
7. punishable infringements of copyright, e.g. by copying software in violation of copyright (Sec. 106 ff., UrhG);
8. violation of the secrecy of telecommunications (Sec. 206, StGB).

(4) If the permit of use pursuant to Sec. 4, para. 2 in combination with Sec. 3, para. 2 and 3 includes the separate permission of private use or use by third parties, and if that permit of use also allows hosting of personal web pages, these pages must not be designed in such a way that they

could be regarded as web pages of the KIT and its administrative units, respectively. Users shall be obliged to comply with the legal provisions about web appearance.

(5) If links to unlawful contents are established from web pages under the responsibility of the operator, or if there are actual indications of their containing unlawful contents, and if this is detected by an operator, or if an operator is informed about such referencing or contents, the user shall be informed. The user shall immediately remove the respective references or contents. The operator shall have the right to block the presence of the web pending amendment by the user or satisfactory clarification of the legal situation.

Section 6 Exclusion from Use

(1) Users may be limited in, or excluded from, using the I&C infrastructure temporarily or permanently

1. if they negligently violate the provisions of these Regulations, especially the duties listed in Sec. 5, or
2. if they misuse the I&C infrastructure for criminal acts, or
3. if they cause disadvantages to the KIT by some other unlawful user behavior.

(2) Measures pursuant to para. 1 should be taken only after unsuccessful previous warning. The person concerned shall be given an opportunity to comment. Upon request, he or she shall be left the data legally owned by him/her. Before measures are instituted, misuse measures under Sec. 7 shall be initiated. In case the KIT is in danger of suffering detriments, temporary measures to avoid damage may be taken even before misuse measures are started.

(3) Temporary restrictions of use as decided by the operator shall be lifted as soon as proper use seems to be ensured again.

(4) Permanent restrictions of use, or complete exclusion of a user, shall be possible only in severe or repeated violations within the meaning of para. 1, where no proper behavior is to be expected in the future. The decision about permanent exclusion shall be taken by KIT's Executive Board deciding on an application by the management of the operator. Any claims of the KIT arising from the use relations shall be unaffected. The user shall have no right to claim damages on grounds of the exclusion.

Section 7 Measures in Case of Misuse / Joint Committee

(1) In case of suspected misuse of these Regulations on the part of employees represented by the Staff Council, a Joint Committee shall be established promptly by the CIO of the KIT upon application by the employer's side or the staff representation. The Joint Committee shall be composed equally of employer representatives and members of the Staff Council of the competent service unit. One representative of the data protection team shall be invited in an advisory capacity. The human resources department (PSE) shall be informed about the appointment, measures, and the outcome of the Joint Committee.

(2) If there is suspected misuse by a student pursuant to Sec. 6, para. 1, the CIO of the KIT shall convene a Joint Committee. The composition of the Joint Committee (e.g. also including student representatives) shall be determined by the CIO in the light of the specific case. A representative of the data protection team shall be invited in an advisory capacity.

(3) If misuse pursuant to Sec. 6, para. 1 by any other user is suspected, a Joint Committee shall be convened by the CIO of the KIT. The composition of the Joint Committee shall be determined by the CIO in the light of the specific case. A representative of the data protection team shall be invited in an advisory capacity.

(4) The Joint Committee shall determine whether or not there is a case of misuse. In case the suspected misuse has been confirmed, the KIT shall institute the appropriate legal steps.

(5) The Joint Committee shall decide in each case which data may be accessed to examine potential misuse. This shall also apply to data protected from access because of operational regulations. As soon as joint evaluation indicates that there is no misuse, all data and documents established in connection with the suspected misuse shall be destroyed immediately. Otherwise there shall be no duty to destroy data as long as the Joint Committee has found a case of misuse and these data are needed.

Section 8 Rights and Duties of the Operator

(1) For operational reasons, the operator shall have the right to restrict temporarily the use of the I&C infrastructure or block temporarily individual user ID's. Where possible, the users affected by these measures shall be informed in advance. In any case, the users affected shall be explained at short notice why the respective measure had been necessary.

(2) If there are real indications showing that a user keeps unlawful contents ready for use on the I&C infrastructure of the operator, the operator shall have the right to prevent any further use until the legal situation has been cleared up sufficiently.

(3) The operator shall have the right to verify the security of authentication keys and the user data by regular manual or automatic procedures and carry out any necessary measures of protection in order to protect the I&C infrastructure and user data from unauthorized access by third

parties. The user shall be informed immediately of any measures taken which affect him / her directly.

(4) Records of the operating system and the system-related software (log files) may be documented and evaluated to ensure proper, secure, and smooth operation, for resource planning, to protect personal data of other users, and to determine the costs of system use, but only to the extent in which this is necessary.

