Document of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences

SYKZI [2019] No. 137

Notice of Shenzhen Institute ofAdvanced Technology, Chinese Academy of Sciences on Issuance of the *Management Measures of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences on Cybersecurity*

All units (department) ofthe SIAT:

To strengthen the cybersecurity construction ofthe SIAT, standardize the use of network information resources, the *Management Measures of Shenzhen Institute Of Advanced Technology, Chinese Academy of Sciences on Cybersecurity has been formulated*, which was deliberated and approved at 2nd Institute Administrative Affairs Meeting in 2019, it is hereby issued. Please comply and execute accordingly.

Shenzhen Institute ofAdvanced
Technology, Chinese Academy of
Sciences

November 1, 2019

Attachment: Management Measures of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences on Cybersecurity

Public Finance Department of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences Issued on November 8, 2019

Management Measures of Shenzhen Institute ofAdvanced Technology, Chinese Academy of Sciences on Cybersecurity

Chapter 1 General .

Article 1 To strengthen the cybersecurity work of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences (SIAT), safeguard the cybersecurity of SIAT, according to the related laws, regulations, policies, and guidance document, such as the *Cybersecurity Law of the People 's Republic of China*, the *Provisional Regulations of the People 's Republic of China on the Administration of the International Networking of Computer Information Networks*, the *Management Measures of Chinese Academy of Sciences on Cybersecurity Work* (Trial), these Measures are hereby formulated.

Article 2 The cybersecurity work ofthe SIAT follows the principle of "the managers, users, and O&M personnel should take corresponding responsibilities", implementing centralized leadership, hierarchical governance, and individual-assigned responsibility.

Article 3 The cybersecurity should be synchronously planned, constructed, implemented, and developed with informatization work.

Article 4 The cyber in these Measures refers to a system composed of computers or other information terminals and related equipment that collects, stores, transmits, exchanges and processes information according to certain rules and procedures.

The cybersecurity refers to the capabilities preventing network from attack, intrusion, interference, sabotage, illegal use, and accidents by taking necessary measures to keep the network in a stable and reliable operation status and safeguard the integrity, confidential, and availability of the network data.

Chapter 2 Organization Structure

Article 5 As the cybersecurity work coordination and decision-making institution ofthe SIAT, the Cybersecurity and Informatization Leadership Group of the SIAT (ILGI) organizes cybersecurity work ofthe SIAT according to the relevant government deployment; study and formulate strategies, development plans and major policies for the cybersecurity work ofthe SIAT; approved the deployment of cybersecurity work and important projects of the SIAT, make decisions and determination on relevant major issues, and coordinate the working relationship between various parties.

Article 6 The Security Work Committee ofthe SIAT (Security Committee) is responsible for analyzing whole-institute cybersecurity work situation, discussing and developing related rules and regulations, management measures for the SIAT, as well as their deployment and implementation; discussing and handling major issues and events, discussing and determining the treatment opinions to major cybersecurity accident liability.

Article 7 The Department of Science & Technology Development is the implementation subject of cybersecurity work, which practises cybersecurity jobs in the guidance of ILGI and Security Committee. The part-time Network and Information Administrator of each institution assist the Network and Information Office in practising cybersecurity jobs in the institute.

Chapter 3 Security Responsibilities

Article 8 The Department of Science & Technology Development is responsible for formulating and implementing the cybersecurity management system and contingency plan ofthe unit; carrying out cybersecurity inspections, risk disposal and rectification of hidden dangers; carrying out cybersecurity education and training as needed; carrying out an annual inspection for all websites and information systems of the unit. In case of an incident occurred to imperil cybersecurity, it should activate the contingency plan immediately, taking corresponding remedial measures and reporting to the Security Committee and other related departments.

Article 9 The Department of Science & Technology Development should implement technical safeguard measures for cybersecurity according to codes and requirements; take technical measures to monitor and record network operation status and cybersecurity events, preserve relevant network logs for not less than six months according to the regulations; carry out inspection matters for cybersecurity; timely dispose of cybersecurity events, potential risks, patching vulnerabilities; regularly provide confidential education and skill training to O&M personnel.

Article 10 Network users should abide by national laws and regulations, obey cybersecurity management, enhance security awareness, properly keep their accounts and passwords without disclosure; adhere to self-discipline when using Internet, do not communicate illegal and false information.

Chapter 4 Business System Security

Article 11 Cybersecurity level should be appropriately rated to each business system in the SIAT in the guidance of the Security Committee. If the security protection level is proposed to be Level 1 or 2, it is necessary to timely fulfill formalities ofcybersecurity level protection filing at the local police; ifit is proposed to be Level 3 or above, it is necessary to submit filing application to the institution of the Chinese Academy of Sciences, and fulfill formalities offiling at the police after the application is reviewed and approved. Before the acceptance of information infrastructure and important information system construction projects supporting major scientific research tasks, the construction unit should evaluate their protection level, and the evaluation report should be used as an important basis for acceptance evaluation.

