CHINESE LAW AND GOVERNMENT
2016, VOL. 48, NO. 1, 60–64
http://dx.doi.org/10.1080/00094609.2015.1048136

Routledge
Taylor & Francis Group

Regulations for the Protection and Management of the International Networking of Computer Information Networks

Approved by the State Council on December 11, 1997, promulgated by Order No. 33 of the Ministry of Public Security on December 16, 1997, and revised in accordance with the Decision of the State Council on Annulling and Revising a Number of Administrative Regulations, of January 8, 2011.

Chapter 1. General provisions

Article 1. These regulations are formulated, according to the Regulations on Protecting the Security of the Computer Information System of the People's Republic of China, the Interim Provisions on Management of the International Networking of Computer Information Networks of the People's Republic of China, and other laws and administrative regulations, in order to strengthen the security and protection of the computer information network and the Internet.

Article 2. These regulations apply to the security and protection management of international networking of computer information networks within the borders of the People's Republic of China.

Article 3. The computer management and monitoring agencies of the Ministry of Public Security are responsible for the security and protection management work of international networking of computer information networks.

The computer management and monitoring agencies of the Ministry of Public Security shall protect the public safety of the international networking of computer information networks, and shall safeguard the lawful rights and interests of the entities and individuals engaged in the business of international network connection and the public interest.

Article 4. No entity or individual is allowed to use the international network connections to harm state security or leak state secrets, or violate the interests of the state, society, and the collective, and the lawful rights and interests of individuals, or engage in unlawful or criminal activities.

Article 5. No entity or individual may use international network connections to create, copy, access, or disseminate the kind of information as set forth below:

1. information that instigates resistance to and undermining of the constitution or the implementation of laws and administrative regulations;

2. information that instigates the subversion of state power and overthrowing of the socialist system;
3. information that instigates splitting the country and undermining national unity;
4. information that instigates ethnic hatred or ethnic discrimination or undermines ethnic solidarity;
5. information that fabricates or distorts facts, spreads rumors, and disturbs social order;
6. information that promotes feudal superstitions, obscenities, pornography, gambling, violence, murder, and terror or incites crimes;
7. information that publicly defames others or fabricates facts to slander others;
8. information that damages the reputation of state organs; or
9. information that in other ways violates the constitution, laws, and administrative regulations.

Article 6. No entity or individual may engage in the acts harmful to computer information and network security as set forth below:

1. acts that, without permission, access computer information networks or use computer information and network resources;
2. acts that, without permission, delete, modify, or add to the functions of computer information networks;
3. acts that, without permission, delete, modify, or add to the data or applications stored, handled, or transmitted by computer information networks;
4. acts that deliberately create or transmit computer viruses and other destructive programs; and
5. other acts that compromise the security of computer information networks.

Article 7. The freedom and privacy of correspondence of users is protected by law. No entity or individual may violate laws or regulations by using international networking of networks to infringe on the freedom and privacy of users' correspondence.

Chapter 2. Responsibility for security and protection

Article 8. Entities and individuals that engage in the international networking business shall accept safety supervision, inspection, and guidance by public security organs, truthfully provide public security organs with information, data, and data files, and assist public security organs in their investigations of unlawful and criminal acts committed by means of international networking of computer information networks.

Article 9. International information gateway channel providers and departments or entities in charge of interconnection units shall be responsible for the security and protection management of international networking of information gateway channels within their jurisdictions in accordance with the provisions of laws and the relevant state regulations.

Article 10. Interconnection units, access units, and legal persons and other organizations that use international networking of computer information networks shall fulfill the following security functions:

1. take responsibility for the safety and protection management work of their own networks, and set up and perfect security and protection management systems;
2. carry out security and protection technical measures and ensure the safety of their own network operations and information;
3. take responsibility for the security education and training of their network users;
4. conduct registrations of the entities and individuals that commission the issuance of information, and conduct reviews of the contents of the information they provide in accordance with Article 5 of these regulations;
5. set up a system for registration of the users of computer information network electronic bulletin boards as well as an information management system;
6. preserve the relevant original records when any of the circumstances listed in Article 4, Article 5, Article 6, and Article 7 of these regulations are discovered, and report to the local public security organ with twenty-four hours; and
7. in accordance with the relevant state regulations, delete the addresses and directories in their own networks that contain the elements specified by Article 5 of these regulations, or shut down the servers.

Article 11. When users conduct access procedures with access units, they should fill out user for-the-record forms. The for-the-record forms will be produced under the supervision of the Ministry of Public Security.

Article 12. Interconnection units, access units, legal persons that use international networking of computer information networks (including the network interconnection units and their subsidiary agencies in provinces, autonomous regions, and municipalities directly administered by the central government) should, within thirty days after being officially connected, proceed to the acceptance agencies designated by the people's government public security authority of the province, autonomous region, or directly administered municipality in which they are located to file procedures for the record.

