Safety Management System of Shenzhen Institute ofAdvanced Technology, Chinese Academy of Sciences on the Server Room

I. Rules for Daily Behavior in the Server Room

1. Environmental hygiene must be observed. Eating, smoking, and spitting are prohibited in the server room. In case of accidental spills or stains on the server room floor or other items during work, measures must be taken promptly to clean them and maintain a dust-free and clean environment in the server room.

2. Personal hygiene must be maintained. Personnel shall present themselves neatly, speak politely, and behave appropriately.

3. Items in the server room shall be properly arranged and not placed randomly.

4. Personnel shall take turns to be on duty in the server room, responsible for daily cleaning and behavioral supervision in the server room.

5. Shoes must be changed as required when entering or exiting the server room, and rain gear, shoes, and other items shall be neatly placed in their designated locations.

6. Check the sun protection, waterproofing, and moisture-proofmeasures in the server room, maintain good ventilation, be aware ofthe impact ofweather conditions on the server room, and promptly inspect and close windows, check drainage, and ventilation facilities on rainy days.

7. Within the server room, loud noise shall be avoided, and attention shall be paid to controlling noise/sound volume to maintain a quiet working environment.

II. Safety System for the Server Room

1. Ensure that the anti-theft door is securely locked when entering or exiting the server room. For guests entering or exiting the server room, relevant personnel ofthe server room shall be responsible for their safety and security. Personnel leaving the server room must conscientiously check and close all doors and windows, and lock anti-theft devices. Refuse entry ofunfamiliar individuals into the server room.

2. Before leaving the work area, personnel shall ensure that important documents, materials, equipment, and data in the work area are securely protected, check and lock their workstations, lock their work computers, and securely store important documents and data on their desktops, etc.

3. Personnel and visitors must register when entering or exiting.

4. Outsiders entering the server room must be fully supervised by designated personnel to ensure their safety.

5. The disclosure ofserver room related keys or passwords to others without the approval of principal leaders is prohibited, and individuals are responsible for maintaining information confidentiality. Lost items must be reported immediately, and proactive measures must be taken to ensure the safety ofthe server room.

6. Server room personnel are responsible for promptly identifying and suggesting improvements for any vulnerabilities or deficiencies in the server room safety system.

7. It is prohibited to allow individuals unrelated to server room operations to enter or exit the server room.

8. Direct or indirect manipulation of any equipment in the server room by individuals unrelated to server room operations is strictly prohibited.

9. In the event of serious incidents such as theft, forced entry, fire alarms, flooding, or 110 emergency calls, server room personnel are obliged to arrive at the scene as quickly as possible and assist in handling the situation.

III. Electrical Safety System for the Server Room

1. Server room personnel shall learn regular electrical safety operations and knowledge, understand the operation procedures of the power supply and electrical facilities inside the server room.

2. Server room personnel shall regularly practice and master emergency procedures, measures, and essentials for server room electricity use.

3. Qualified personnel shall be arranged to conduct regular inspections of power supply and electrical equipment and facilities in the server room.

4. Unauthorized wiring or connections are not allowed, and safe and guaranteed power supply and electrical equipment shall be used.

5. Before actually connecting the equipment to the power supply, check whether the lines, connectors are safely connected, whether the equipment is ready, and whether personnel have safety protection.

6. It is strictly forbidden to randomly power off equipment or change equipment power supply lines. It is also forbidden to randomly connect, connect in series, or overlap various power supply lines.

7. If electrical safety hazards are discovered, measures shall be taken immediately to resolve them. If they cannot be resolved, relevant responsible personnel must be informed promptly.

8. Server room personnel are responsible for their personal electrical safety. External personnel needing electricity must obtain permission from server room management personnel and use the safest and least impactful power supply method for server room equipment.

9. Server room personnel shall check and ensure the electrical safety of the work environment before leaving.

10. The last staff member leaving the server room must check all electrical equipment, and any electrical equipment that may cause serious consequences if left operating for a long time shall be turned off.

11. It is prohibited to use high-temperature, hot, or spark-producing electrical equipment in the server room without supervision.

12. Prior approval from higher-level supervisors must be obtained before using electrical equipment with power ratings exceeding specific wattages, and such equipment shall be used on circuits with proper fuses.

13. Appropriate safety operation methods, warnings, and instructions shall be posted at high-risk locations, and they shall be strictly followed during practical operations.

14. In the event of an external power system outage, server room personnel shall fully cooperate to complete emergency power outage work.

15. Attention shall be paid to saving electricity.

IV. Fire Safety System for the Server Room

1. Server room personnel shall be familiar with the internal fire safety operations and regulations of the server room, understand the operation principles of fire equipment, and master emergency procedures, measures, and essentials for fire safety.

2. No one is allowed to change the working status of the fire system or the location of equipment arbitrarily. Approval from principal leaders must be obtained for any changes to the working status of the fire system and the location of equipment. Personnel shall protect fire equipment from damage.

3. Regular fire drills, fire safety knowledge training, and fire equipment use training shall be conducted.

4. If fire safety hazards are discovered, measures shall be taken immediately to resolve them. If they cannot be resolved, relevant responsible personnel must be informed promptly.