Article 12 Strictly management the design scheme, implementation plan, topology diagram, software codes, system settings, system administration account, operation and maintenance account, passwords and other key information data ofthe information system without disclosure; sign agreements with system constructors and operation and maintenance providers to clarify their confidentiality responsibilities, specify the terms ofaccountability, and enforce strictly management.

Article 13 In addition to fulfilling related cybersecurity regulations, each unit containing key information infrastructure should properly:

(1) designate a special security management department and a security management principal, and conduct background survey in security for such security management principal and personnel in key positions;

(2) regularly provide cybersecurity education and technology training for, conduct skill assessment on practitioners;

(3) make disaster recovery backup for important system and data;

Chapter 5 Security Management ofBasic Network Operation and Internet Addresses

Article 14 The internal IP addresses ofthe SIAT are centrally planned by the Department of Science & Technology Development, and any user device should not set a static IP address. The public IP addresses of the SIAT are centrally administrated by the Department of Science & Technology Development. Each user unit should obtain approval by the department principal, the Network and Information Office of the Department of Science & Technology Development, Department of Science & Technology Development Director, and principal leaders of the Institute before use public IP addresses. Responsibilities should be assigned to the personnel who assign and use public IP addresses, with the information records preserved for over one year.

Article 15 If the IP address is used for public services, apart from requiring internal approval by the SIAT and reviewing the identity ofthe service contract Party B, it is necessary to go through pre-approval and filing procedures at the corresponding functional government department according to the service type. It is strictly prohibited to use virtual private network service providers that carry out cross-border activities without the approval of the telecommunications competent department.The emails, published information, and other types of data content transmitted through the IP addresses must strictly comply with relevant national laws and regulations.

Article 16 Unless a user is assisted by the Network and Information Office of the Department of Science & Technology Development, he/she is not allowed to connect a wireless router to the network of the SIAT privately. Supervision, management and security protection should be strengthened to the use of wireless network, and the temporary access of foreign personnel to the network should be registered. Networking in an office area accommodating 5 persons or above must be filed at the Network and Information Office of the Department of Science & Technology Development that will not be responsible for treating any abnormality of networking without filing. Any department needs accessing a dedicated line from the ISP should obtain approval by the department, the

Network and Information Office of the Department of Science & Technology Development, the Department of Science & Technology Development Director, and the principal leaders ofthe Institute before access. Meanwhile, the person in charge of the dedicated line should bear full responsibility for the risk arising from the access.

Article 17 Desktop computers, laptop computers, printers and mobile terminals used for scientific research and office should have basic security protection capabilities such as anti-virus, anti-attack, and vulnerability fixing. System password and account permissions and IP address operation permissions setting should be strictly administrated, which external disclosure should be avoided. Office terminals without basic protection capabilities are not allowed to access the network ofthe unit. It is strictly prohibited to click or open unknown links or attachments.

Article 18 The access control system ofthe server room ofthe SIAT adopts the mechanism of "one employee and one student", and the number ofpersons who are added to the access control system ofthe same computer room in the same center should be not more than 2. Those who temporarily access to the server room may get a access card from the Network and Information Office of Department of Science & Technology Development after make registration. The servers hosted in the server room must meet the standard rack requirements. See the *Contingency Plan of Faults in Server Room* for the management measures of server room.

Chapter 6 Security Management ofInternet Information Service

Article 19 Each website in the SIAT should only be built after obtaining approval by the department principal, the Development Department (Office of Cultural Propaganda), the Network and Information Office of the Department of Science & Technology Development, the Department of Science & Technology Development Director, and the leaders of institute in charge; At the same time, the business license, ICP filing and international networking filing registration procedures should be handled according the requirements of administrative regulations on Internet information services. The website using the second-level domain name of the SIAT must be built on the institute's web servers. Every year after the website was put into operation, the person in charge of the website needs to confirm the status of the website and the profile ofthe person in charge at the Network and Information Office of the Department of Science & Technology Development, and the website without confirmation and filing for two consecutive years will be shut down. Websites and information systems having not been maintained for 1 month or more, with many code vulnerabilities and security risks, or existing high risk vulnerabilities and security risks that cannot be rectified will be shut down.

Article 20 For interactive websites such as electronic bulletin boards, forums, chat rooms, blog space, WeChat, and we-media, security management should be strengthened in website construction requirements, system safeguard, account registration, security maintenance, and audit capabilities.