The units listed in the preceding paragraph should be responsible for reporting the circumstances of the access units connected with their own networks to the local public security organ for the record, and should promptly report any changes in the circumstances of network access units and users.

Article 13. Registrants that use public accounts should strengthen the management of public accounts and establish an account registration system. User accounts may not be lent or transferred to others.

Article 14. When entities that involve national affairs, economic construction, national defense construction, cutting-edge science and technology file procedures for the record, evidence of the approval of the relevant supervisory authorities should be shown.

Appropriate safety and protection measures should be taken when the computer information networks listed in the preceding paragraph are connected with international networks.

Chapter 3. Security oversight

Article 15. The public security divisions (bureaus) of provinces, autonomous regions, and directly administered municipalities and the public security bureaus of prefectures (municipalities) and counties (cities) should have appropriate institutions in charge of security and protection management work for international network connections.

Article 16. The computer management and supervision agencies of public security organs should have information on the interconnection units, access units, and users' registrations for the record. They should set up a filing system for this information, compile statistics thereof, and submit these, level by level, to the higher authorities in accordance with the relevant state regulations.

Article 17. The computer management and supervision agencies of public security organs should urge interconnection units, access units, and the relevant users to set up and perfect security and protection management systems, and should monitor and inspect the implementation of network safety, protection management, and technical measures.

When the computer management and supervision agencies of public security organs organize security checks, the relevant entities should send staff to participate. When any problems are found by the security checks, the computer management and supervision agencies of public security organs should make suggestions for improvements, make detailed records, and archive these for future reference.

Article 18. When the computer management and supervision agencies of public security organs find addresses, directories, or servers that contain the elements listed in Article 5 of these regulations, they should notify the relevant entities to shut these down or delete them.

Article 19. The computer management and supervision agencies of public security organs should be responsible for tracking and dealing with unlawful acts committed by means of computer information networks and criminal cases involving computer information networks, and should, in accordance with the relevant state regulations, transmit the unlawful and criminal acts that violate the provisions of Article 4 and Article 7 of these regulations to the relevant departments or judicial organs for processing.

Chapter 4. Legal liabilities

Article 20. If there are any one of the acts in violation of laws or administrative regulations as set forth in Article 5 and Article 6 of these regulations, public security organs will issue warnings and, if there are illegal gains, will confiscate the illegal gains and may concurrently impose fines of not more than 5,000 yuan in the case of individuals or fines of not more than 15,000 yuan in the case of work entities; if the circumstances are serious, they may also impose the penalties of suspending network connections for a period of no more than six months and closing down computer operations for the making of corrections, and when necessary, may suggest to the original permit-issuing and review-and-approval agencies that the perpetrators' business permits be revoked or their networking qualifications cancelled. If the acts constitute violations of public order administration,

these shall be handled in accordance with the provisions of the Law on Public Order Administration Punishments, and if they constitute crimes, the perpetrators shall be pursued by law for criminal liability.

Article 21. For any one of the acts set forth below, public security organs shall order corrections within set time limits, issue warnings, and confiscate illegal gains if these have been obtained. If corrections have not been made within the set time limits, fines of not more than 5,000 yuan may be concurrently imposed in the case of the directly responsible persons in charge and other directly responsible persons, and fines of not more than 15,000 yuan may be concurrently imposed in the case of work entities; if the circumstances are serious, they may also impose the penalties of suspending network connections for a period of no more than six months and closing down computer operations for the making of corrections, and when necessary, may suggest to the original permit-issuing and review-and-approval agencies that the perpetrators' business permits be revoked or their networking qualifications canceled:

1. if security and protection management systems have not been set up;
2. if security technology protective measures have not been adopted;
3. if network users have not undergone education or training;
4. if the information, data, and data files required for security and protection management have not been provided, or if the contents provided are untruthful;
5. if the contents of the information entrusted for publication have not been examined and approved or the entrusting entity or individual has not undergone registration;
6. if systems for the registration of electronic bulletin board users or for information management have not been set up;
7. if network addresses or directories have not been deleted or servers shut down in accordance with the relevant state regulations;
8. if systems for the use and registration of public account numbers have not been established; and
9. if user account numbers have been lent out or transferred.

Article 22. If the provisions of Article 4 and Article 7 of these regulations have been violated, penalties shall be imposed in accordance with the relevant laws and regulations.

Article 23. If, in violation of the provisions of Article 11 and Article 12 of these regulations, the duty and responsibility of filing for the record have not been performed, the public security organs shall issue warnings to the perpetrators or punish them by suspending computer operations for their rectification for periods of time not to exceed six months.

Chapter 5. Supplementary provisions

Article 24. Security and protection management of computer information networks connected with the Hong Kong Special Administrative Region and the Taiwan and Macau regions shall be implemented with reference to these measures.

Article 26. These regulations shall be implemented as of December 30, 1997.