Measures for Security Protection Administration of the International Networking of Computer Information Networks

Full text

Chapter I General Provisions

Chapter II Security Protection Liability

Chapter III Security Supervision

Chapter IV Legal Liability

Chapter V Supplementary Provisions

(Approved by the State Council on December 11, 1997 and promulgated by

Decree No. 33 of the Ministry of Public Security on December 16, 1997)

Chapter I General Provisions

Article 1

These Measures are formulated in accordance with the provisions of the Regulations of the People's Republic of China for the Security Protection of Computer Information Systems, Interim Provisions of the People's Republic of China on the Administration of the International Networking of Computer Information Networks and other laws and administrative regulations with a view to strengthening the security protection of the International networking of computer information networks and maintaining public order and social stability.

Article 2

These Measures shall be applicable to the security protection administration of the international networking of computer information networks within the territory of the People's Republic of China.

Article 3

The agency of computer administration and supervision under the Ministry of Public Security shall be responsible for the work of security protection administration of the international networking of computer information networks.

Agencies of computer administration and supervision of public security organs should protect the public security of the international networking of computer information networks and safeguard the legitimate

rights and interests of units and individuals engaging in international networking businesses and public interest.

Article 4

No unit or individual shall use the international networking to endanger state security, divulge state secrets, nor shall it/he/she infringe on national, social and collective interests and the legitimate rights and interests of citizens, nor shall it/he/she engage in illegal criminal activities.

Article 5

No unit or individual shall use the international networking to produce, duplicate, search and disseminate the following information:

(1) Information that instigates the resistance and disruption of the implementation of the Constitution, laws and administrative regulations;

(2) Information that instigates the subversion of the state political power and overthrow of the socialist system;

(3)information that instigates the splitting up of the country and sabotage of national unity;

(4)information that instigates hatred and discrimination among nationalities and sabotages solidarity among nationalities;

(5)information that fabricates or distorts facts, spreads rumours and disrupts social order;

(6)information that propagates feudalistic superstitutions, obscenity, pornorgraphy, gambling, violence, murder and terror and instigates crimes;

(7)information that openly insults others or fabricates facts to slander others;

(8)information that damages the reputation of state organs; and

(9)other information that violates the Constitution, laws and administrative regulations.

Article 6

No unit or individual shall engage in the following activities endangering the security of computer information networks:

(1)access to computer information networks or use of computer information network resources without permission;

(2)deletion, revision or addition of computer information network functions without permission;

(3)deletion, revision or addition of the data and applied procedures in memory, processing or transmission in computer information networks without permission;

(4)deliberate production and spread of computer viruses and other disruptive programs;

(5)other activities that endanger computer information network security.

Article 7

Users' freedom of communication and communications secrecy are protected by law. No unit or individual shall use the international networking to infringe on users' freedom of communication and communications secrecy in violation of the provisions of law.

Chapter II Security Protection Liability

Article 8

Units and individuals engaging in the international networking businesses should accept security supervision, inspection and guidance of public security organs, truthfully provide relevant information, materials and documents on data to public security organs, and assist public security organs in investigating and handling illegal criminal acts through international networking of computer information networks.

Article 9

Supply units of international exit and entry channels, the competent departments or the competent units of internetworking units should in pursuance of the relevant provisions of law and the state, be responsible for the work of security protection of international exit and entry channels and the subordinate internetworking.

Article 10

Internetworking units, receiving units and legal persons and other organizations that use the international networking of computer information networks should fulfil the following security protection responsibilities:

(1)to be responsible for the work of security protection administration of the network and establish and perfect rules for security protection administration.

(2)to implement technical measures for security protection to ensure the operational security and

information security of the network;

(3)to be responsible for the security education and training of the users of the network;

(4)to register the units and individuals that entrust it to publish information and carry out scrutiny of the contents of the information provided in accordance with Article 5 of these Measures;

(5)to establish user registration and information management system of computer information network electronic announcement system;

(6)to preserve the relevant original records upon discovery of any of the circumstances listed in Articles 4, 5, 6 and 7 of these Measures and report to the local public security organ within 24 hours; and

(7)to delete the addresses and contents in the network containing contents of Article 5 of these Measures or close down the server in pursuance of relevant provisions of the state.

Article 11

A user should fill in the user record form when going through the formalities of access to the network at the receiving unit. The record form shall be made under the supervision of the Ministry of Public Security.

Article 12

Internetworking units, receiving units, legal persons and other organizations that use the international networking of computer information networks(including cross-province, cross-autonomous region and cross-municipality directly under the Central Government internetworking units and their susbordinate branches) should, within 30 days starting from the date of formal hooking up of the network, go through the formalities for the record at the processing agencies designated by the public security organs of people's governments of the provinces, autonomous regions and municipalities directly under the Central Government wherein the units are located.