Article 21 The information cannot be released on the website until the publicity department and relevant leaders ofthe SIAT review it to ensure that the information content is accurate, true and traceable, containing no state secrets and internal sensitive information.

Article 22 For public website, responsible operator and technical person in charge should be explicitly designated. The responsible operator should be a fixed person who is responsible for the security management ofthe interactive columns, such as website information release, system operation and comments. For interactive websites directly available for the public, a website, system, and information administrator should be explicitly designated, with operation administration being carried out by special personnel.

Article 23 Mailbox has two types: personal e-mailbox and department (function) e-mailbox, and a corresponding administrator ofmailbox is responsible for the information security ofthe e-mailbox. A personal e-mailbox ofa resigned person will be locked after one week and deleted after two months. Personal e-mailbox can be retained for a maximum of two years by filling out the *Application of E-mailbox Retention for Resigned Person*. Department (function) mailboxes are mainly used to process department business or forward emails or send emails on behalf of others. Mass emailing by a department (function) of the SIAT should distinguish between employees and students to ensure the purpose, accuracy and security of information transmission. An e-mailbox that has not been logged in for two consecutive years is regarded as a zombie e-mailbox and will be locked for one week before being deleted.

Chapter 7 Monitoring, Early Warning and Emergency Response

Article 24 The Security Committee coordinates with relevant departments to strengthen the collection, analysis and notification ofonline information.

Article 25 In the case of a cybersecurity incident, the Department of Science & Technology Development will activate the cybersecurity incident contingency plan, investigating and evaluating the cybersecurity incident, taking technical and other necessary measures to eliminate security hidden dangers and preventing hazards from expansion.

Chapter 8 Award and Punishment

Article 26 Cybersecurity work is included in the selection of advanced collectives and individuals in security work, and collectives and individuals with outstanding achievements or contributions should be commended and awarded; ifa cybersecurity incident or a major cybersecurity incident occurs, the qualification for evaluation within the period should be revoked.

Article 27 Any unit or individual in the SIAT that is inadequate in cybersecurity administration or has many cybersecurity hidden dangers which have not been rectified for a long time should be notified and the relevant personnel should be held accountable.

Chapter 9 Bylaw

Article 28 These Measures are interpreted by the Department of Science & Technology Development.

Article 29 These Measures are implemented as ofthe date ofpromulgation.

Attachment: 1.Related Approval Processes on AOP System

2.Approval Form of SIAT on Public IP Address Application

3.Approval Form of SIAT on Website Application

4.*Approval Form of SIATon Dedicated Line Application*

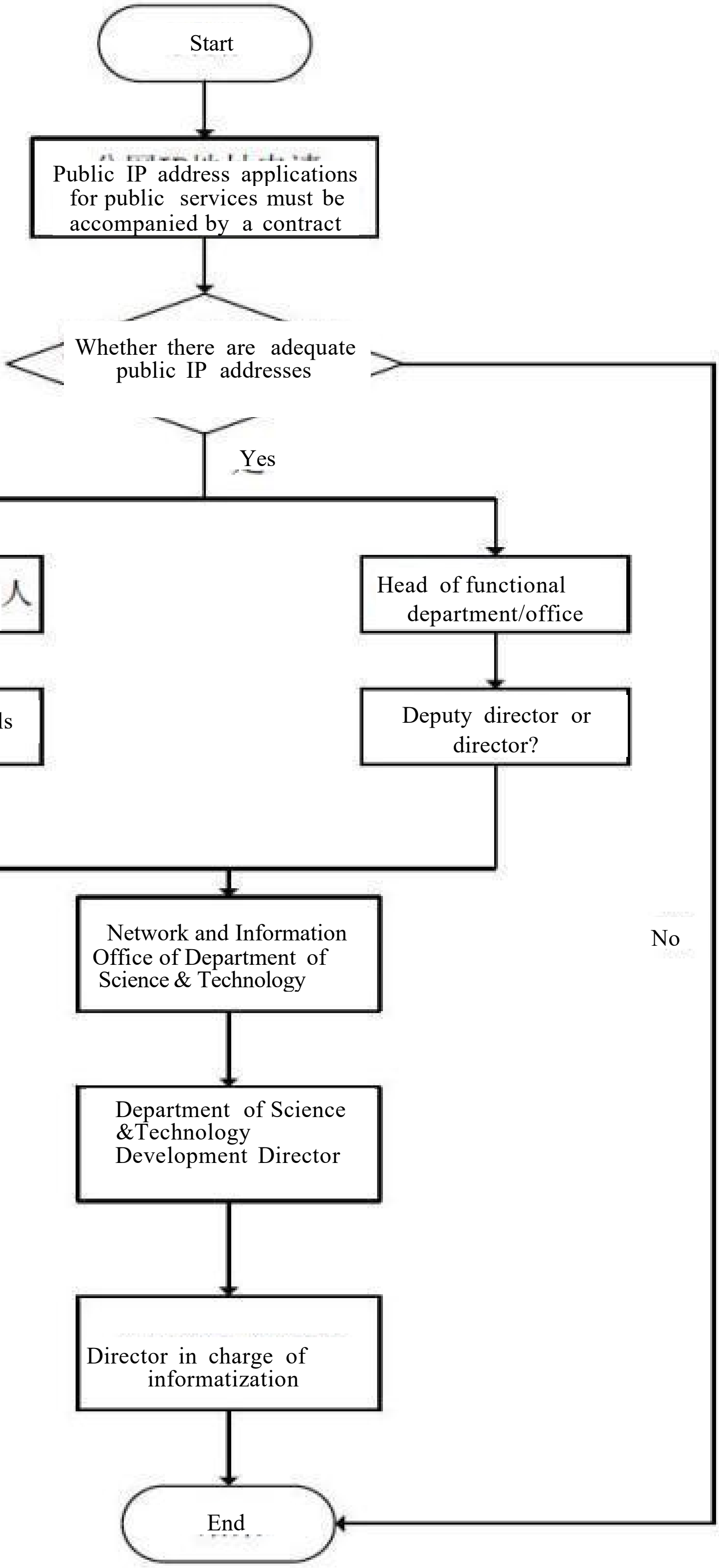
5.*Application of E-mailbox Retentionfor Resigned Person*

