Management System of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences on Operation, Maintenance, and Management of the Archive Information System

Chapter 1 General

Article 1 To ensure the safety management of the Institute's archive information system, this System is specially formulated.

Article 2 The archive information system referred to in this System refers to the information management systems used for archive business, including archive information management systems, archive information service systems, and archive office systems.

（1） The archive information management system includes archive catalog management systems, digital archive reception systems, digital archive management systems, archive digitization processing systems, etc.;

（2） The archive information service system includes archive utilization service systems, archive website systems, etc.;

（3） The archive office system includes SIAT's office business system responsible for archive work management.

Article 3 The safety referred to in this System includes two aspects: archive information safety and system service safety. Archive information safety ensures the authenticity, integrity, and availability of information within the archive information system, while system service safety ensures that the information system can provide services in a timely and effective manner.

The scope of safety management includes account and key management, risk assessment, emergency response, disaster recovery, etc.

Chapter 2 Account and Key Management

Article 4 Accounts refer to user accounts at both the system level (operating system, database, firewall, and other network devices) and the application level.

Keys refer to the encryption technology applied to the archive information system, which effectively supervises the system and information.

Article 5 System administrators are responsible for the unified distribution and management of system accounts and keys and must keep records.

Each user shall be assigned a unique account and key for each system and must not share or borrow accounts and keys. Account names shall not reveal user permission information.

Article 6 In accordance with the principle of "who uses, who is responsible", users shall ensure the safety of their accounts and keys.

Article 7 If an account or key is found lost or compromised, it shall be reported to the system administrator immediately, who shall then immediately stop the use of the account or key and investigate the cause.

Chapter 3 Risk Assessment

Article 8 Risk assessment involves analyzing the threats and vulnerabilities faced by the network and information systems, assessing the potential harm caused by safety incidents, and proposing targeted protective measures and corrective actions.

Article 9 Risk assessment work shall follow the principles of "strict organization, standardized operation, scientific rigor, and practical effectiveness".

Article 10 Risk assessment can be conducted in the form of self-assessment or inspection assessment. Self-assessment or inspection assessment can be carried out by internal technical forces or entrusted to third-party organizations.

Article 11 Conducting information safety level protection grading is the main method of archive information system risk assessment.

Article 12 The safety level protection grading for archive information systems shall be carried out in accordance with the requirements of independent grading, key protection, dynamic protection, and synchronous construction.

Chapter 4 Physical Environment

Article 13 Emergency response shall strictly follow the *Management System of the Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences on Contingency Plan*.

Chapter 5 Disaster Recovery

Article 14 Disaster recovery refers to the process of reactivating system data, hardware, and software devices after a disaster to restore the normal operation of the information system.

Article 15 Disaster Recovery Strategy

Data Recovery Strategy: When system data encounters problems, use the latest backup data to restore the system data;

System Recovery Strategy: When the system encounters problems, reinstall and deploy the system based on backup system installation resources, and then combine the data backup strategy to restore the system data with the latest backup data;

Power Recovery Strategy: If the external power supply system is scheduled to be cut off, preparations shall be made in advance, and the generator shall be started in time. If the generator cannot supply power normally, server room personnel of the technical department shall be notified promptly, and corresponding protection measures shall be taken. Gradually shut down the load equipment to extend the UPS power supply time until all load equipment is shut down;

Disaster Recovery Strategy: In the event of environmental damage to the system environment, rebuild the system equipment and other environments. Then, reinstall and deploy the system based on the backup system installation resources, and restore the system data with the latest backup data.

Article 16 Backup and recovery of servers, storage devices, network devices, and important data are the responsibility of the technical department. Backup and recovery of file data managed by departments and individuals are the responsibility of the respective departments and individuals.

Article 17 Backup data and media shall be strictly managed and properly preserved.

Article 18 Regular system disaster recovery drills shall be conducted, including backup data recovery, system recovery, fault troubleshooting, etc., to ensure that relevant personnel are clear about their tasks.

Chapter 6 Bylaw

Article 19 This System is interpreted by Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences.

Article 20 This System shall be implemented from the date ofpromulgation.