

Regulations on the Safety Protection of Computer Information Systems of the PRC

Dan Young Business Consultancy — www.danyoungcpa.com
Unofficial English translation prepared for reference only. The official Chinese text prevails.

Contents

Table of Contents	1
Chapter I — General Provisions	1
Chapter II — Protection of the Security of Computer Information Systems	2
Chapter III — Legal Liability	3
Chapter IV — Supplementary Provisions	4

Promulgated by Decree No. 147 of the State Council of the People's Republic of China on February 18, 1994
Effective: February 18, 1994

Amended in accordance with the Decision of the State Council on Abolishing and Amending Certain Administrative Regulations on January 8, 2011

Table of Contents

- Chapter I — General Provisions
- Chapter II — Protection of the Security of Computer Information Systems
- Chapter III — Legal Liability
- Chapter IV — Supplementary Provisions

Chapter I — General Provisions

Article 1 — These Regulations are formulated for the purposes of protecting the security of computer information systems, promoting the application and development of computers, and safeguarding the smooth progress of the socialist modernization drive.

Article 2 — For the purposes of these Regulations, "computer information system" means a system consisting of computers and their ancillary and peripheral equipment and facilities (including networks) that collects, processes, stores, transmits, and retrieves information in accordance with certain application objectives and rules.

Article 3 — The security protection of computer information systems shall safeguard the security of computers and their ancillary and peripheral equipment and facilities (including networks), the security of the operating environment, the security of information, and the normal functioning of computer functions.

Article 4 — The security protection of computer information systems shall be the key focus of the Ministry of Public Security in the national public security work. The national public security organs shall be responsible for the security protection of computer information systems nationwide. The national security organs, the state secrecy organs, and other relevant departments of the State Council shall, within their respective scopes of duties as prescribed by the State Council, carry out the work relating to the security protection of

computer information systems.

Article 5 — The security protection of computer information systems in any work unit within the territory of the People's Republic of China shall be governed by these Regulations. The security protection of computer information systems not connected to the Internet shall be governed by separate provisions.

Article 6 — The security protection of computer information systems in any work unit shall be managed under the principle of "whoever uses the system shall be responsible for its security." The competent department of the industry to which a computer information system belongs shall be the administrative authority in charge of the industry for the security protection of such computer information system.

Chapter II — Protection of the Security of Computer Information Systems

Article 7 — Any work unit's computer information system shall undergo a security level classification and a security protection level assessment. The specific measures for the security level classification and assessment of computer information systems shall be separately formulated by the Ministry of Public Security in conjunction with other relevant departments.

Article 8 — The construction and application of a computer information system shall comply with the requirements of the security level classification and security protection level of such system. The construction of a computer information system shall be carried out simultaneously with the design, construction, and use of the security protection facilities.

Article 9 — The security protection of a computer information system shall adopt security protection technologies and measures that comply with the relevant national standards and industry standards.

Article 10 — For a computer information system that is required to undergo a security assessment or security testing in accordance with the law, the security assessment and security testing shall be conducted by qualified testing and assessment institutions or specialized technical institutions. The specific measures shall be formulated by the Ministry of Public Security in conjunction with other relevant departments of the State Council.

Article 11 — A computer room of a computer information system shall comply with the relevant national standards and the relevant provisions of the State. In the vicinity of a computer room, no facilities that may pose a hazard to the security of the computer information system may be constructed, installed, or used. No work unit or individual may engage in any activity that endangers the security of a computer information system.

Article 12 — The operator of a computer information system shall establish and improve the security management system, be responsible for the security protection of the computer information system, designate the persons responsible for security management, provide necessary security protection conditions, periodically carry out security inspections and risk assessments, promptly address potential security hazards, formulate contingency plans for emergency response, and conduct emergency drills on a regular basis.

Article 13 — Where a computer information system is connected to an international network, the operator shall file a record with the public security organ of the people's government of the province, autonomous region, or municipality directly under the Central Government at the place where the operator is located within 30 days from the date of establishment of the network connection.

Article 14 — The operator of a computer information system shall, in accordance with the law, retain network logs for not less than six months. The public security organs may, in the course of performing their duties of supervising and inspecting the security protection of computer information systems in accordance with the law, consult the network logs and the relevant materials.