6. *Contingency Plan of Faults in Server Room*

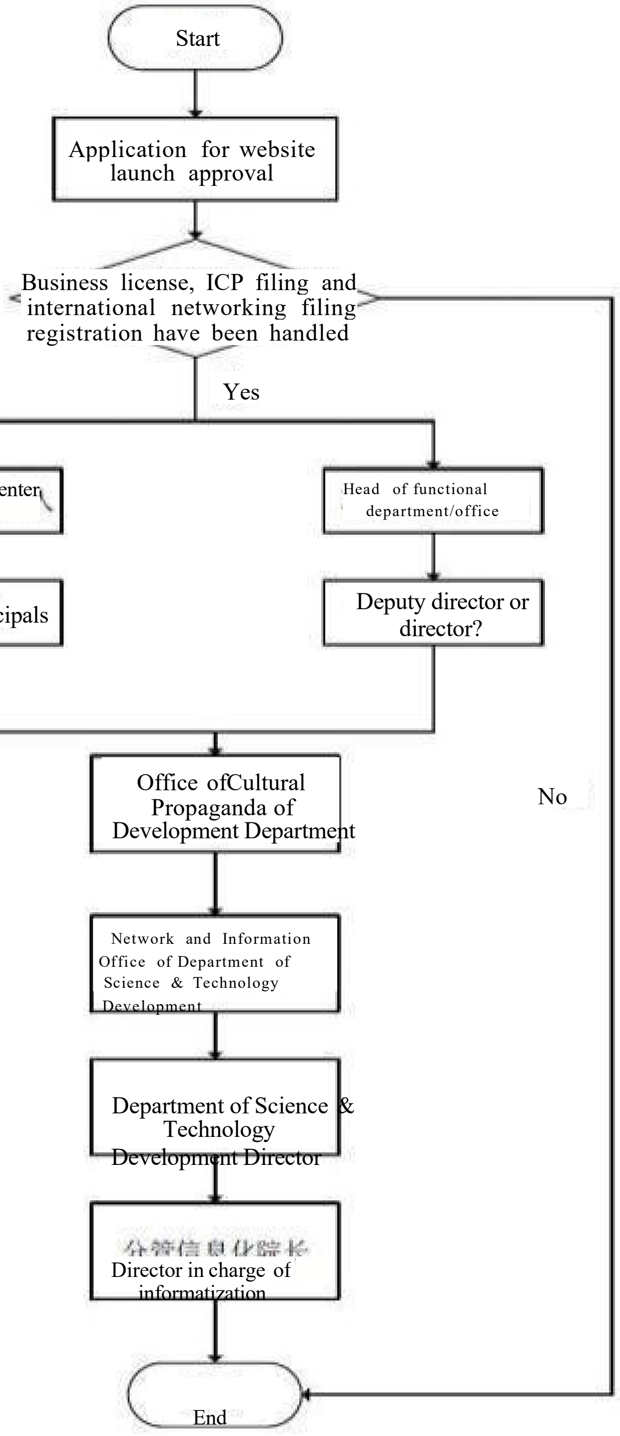
Attachment 1

Related Approval Processes on AOP System

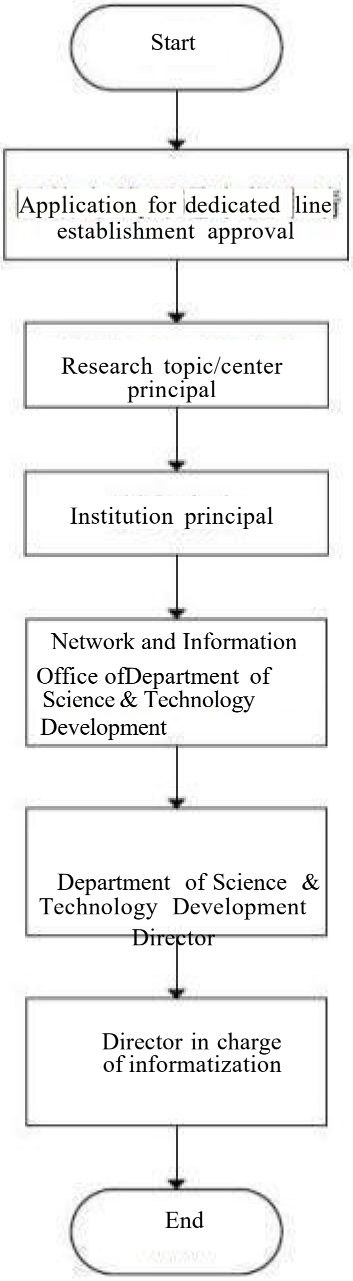
1. Approval process ofIP addresses and public services application:


Start
Public IP address applications for public services must be accompanied by a contract
Whether there are adequate public IP addresses
Yes
No
Research topic/center principal
Head of functional department/office
Institution principals
Deputy director or director?
Network and Information Office of Department of Science & Technology
Department of Science &Technology Development Director
Director in charge of informatization
End

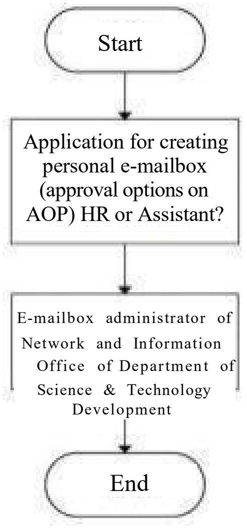
2. Approval process of website launch application:


Start
Application for website launch approval
Business license, ICP filing and international networking filing registration have been handled
Yes
No
Research topic/center principal
Institution principals
Head of functional department/office
Deputy director or director?
Office ofCultural Propaganda of Development Department
Network and Information Office of Department of Science & Technology Development
Department of Science & Technology Development Director
分管信息化院长
Director in charge of informatization
End

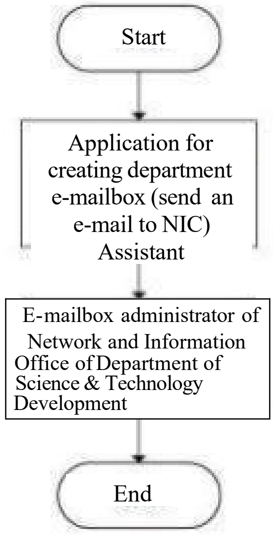
3. Approval process ofdedicated line application:


Start
Application for dedicated line establishment approval
Research topic/center principal
Institution principal
Network and Information Office ofDepartment of Science & Technology Development
Department of Science & Technology Development Director
Director in charge of informatization
End

