Management Regulations of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences on Computer Network and Information Security (Trial)

Article 1: Purpose

Ensure the network and information security of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences (SIAT) and standardize the network resource use in the SIAT and the Internet use behavior in each institute.

Article 2: Applicable Scope

All network users ofthe SIAT.

Article 3: Reference

Provisional Regulations of the People 's Republic of China on the Administration of the International Networking of Computer Information Networks.

Article 4: Responsibilities

I. The Network and Information Security Leading Group of the SIAT is responsible for dealing with major issues of network and information security of the SIAT, coordinating and handling major and sudden emergencies.

1. Deal with network and information security events ofthe SIAT;

2. Monitor network events, timely report problems to the Emergency Group of the Science and Technology Network;

3. Provide network and information security consulting and technical support to all users of the SIAT;

4. Periodically scan the network for security vulnerabilities and notify end users;

5. Provide network and information security education and training;

II. The network and information security management of the SIAT is the responsibility ofthe Department of Science & Technology Development of the SIAT.

1. Responsible for the planning, construction, management, and maintenance of the network infrastructure ofthe SIAT;

2. Responsible for the safeguard ofthe network and information security of the SIAT;

3. Responsible for the daily liaison and transaction handling for the network management;

4. Designate special personnel to manage and maintain computer network;

5. Regularly optimize network security performance, acquire necessary hardware and software facilities and effectively resist external intrusion.

III. Responsibilities ofpart-time network administrator ofeach unit

1. Responsible for monitoring and analyzing the network and information security in his/her unit, timely discovering and handling network faults, summarizing security event information;

2. Get familiar with the members of the Network and Information Security Leading Group of the SIAT, clearly understand the responsibilities of each member and grasp the emergency handling process;

3. Strengthen security and confidentiality prevention, improve the backup mechanism of important scientific research and business data in his/her unit;

4. Strengthen the management of information content security, discover, remove and report harmful information timely;

5. Cooperate with and assist the Department of Science & Technology Development to implement relevant system.

Article 5: Management Measures

1. The SIAT provides paid network access services for the users of the SIAT, and the fee is charged in the form of departmental expenses (charge rules refer to the financial related management system);

2. The SIAT provides paid network access services for the users of the external cooperation units or companies cooperating with the SIAT,

and the management content and tariff refer to the *Agreement of External Cooperation Personnel Using Network Resources of Shenzhen Institute of Advanced Technology*.

3. All network users must abide by related laws and regulations such as the *Provisional Regulations of the People 's Republic of China on the Administration of the International Networking of Computer Information Networks*.

4. The computer network, software and hardware resources in the SIAT are only used for scientific research, education and related business. When using the network to conduct data transmission, e-mail communication or news release, the contents must be related to the above work nature and should not violate the provisions of national security regulations relating to computers and the international Internet. The users should strictly implement the security and confidentiality system, and be responsible for the information provided.

5. The computer accounts of the SIAT are only granted to the employees of the SIAT for personal use, and the authorized persons have the responsibility to protect the resources enjoyed by himself or collectively. A password must be more than six characters and must not be disclosed to others. Collective accounts should have a perfect registration system when being used for Internet. If the account information is disclosed, it should be changed in time, and it is strictly forbidden to share an account with others. The received e-mails cannot be retained on the mail server.

6. Without authorization, any unit or individual should not modify or delete network data. It is strictly forbidden to make or distribute destructive programs, endanger the security of computer information networks, disassemble, misappropriate or occupy network equipment and resources.

7. Comply with the international practice conducive to scientific and technological exchange. Without authorization, it is forbidden copy software resources that do not belong to oneself, and it is strictly forbidden to input files infected viruses into the computer. Install the latest system upgrade program and upgrade the virus library timely.

8. Abide by the relevant laws and administrative regulations ofthe State, strictly implement the rules and regulations ofthe SIAT on security and confidentiality, it is forbidden to use the Internet to engage in illegal and criminal activities such as endangering national security and leaking state secrets, or produce, search, copy and distribute information that impedes social security or contains pornographic contents; computers accessing the Internet are strictly prohibited from handling classified information, state secret information is strictly prohibited to be distributed through any communication equipment without security safeguard measures, and classified computer systems must comply with relevant state regulations and standards.

9. It is strictly prohibited to spread the malicious information passively received on the computer. The users should report to the network administrator timely and assist the administrator to delete such information, and report to the relevant department for handling.

10. It is strictly prohibited to conduct resource-consuming and non-scientific-significance test operations, advertising or chain communication operations, game or gambling operations on networks and computers. It is prohibited to use BT, eDonkey, Thunder, Super Cyclone and P2P protocol download software. It is strictly prohibited to download and watch online TV and movies in the SIAT.

11. All regular employees ofthe SIAT must use the e-mail system with the domain name ofthe SIAT when they send/receive e-mails on business.

12. The e-mail system with the domain name of the SIAT is only applicable to the regular employees of the SIAT, and external cooperation units or companies are not allowed to use the such e-mail system. If it is really necessary for them to create the e-mailbox with the domain name of the SIAT due to work relations, it must be approved by the relevant departments and leaders of the SIAT before creating the e-mailbox and they should sign the relevant agreement.

13. It is forbidden to fraudulently use others' IP addresses or use unassigned IP addresses. The traffic cost arising from it should be paid by oneself.

14. Anyone are prohibited to publish any of the following information on the BBS:

(1) Violate the fundamental principles enshrined in the Constitution;

(2) Endanger national security, divulge state secrets, subvert state power or undermine national unity;

(3) Damage national honor and interests;

(4) Incite ethnic hatred, ethnic discrimination and undermine ethnic unity;

(5) Sabotages the state's religious policies and propagates cults and feudal superstitions;

(6) Spreading rumors, disturbing social order and undermining social stability;

(7) Spread pornography, gambling, violence, murder, terror information or instigation ofcrime;

(8) Insult or slander others or infringe upon the lawful rights and interests of others;

(9) Contain other contents prohibited by laws and administrative regulations.

15. Those who violate any ofthe above regulations will be given a punishment from suspending network and account use for 3 - 6 months to handing over to relevant department for legal accountability, depending on the severity of the circumstances and the impact and loss caused.

16. Any violation of any ofthe above regulations by others should be reported to the network administrator immediately.

17. Sending network equipment for repair outside the SIAT must be approved by the head of the equipment management department. Before sending for repair, the data stored in the equipment involving scientific research and information security or confidentiality should be backed up and deleted, and formatted by the network administrator, with confirmation by registration. The repaired network equipment should be accepted by the administrator, along with virus scanning, and registration before use.

18. The relevant personnel and users involved in the network ofthe SIAT must accept and cooperate with the supervision and inspection conducted by the relevant state departments as per laws.

Article 6: These Measures are interpreted by the Department of Science & Technology Development

Article 7: These Regulations should be implemented as of the data of promulgation

July 18, 2009