Article 15 — Where a security incident occurs in a computer information system, the operator shall take emergency measures promptly, retain the relevant data, and report the incident to the local public security organ of the people's government at or above the county level within 24 hours.

Article 16 — The operator of a computer information system shall adopt protective measures against computer viruses and network attacks, such as classification management, authorization management, verification of identity, and encrypted transmission.

Article 17 — No work unit or individual may, without the consent of the operator of a computer information system, access, delete, modify, or add to the functions of the computer information system, or delete, modify, or add to the data and application programs stored, processed, or transmitted in the computer information system. No work unit or individual may intentionally create or disseminate computer viruses or other destructive programs.

Article 18 — The transport, carrying, or mailing of computer information media into or out of the territory of China shall be subject to declaration to the customs authorities in accordance with the law.

Chapter III — Legal Liability

Article 19 — Where an operator of a computer information system violates the provisions of these Regulations by committing any of the following acts, the public security organ shall give it a warning or order it to suspend the use of the computer information system for a specified period of time; and where the circumstances are serious, a fine of not less than RMB 5,000 yuan and not more than RMB 15,000 yuan may be imposed; and where the illegal income exceeds RMB 5,000 yuan, a fine of not less than one time and not more than three times the illegal income may be imposed; and where it constitutes a violation of public security administration, penalties shall be imposed in accordance with the provisions of the Law on Penalties for Administration of Public Security; and where a crime is constituted, criminal liability shall be investigated in accordance with the law: (1) failing to adopt security protection measures or failing to adopt security protection measures that comply with the relevant national standards and industry standards; (2) failing to conduct security assessments or security testing for the computer information system; (3) failing to file a record in accordance with the provisions; (4) failing to retain network logs in accordance with the provisions; (5) failing to report a security incident in accordance with the provisions; or (6) failing to comply with other provisions on the security protection of computer information systems.

Article 20 — Where the operator of a computer information system violates the provisions of these Regulations, the public security organ may impose penalties in accordance with the provisions of Article 19 of these Regulations on the directly responsible person in charge and other directly liable persons; and where the circumstances are serious, it may be recommended that the work unit impose disciplinary action on the relevant responsible persons.

Article 21 — Where a person, in violation of the provisions of these Regulations, commits any act endangering the security of a computer information system, which constitutes a violation of public security administration, penalties shall be imposed in accordance with the provisions of the Law on Penalties for Administration of Public Security; and where a crime is constituted, criminal liability shall be investigated in accordance with the law.

Article 22 — Where a computer information system is harmed as a result of a failure to perform the security protection obligations in accordance with the provisions of these Regulations, the operator shall bear corresponding liability in accordance with the law.

Article 23 — Where a functionary of a public security organ neglects his or her duties, abuses his or her power, or engages in malpractices for personal gain, disciplinary action shall be imposed in accordance with the law; and where a crime is constituted, criminal liability shall be investigated in accordance with the law.

Chapter IV — Supplementary Provisions

Article 24 — The security protection of computer information systems used for matters of national defense or State secrets shall be governed by the relevant laws and regulations of the State.

Article 25 — The specific meanings of the following terms as used in these Regulations are: (1) "computer virus" means a set of computer instructions or program codes that are compiled or inserted into a computer program, which destroy computer functions or data, affect computer use, and are capable of self-replication; and (2) "operator of a computer information system" means the owner and the administrator of a computer information system.

Article 26 — The Ministry of Public Security shall be responsible for the interpretation of these Regulations.

Article 27 — These Regulations shall come into force on the date of promulgation.

Disclaimer: This English translation is provided for reference and informational purposes only. It is not an official translation and has no legal effect. While every effort has been made to ensure accuracy, the original Chinese text promulgated by the State Council of the People's Republic of China shall prevail as the authoritative version. Dan Young Business Consultancy makes no warranty, express or implied, as to the accuracy, completeness, or fitness for any particular purpose of this translation. Users should consult qualified legal professionals for advice on specific legal matters. This translation does not create any attorney-client or advisory relationship.