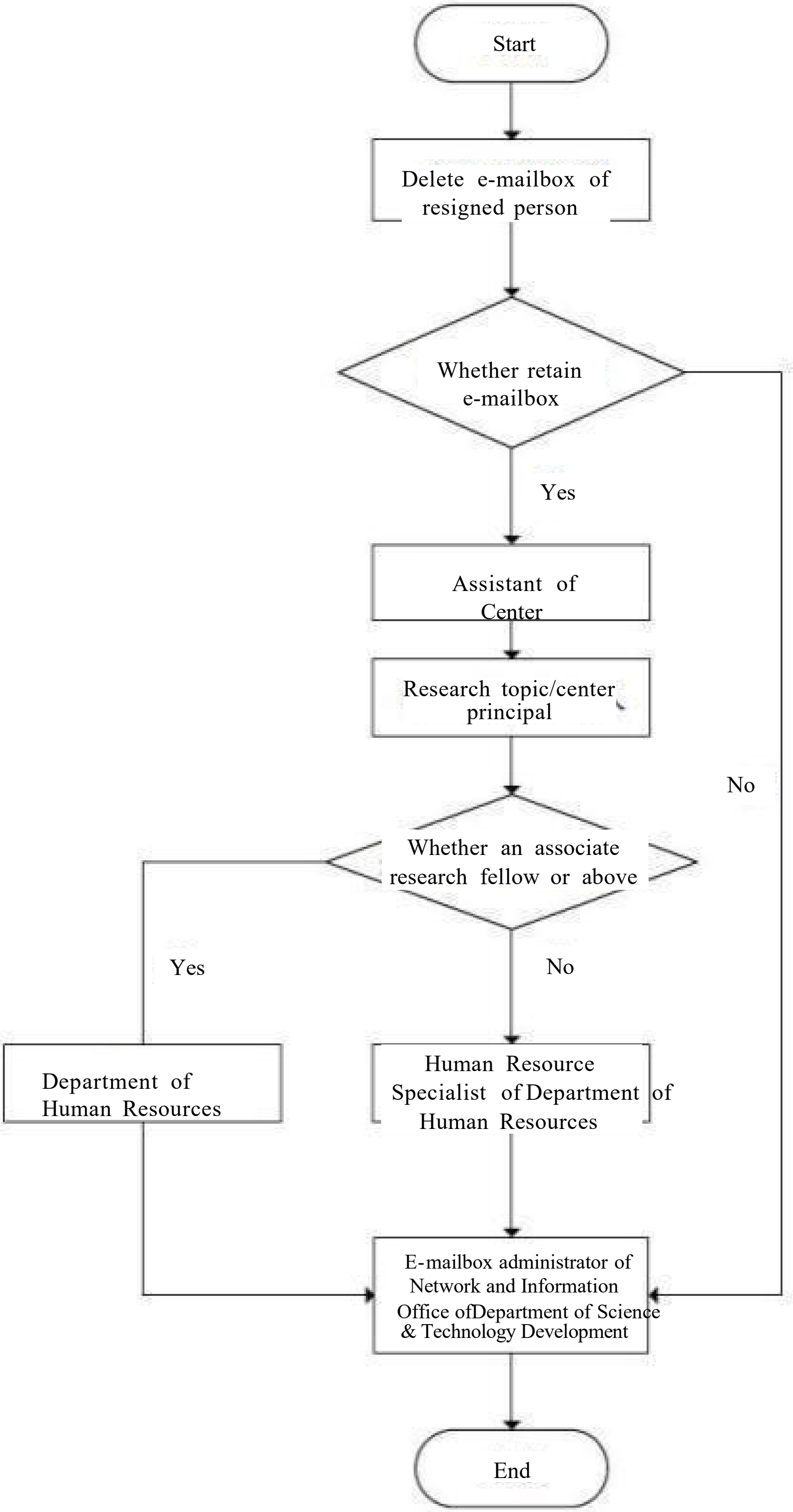
4. Approval process ofcreating e-mailbox application:
(personal e-mailbox)


Start
Application for creating personal e-mailbox (approval options on AOP) HR or Assistant?
E-mailbox administrator of Network and Information Office of Department of Science & Technology Development
End

(department e-mailbox)


Start
Application for creating department e-mailbox (send an e-mail to NIC) Assistant
E-mailbox administrator of Network and Information Office of Department of Science & Technology Development
End

5. Approval process ofdeleting e-mailbox:


Start
Delete e-mailbox of resigned person
Whether retain e-mailbox
Yes
No
Assistant of Center
Research topic/center principal
Whether an associate research fellow or above
Yes
No
Department of Human Resources
Human Resource Specialist of Department of Human Resources
E-mailbox administrator of Network and Information Office ofDepartment of Science & Technology Development
End

Attachment 2

Approval Form of SIAT on Public IP Address Application

Applicant		Department/unit		Employee ID	
Public IP address			Port No. (optional)		
Brief of public purpose					
Responsible operator		Cellphone		E-mailbox	
Technical responsible person		Cellphone		E-mailbox	
Approval of center	Approval opinion: Signed and confirmed by head ofcenter:				
Approval of institution headquarters	Approval opinion: Signed and confirmed by institution principal:___				
Confirmed by Network and Information Office of Department of Science & Technology Development	Approval opinion: Signed and confirmed by Network and Information Office head:___				

Confirmed by Department of Science & Technology Development Director	Approval opinion: Signed and confirmed by Department of Science & Technology Development Director:___
Approved by institute leader in charge of informatization	Approval opinion: Confirmed and signed by institute leader in charge of informatization:__