Access to those data shall be restricted to the systems administrators. The period of storage of such records shall be limited to the period of time necessary to meet the purpose referred to above. The systems administrators shall be allowed to transmit any information obtained from the systems records only within the framework of the purposes referred to in this section.

(5) The operator shall make available to the users mechanisms ensuring the personal use of data storage areas in such a way that only the respective individual user shall have access to that area.

(6) Subject to the conditions in para. 4 above, also connection and use data in message transmission, especially mail use, may be documented. However, only the immediate circumstances of telecommunication, not the non-public contents of communication, may be collected, processed, and used.

(7) To support users, the systems administrators may require access to the workstations of users and their user interfaces, respectively. Such access shall be permitted, as a matter of principle, only with the consent of the users.

(8) To localize malfunctions and vulnerabilities, an operator shall have the right to use programs which analyze the services offered in the network by the respective system. If any peculiarities of the system were detected in this way which would raise doubt about proper operation, security, and availability of the I&C infrastructure, the operator shall have the right to disconnect the system from the network. Such peculiarities shall include, in particular, actual indications pointing to the existence of a technical defect or a fault. Analyses of services of the system not offered in the network shall not be permitted without prior consent of those responsible for the system.

(9) The use of the I&C infrastructure documented under the preconditions of paras. 4 and 6 to 8 shall be processed only for the purposes justifying logging pursuant to para. 4, and shall be destroyed immediately when no further storage is required. Logging personal data and the periods of destroying such data as well as the responsibility for conducting the destruction process shall be documented.

(10) If a suspicion of criminal acts becomes tangible, the misuse measures pursuant to Sec. 7 shall be initiated. The operator shall have the right to take measures protecting evidence even before initiating misuse measures. The KIT expressly reserves the right to initiate criminal proceedings and pursue claims under civil law.

(11) Transmission to third parties of any personal data logs shall be examined for admissibility by the Joint Committee pursuant to Sec. 7, where appropriate with the inclusion of other experts.

(12) Subject to legal provisions, the operator shall be required to protect telecommunication and data privacy. When processing personal data, the operator shall be obliged to take into account legal requirements of data privacy.

(13) The operator shall be obliged in transactions with other operators to comply with their supplementary use and access regulations to the extent in which they do not contradict these Regulations.

(14) The operator shall have the right, in case of expiry or revocation of the user permit, to destroy, after a reasonable period of time, the data filed by the user and under the permit for use of that user.

Section 9 User Liability

(1) The user shall be liable for any and all damage arising to the KIT out of wrongful or unlawful use of the I&C infrastructure or out of the fact that the user negligently fails to observe his / her duties under these Regulations.

(2) The user shall also be liable for damage caused by third-party use within the framework of the access and user rights available to him / her if he / she is responsible for such third-party use, especially in case of a transmission of his / her user ID to third parties. In this case, the KIT shall be allowed to claim from the user payment for the use by third parties subject to the payment regulations.

(3) The user shall exempt and hold harmless the KIT from any and all claims in cases where third parties sue the KIT for damages, default, or in any other way, because of misuse or unlawful behavior of the user. The KIT may give third-party notice to the user when third parties initiate legal proceedings against the KIT.

Section 10 KIT Liability

(1) The KIT shall not assume any warranty for faultless and smooth operation of the I&C infrastructure and for the correctness of its results. Any losses of data and the dissemination of confidential data as a result of unauthorized access of third parties cannot be excluded.

(2) The KIT shall not assume responsibility for the correctness of the programs and data made available. Nor shall the KIT be liable for the content, in particular for the correctness, completeness and topical nature of the information for which it merely mediates access to use.

(3) For the rest, the KIT shall be liable only in cases of intent and gross negligence of its staff members, unless there is a case of criminal violation of key duties. In this case, the liability of the KIT shall be limited to typical damage foreseeable when the use relations were established, except for intent or gross negligence.
(4) Any official claims for liability against the KIT shall be unaffected of the provisions above.

Section 11 Calculation of Service Fees

The SCC and other operators are free to offer their services to other universities or other third parties for a fee. The details shall be laid down in fee regulations.

Section 12 Entry into Force

These Regulations shall enter into force as statutes on the day after publication in the official announcements of the KIT. At the same time, the Administration and User Regulations of the Computer Center dated July 17, 2003, and the previous User Regulations for Information Processing Systems of the University of Karlsruhe (TH) dated December 21, 1999 shall cease to be valid.

Karlsruhe, October 15th 2013
Professor Dr. Holger Hanselka
(President)