# Detailed Operating Rules on the Use of Computer Resources

Established Dec. 20, 1999
Amended Jun. 1, 2001

Article 1 (Purpose) These detailed operating rules set forth matters concerning the protection of computer resources and the creation of a computing environment for efficient use of computer resources.

Article 2 (Definition of Terms) The terms used in these regulations shall be defined as follows:

1. “User” refers to any of the professors, staff members, researchers, and students of Pohang University of Science and Technology (hereinafter referred to as “University”) and other persons authorized to use the computer resources of the University.
2. “Computer resource” refers to any and all computers, network equipment, peripheral devices, software, and related (built-in) information resources regardless of connection to the computer network of the University, research purpose, business purpose, instruction purpose, or personal purpose.
3. (Deleted)
4. “Computer security” refers to any and all accesses to computer resources in an unauthorized manner or without legitimate authority and infringement on or misuse of the computer resources.
5. “System administrator” refers to any system administrators of the Office of Academic Information Affairs and any persons appointed for the system administration of the organizational subunits such as research laboratories or academic departments, etc., of the University.

Article 3 (Scope of Computer Resource Use) ① In principle, the computer resources of the University shall be used for purposes of instruction, research, and business only.

② In case of violation of the standard of use as specified in Article 4, the use of computer resources shall be restricted as specified in Article 6, or disciplinary action shall be taken based on the school regulations.

Article 4 (Standard of Computer Resource Use) Any of the following acts committed by a computer resource user shall be deemed misuse/abuse of the computer resources of the University:

1. An act of copying copyrighted software on the computer resources of the University without permission or distributing such software to the public
2. An act of using copyrighted data such as document, image, moving pictures, logo, program, other files, etc., other than software without permission, that can be obtained from computers or through computer networks
3. An act of copying or distributing in excess of the limited number of uses after obtaining software
4. An act of modifying, destroying, or moving the computer resources owned by other user or whose installation place is designated
5. An act of installing a server and providing service internally and/or externally without obtaining prior approval from the University
6. An act of using an IP address or a domain name that is not accepted by the University without permission
7. An act of intentionally accessing unauthorized computer resources or letting other persons access such
8. An act of hacking computer resources for which he/she has no authority to access and perusing, copying, leaking, or damaging the computer system file, data, etc., of other person
9. An act of intentionally developing or using a program (e.g., virus program, etc.) that may damage the configuration of the computer resource
10. An act of misusing or abusing a computer in another site connected to the network of the University

11. An act of intentionally disclosing his/her encrypted account information to other person
12. An act of using the computer resources of the University for a commercial, political or personal purpose without appropriate approval
13. An act of misusing or abusing electronic mail (e.g. by sending spam mail) or using the computer resources as a source of spamming
14. An act of using an email mailing list for purposes other than prescribed
15. Violation of the Detailed Rules for System Operation as determined in Article 40, Regulations for the Operation of the Office of Academic Information Affairs
16. Other cases regarded as misuse/abuse of computer resource by the Academic Information Committee

Article 5 (Responsibility and Authority of the System Administrator) ① Tasks related to the management and supervision of computer resources shall be delegated to a person responsible for the management of each department; a “system administrator” may be appointed, whose role is to establish and determine detailed guidelines within the scope of these regulations and to operate the system.

② The system administrator shall have the following responsibilities for the system under his/her control:

1. Take preventive action against theft of, damage to, or intrusion on computer system or its component.
2. Maintain the right to use the software of the computer system.
3. Manage the information stored in the system or the information on users.
4. Take auxiliary action to prevent hacking or information leakage.
5. Issue public notice on the guidelines or procedure as to the service provided or not provided to the system users.
6. Respond to the request of the department concerned or other system administrators in case of a misuse or an abuse of computer resources.

③ The following authority shall be granted to take reasonable measures for the protection of the system when the regulations on the use of computer resources are violated:

1. The right of any user may be temporarily suspended when deemed necessary to maintain the integrity of the computer or network.
2. If there is a valid reason to expect inappropriate use of computer or network resources, personal data (file, diskette, tape, and other recording media) may be investigated, or messages may be monitored.

Article 6 (Sanction) ① If misuse/abuse of computer resources or distribution of unhealthy information arises, each system administrator shall notify the system administrator of the Office of Academic Information Affairs.

② The system administrator may take preemptive action such as restriction on the use of the system, etc., if necessary for the protection of the computer resources.

③ In case of violation of the provisions of Articles 4 and 5, the sanctions shall be as follows:

1. Warning
2. Restriction on the use of computer resources or services

④ If an offense requires a more severe disciplinary action than restriction on the use of the system, the Academic Information Committee shall request that disciplinary action be taken by the Vice President of Admissions and Student Affairs against a student; the Vice President of Business Affairs against a staff member; the Vice President of Academic Affairs against a professor; the dean of his/her professional graduate school against a professional graduate student ; and the head of an office or agency with the authority for personnel management against a researcher.

Article 7 (Petition) ① A person under sanction may raise an objection and present a petition for the restoration of user rights by presenting the petition in writing to the heads of the departments or agencies specified in Article 6, Clause 4.

② Once the petition is received, the department concerned must conduct a review in accordance with the regulations and notify the petitioner and the Office of Academic Information Affairs of the review result.

Article 8 (Deleted)

# Addenda

1. In case of misuse/abuse of computer resources other than any of those set forth in these regulations, the Academic Information Committee shall make decisions on such cases.
2. The detailed guidelines necessary for the regulations on the use of computer resources use shall be stipulated separately.
3. These regulations shall take effect on December 20, 1999.

## Addenda

1. (Effective Date) These amended detailed operating rules shall take effect on June 1, 2001.
2. (Interim Measure) Since the previous Regulations on the Use of Computer Resources are divided into these detailed rules and the Detailed Operating Rules on the Ethical Use of Information, the Regulations on the Use of Computer Resources are hereby abolished on the effective date of these detailed rules.