Attachment 3

Approval Form of SIAT on Website Application

Applicant		Department/unit		Filing No.	
Website name			Second-level domain of website		
Brief of website purpose					
Responsible operator		Cellphone		E-mailbox	
Technical responsible person		Cellphone		E-mailbox	
Approval of center	Approval opinion: Signed and confirmed by head ofcenter:				
Approval of institution headquarters	Approval opinion: Signed and confirmed by institution principal:___				
Confirmed by Cultural Construction and Publicity Office of Department of Development	Approval opinion: Signed and confirmed by Cultural Construction and Publicity Office head:___				

Confirmed by Network and Information Office of Department of Science & Technology Development	Whether to allocate cyber resources: □ Yes (fill in IP address and port of web server) □ No IP address ofweb server: Port No.: Signed and confirmed by Network and Information Office head :___
Approved by institute leader in charge of informatization	Approval opinion: Confirmed and signed by institute leader in charge of informatization:__

Attachment 4

Approval Form of SIAT on Dedicated Line Application

Applicant		Department/unit		Employee ID	
Dedicated line operator name			Dedicated line expense		
Brief of purpose of dedicated line					
Responsible operator		Cellphone		E-mailbox	
Technical responsible person		Cellphone		E-mailbox	
Approval of center	Approval opinion: Signed and confirmed by chairman ofcenter:___				
Approval of institution headquarters	Approval opinion: Signed and confirmed by institution principal:___				
Approval of Network and Information Office of Department of Science & Technology Development	Approval opinion: Signed and confirmed by Network and Information Office head:___				

Approval of Department of Science & Technology Development Director	Approval opinion: Signed and confirmed by Department of Science & Technology Development Director:___
Approved by institute leader in charge of informatization	Approval opinion: Confirmed and signed by institute leader in charge of informatization:__

Attachment 5

Application ofE-mailbox Retention for Resigned Person

Name		Department/unit		Employee ID	
Retention date		E-mailbox address		Position/Title	
After your resignation, the e-mailbox will be used by □ Myself□ Agent Signed and confirmed by agent/date:					
Reason for e-mailbox retention	Signed and confirmed by applicant/date:				
Approval opinion of department	Signed and confirmed by department principal/date:				
Signed by department assistant	1. The e-mailbox address has been deleted from the department/unit e-mail automatic forwarding list. □ 2. The e-mailbox address is retained in the department/unit email automatic forwarding list. □ Signed and confirmed by assistant/date:				
Opinion of Personnel And Education Department	Review opinion: Signed and confirmed by Personnel and Education Department/date: ·				

Attachment 6

Contingency Plan ofFaults in Server Room

I. Contingency plan ofwater leakage prevention in server room

1. In the case of water leakage in server room, the first witness should immediately notify the Network and Information Office ofthe Department of Science & Technology Development.

2. In case of water leakage from air conditioning system, immediately stop using the faulty air conditioner, clear the accumulated water in the server room, and timely contact the equipment supplier for repair. If necessary, use fan to cool the servers temporarily.

3. In case ofwater leakage from wall or windows, immediately notify related department, timely clear the accumulated water, repair the wall or windows to avoid unnecessary losses.

II. Contingency plan of equipment theft or intentional damage event

1. In the case of equipment theft or intentional damage event, the user or administrator should immediately report the situation to the Network and Information Office ofthe Department of Science & Technology Development, and secure the scene.

2. After receiving report, the Network and Information Office ofthe Department of Science & Technology Development should notify the security department of the SIAT and local police to jointly verify and determine the situation on the spot, check the stolen materials or inventory the artificial damage, and make necessary video and written records.

3. The personnel involved in the incident should actively cooperate with the police to investigate and report the relevant situation to the Network and Information Office ofthe Department of Science & Technology Development.

4. The Network and Information Office of the Department of Science & Technology Development holds a meeting to discuss the incident. In case

of severe situation, it should report to the leadership of the SIAT to request for further processing decisions.

III. Contingency plan of prolonged power outage in server room

After receiving the notice of prolonged power outage, the power outage notice should be issued through the website or telephone timely, requiring users to stop office, save data and shut down their computers normally before the power outage.

IV. Contingency plan of communication network fault

1. In the case of communication network fault, the computer operator should timely inform the Network and Information Office of the Department of Science & Technology Development.

2. The Network and Information Office of the Department of Science & Technology Development should locate the communication network fault in time, or inform the relevant communication network operators to request assistance in finding out the cause. Meanwhile, it should isolate the fault area and cut off the network connection between the fault area and the server.

3. The system administrator should, together with the telecom technicians or company technicians, detect the fault area, gradually restore the network connection between the fault area and the server, and restore the communication network to ensure normal operation.

4. The responsible person should write the fault analysis report and submit it to the relevant department for reference.

V. contingency plan of malicious messages and network virus event

1. In the case of malicious information or network virus, the responsible person should immediately disconnect the network cable to stop the spread of malicious information or network virus, and inform the Network and Information Office of the Department of Science & Technology Development.