5. Strict compliance with operation and safety warnings and instructions posted at appropriate locations is required.

6. The last staff member leaving the server room shall check the working status of the fire equipment, turn off equipment that may pose a fire hazard, and take measures to ensure fire safety in an unattended state.

V. Water Usage System for the Server Room

1. Installation of water supply pipelines and facilities in the server room is prohibited.

2. Adherence to safety operations, warnings, and safety guidelines posted at appropriate locations is required.

VI. Hardware Equipment Use Safety System for the Server Room

1. Server room personnel must be familiar with the basic safety operations and rules of equipment in the server room.

2. Regular inspection and organization of hardware physical connection lines shall be conducted, and the operating status of hardware (such as equipment indicator lights, instruments) shall be checked regularly. Self-check reports on hardware operation shall be reviewed regularly to promptly understand the operating status of hardware.

3. Moving equipment arbitrarily, installing or disassembling hardware, changing equipment wiring arbitrarily, and resetting hardware arbitrarily are prohibited.

4. Experimental configuration operations on servers are prohibited. Configuration of servers shall be tested and confirmed on other testable machines before being accurately configured on servers.

5. Changes or debugging operations that will affect the overall hardware equipment shall be notified in advance, and there shall be sufficient time, plans, and personnel preparation before making changes to hardware equipment.

6. For changes in major equipment configuration, a scheme document must be formulated first. After discussion and confirmation of feasibility, qualified technical personnel can make changes and adjustments, and detailed records of changes and operations shall be made. Before making changes, upgrades, or configurations to equipment, sufficient preparations shall be made for the negative consequences of the

changes, upgrades, or configurations. If necessary, backup parts and emergency measures shall be prepared in advance.

7. No one is allowed to perform any operations unrelated to their scope ofwork on core equipment such as servers and switching equipment. Without permission from superiors, let alone others, no one is allowed to operate equipment inside the server room. For adjustments and configurations ofcore servers and equipment, the consent ofthe team members is required before proceeding.

8. Attention shall be paid to implementing maintenance and upkeep measures for hardware equipment.

VII. Software Use Safety System

1. Regular checks of software operation status and regular review of software operation logs shall be conducted, and data and software logs shall be backed up.

2. Experimental software debugging on servers is prohibited, and installing software on servers at will is also prohibited. Configuration of servers must be tested and confirmed on other testable machines before accurate configuration on servers.

3. Notices shall be issued in advance for software changes or debugging operations that will affect the overall system, and there shall be sufficient time, plans, and personnel preparation before making software configuration changes.

4. For changes in major software configuration, a scheme document must be formulated first. After discussion and confirmation of feasibility, qualified technical personnel can make changes, and detailed records of changes and operations shall be made. Before making changes, upgrades, or configurations to software, sufficient preparations shall be made for the negative consequences of the changes, upgrades, or configurations. If necessary, the original software system shall be backed up, and emergency measures shall be implemented.

5. No one is allowed to conduct software debugging and operations unrelated to their scope of work on core equipment such as servers. Without permission from superiors, leading or instructing others to enter the server room and make changes or operations to the network and software environment is not allowed.

VIII. Server Room Data, Document, and Data Safety System

1. Data, documents, and other information must be effectively organized, sorted, and archived.

2. No one is allowed to provide information, documents, data, configuration parameters, or any information from the server room to other unrelated individuals or disseminate them externally.

3. Important information, passwords, documents, and data related to network security and data security must be stored properly. If external personnel need to access documents, data, or retrieve related data, they must be checked by relevant personnel in the server room, and only data or documents related to their current work shall be provided to them.

4. Encryption, storage, and backup shall be carried out using appropriate technical means for important data, documents, and data. Encrypted data shall be ensured to be reversible to prevent loss of important data.

IX. Property Registration and Protection System for the Server Room

1. Daily items, equipment, consumables, etc., in the server room must have clear quantity and model registration records. For items and important equipment for public use, a relatively complete borrowing and return system must be established for management.

2. Server room personnel have the obligation to safely and carefully use any equipment, instruments, or other items in the server room. After use, items shall be returned to their original places and not placed arbitrarily.

3. Damaged, consumed, or lost items during use shall be reported and registered, and relevant responsible persons shall be held accountable.

4. Without the consent ofprincipal leaders, server room equipment and items are not allowed to be loaned or provided to others.

X. Team Spirit and Collaboration

1. Members ofthe server room workgroup shall foster a spirit ofteamwork.

2. Any matter that will affect the work and arrangements of other personnel, or require coordination with other staff members, shall be proposed and coordinated in advance. The practice of acting independently is prohibited.

3. Work division shall be clear, responsibilities shall be defined, work plans shall be clear, and work summaries shall be specific.

4. Group members have an obligation to follow work arrangements and to propose more rational suggestions and opinions on work arrangements.

5. A democratic and collaborative work environment shall be fostered. Any individual has the right and obligation to organize and contact other group members, principal leaders, etc., to conduct discussions, hold meetings, promptly address issues, communicate with each other, and collaborate.