The units listed in the preceding paragraph shall be responsible to report the information on the receiving units and users hooked up to the network to local public security organs and report in time changes in the receiving units and users of the network.

Article 13

Registrants that use public account numbers should strengthen the management of the public account numbers and establish the registration system of account number use. No user account number shall be lended or transferred.

Article 14

The units involving such important fields as state affairs, economic construction, national defense construction, highly sophisticated science and technology and others shall, while going through the

formalities for the record, present the proof of examination and approval of its competent administrative department.

Corresponding security protection measures shall be taken in the computer information networks and international networking of units listed in the preceding paragraph.

Chapter III Security Supervision

Article 15

Public security departments(bureaus) of the provinces, autonomous regions and municipalities directly under the Central Government should have correspondidng agencies to be responsible of the work of security protection administration of international networking.

Article 16

Computer administration and supervision agencies of public security organs should keep themselves abreast of the record information of the networking units, receiving units and users, establish record files, make record statistics and report level by level in accordance with relevant state provisions.

Article 17

Computer administration and supervision agencies of public security organs should supervise and urge the networking units, receiving units and relevant users to establish and perfect the security protection administration system, supervise and inspect the state of implementation of network security protection administration and the technical measures.

While computer administration and supervision agencies of public securityorgans organize security inspections, the units concerned should dispatch persons to participate. Computer administration and supervision agencies of public security organs should come up with suggestions for improvement with respect to problems discovered in security inspections and make detailed minutes for the file for future reference.

Article 18

Computer administration and supervision agencies of public security organs should notify the units concerned to close down or delete them on the discoery of the addresses, contents or servers listed in Article 5 of these Measures.

Article 19

Computer administration and supervision agencies of public security organs should be responsible to keep track of and investigate and handle the illegal acts through computer information networks and

criminal cases directed against computer information networks, and should transfer the cases to the departments concerned or the judicial organs for handling in pursuance of relevant state provisions with respect to illegal criminal acts stipulated in Article 4 and Article 7 of these Measures.

Chapter IV Legal Liability

Article 20

Whoever commits any of the acts listed in Articles 5 and 6 of these Measures in violation of laws and administrative regulations shall be administered a warning by the public security organ; where there is illegal gains, the illegal gains shall be confisticated, a fine of less than RMB 5,000 Yuan may concurrently be imposed on an individual and a fine of less than RMB 15,000 Yuan may concurrently be imposed on a unit; where the circumstances are serious, the penalty of suspension of networking and computers for consolidation within 6 months may concurrently be imposed, and when necessary a proposal may be sent to the original licensing, examination and approval authority to revoke the business license or nullify the networking qualifications; where acts in violation of public security administration has been constituted, penalties shall be imposed in pursuance of the regulations for public security administration penalties; where a crime has been constituted, criminal liability shall be investigated in accordance with law.

Article 21

Whoever commits any of the following acts shall be orderedby the public security organ to make a rectification within the specified time period, administered a warning and confisticated of the illegal gains where there is illegal gains; where no rectification has been made within

the specified time period, the person-in-charge and other persons directly responsible of the unit may be imposed a fine of less than RMB 5,000 Yuan, and a fine of less than RMB 15,000 Yuan may concurrently be imposed on the unit; where the circumstances are serious, the penalty of suspension of networking and shutting down of computers for consolidation within 6 months may be imposed, when necessary a proposal may be sent to the original licensing, examination and approval authority to revoke the business license or nullify the networking qualifications.

(1)failure to establish rules for security protection administration;

(2)failure to take technical protective measures for security;

(3)failure to conduct security education and training of network users;

(4)failure to provide information, materials and data documents required for security protection administration or the contents provided are untrue;

(5)failure to carry out scrutiny of the contents of the information entrusted for publication or failure to

register the entrusting units or individuals;

(6)failure to establish user registration and information management system for electronic announcement systems;

(7)failure to delete the website addresses, contents or shut down the servers in pursuance of relevant state provisions;

(8)failure to establish the registration system for the use of public account numbers; and

(9)lending and transfer of user account numbers.

Article 22

Whoever violates the provisions of Articles 4 and 7 of these Measures shall be imposed a penalty in pursuance of the relevant laws and regulations.

Article 23

Whoever fails to fulfill the responsibilities of putting on record in violation of the provisions of Articles 11 and 12 of these Measures shall be administered a warning or imposed a penalty of shutting down the computers for consolidation not exceeding 6 months by the public security organ.

Chapter V Supplementary Provisions

Article 24

Security protection administration of computer information networks hooked up with the Hong Kong Special Administrative Regions and the regions of Taiwan and Macau shall be implemented with reference to these Measures.

Article 25

These Measures shall enter into force as of December 30, 1997.