2. After receiving the report, the Network and Information Office of the Department of Science & Technology Development should immediately notify all computer users in the LAN of antivirus methods, isolate the network, and guide computer operators to carry out antivirus treatment until the network is in a safe state.

3. Make further tracing of the source of malicious information. Those who publish information without the consent of the relevant leaders, causing

adverse effects and breaking the law should be transfered to law enforcement departments for investigating legal responsibility.

VI. Contingency plan of high-performance computer software system fault

1. Carry out early backup for important systems, such as information ofusers and important software in the file system. For existing 2 sets of NFS file system and 1 set ofLuster parallel file system, in addition to establishing special backup system, particularly important data should be mutually backed up in the three file systems.

2. In the case of software fault, the relevant personnel should report the situation to the Network and Information Office of the Department of Science & Technology Development, and should not handle it without authorization.

3. The Network and Information Office of the Department of Science & Technology Development should promptly despatch technicians for handling. If necessary, recover the data on the hard disks.

4. Restore the computer systems while keeping the original data safe; ifthe system is restored successfully, check the data loss and restore the system using the backup data; if the restoring fails, contact the vendor immediately for support.

VII. Contingency plan ofhacker attack event

1. When the network is illegally invaded, the web content is tampered with, the data on the application servers are illegally copied, modified, or deleted, or the intrusion detection system observes the hacker attack, the users or administrators should disconnect the network and immediately report to the Network and Information Office of the Department of Science & Technology Development.

2. After receiving the report, the Network and Information Office of the Department of Science & Technology Development should immediately shut down the network, block or delete the breached login account, and block the channel for suspicious users to enter the network.

3. Timely clean up the system, restore data, programs, and try to restore the system and network to normal status; ifthe situation is serious, immediately report to the Emergency Network and Information Office of the Department of Science & Technology Development to request support and take countermeasures.

VIII. Contingency plan of equipment hardware faults in server room

1. In the case of hardware fault of the equipment in the server room, the Network and Information Office of the Department of Science & Technology Development should immediately determine the faulty equipment and the causes, making preliminary disposal.

2. Ifthe faulty equipment cannot be restored within a short period, switch to the backup equipment to keep the system running normally; remove the faulty equipment from the network and troubleshoot the fault.

3. After the fault is removed, replace the standby device with it when the network is idle; ifthe fault persists, contact the manufacturer immediately and fill in the equipment fault report form for future reference.

4. The outdoor unit ofthe water cooling system should be able to cope with sudden power failure. If an unplanned power failure occurs, use the standby power supply immediately to ensure the cooling ofthe water cooling system. Ifthere is no standby power supply available, open the water-cooled cabinet door to dissipate heat from the air conditioner in the server room. In an emergency, shut down all nodes.

5. When a computing node ofhigh-performance computers fails, immediately notify Sugon and provide the serial number of the corresponding machine.

6. The cluster system has several key nodes, including login node, I/O node, and storage node. Standby nodes must be set up in advance for these nodes (all environment variables need to be backed up, and in order to speed up troubleshooting, it is better to create whole-system ghost image for these nodes. Thus, they can be used to restore the system immediately upon failure). In case offault, switchover can be made immediately. Adequate data security measure should be taken for the storage node.

IX. Emergency disposal

After an emergency occurs, the relevant personnel should report to the Network and Information Office ofthe Department of Science & Technology Development within 5 minutes, and the emergency team should organize personnel to carry out preliminary disposal. Major incidents should be reported to the Network and Information Office of the Department of Science & Technology Development.

X. Aftermath disposal

After the emergency response work is completed, the Network and Information Office of the Department of Science & Technology Development should organize relevant personnel to establish an incident investigation team to conduct a comprehensive investigation and assessment of the cause, nature, impact, consequences, responsibility, emergency response capacity, recovery and reconstruction ofthe incident, sum up experience and lessons, order the organizations with hidden dangers to make rectification, and restore normal work order.

XI. Emergency communication support

The Network and Information Office of the Department of Science & Technology Development should ensure a 24-hour unimpeded communication, and the property should patrol every 1 hour all the day.

XII. Equipment support

Reserve a certain quantity of hardware and software equipment which are safeguarded and maintained by specially designated personnel.

XIII. Data support

Establish backup system for the important systems to ensure that critical data can be urgently restored after being damaged.

XIV. Contingency plan drill

The Network and Information Office of the Department of Science & Technology Development should schedule a drill at least once a year, by which the problems existing in emergency work system and work mechanism can be discovered so that the contingency plans and the emergency handling capacity can be iteratively refined.