四川科道芯国智能技术股份有限公司

Sichuan Keydom Smart Technology Co., Ltd

标准文件

Standard File

系统安全标准

System Security Standard

文 件 编 号: KD-MLJ-01

Doc. No.:

编 制:安全策略部

Prepared by: Security Policy Department

审 核:

Reviewed by:

批 准:

Approved by:

版本 /修订状态: A10

Rev./Revision status:

受 控 状 态:

Controlled status:

2020-1-1 发布 **2020-1-1 实施**

Issued on 1 / 1 /2020 **Implemented on 1/ 1 /2020**

修改记录表 Document Changes

修改条款 Modified terms	修订状态 Revision Status	修改内容 Description	修改日期 Date	修改人 Changed by	审核人 Reviewed by	批准人 Approved By
/	A/0	初次发行 Initial release	2015/09/22	韩德均 Han Dejun	刘劲松 Liu Jinsong	罗长兵 Luo Changbing
5.1, 5.2, 7.6	A/1	1.格式调整 1.Format adjustment 2.物理架构调整 2.Physical architecture adjustment 3.安全策略调整 3.Security policy adjustment 4.维修报废流程调整 4.Process adjustment for maintenance and obsolescence	2016/3/11	曹良攀 Cao Liangpan	刘劲松 Liu Jinsong	罗长兵 Luo Changbing
6.3, 6.4, 7.3, 9.2	A/2	1.打印服务器去重 1.Print server de-emphasis 2.office 更新 2013 2.Office update to 2013 version 3.设备安装语病修改 3.Faulty wording modification on equipment installation	2016/5/20	徐锐 Xu Rui	刘劲松 Liu Jinsong	罗长兵 Luo Changbing

		4.日志管理增加数据准备服务器日志 4.Log management adds data preparation server logs 5.申请批审顺序修改 5.Sequence modification on application approval				
5	A/3	1、升级网络安全程序为系统安全程序 Upgrading the network security procedures to system security procedures 2、新增 5 系统管理 Adding 5. System Management 3、部分表名统一 Unification of partial table names	2016/9/18	徐锐 Xu Rui	刘劲松 Liu Jinsong	罗长兵 Luo Changbing

6	A/4	1. 新增设备分类编码 Adding equipment classification code 2. 设备安装标准更新 Equipment installation standard update 3. 设备档案详细记录 Detail record on equipment archives 4. 合并设备备份管理 Merging device backup management 5. 报废说明修改 Modification on scrapping description 6. 员工帐号命名规则修改 Modification	2017/03/01	徐锐 Xu Rui	刘劲松 Liu Jinsong	罗长兵 Luo Changbing

		on employee account naming rules				
11	A/5	新增日志管理 Adding log management	2017/8/12	王建勋 Wang Jianxun	刘劲松 Liu Jinsong	杜强林 Du Qianglin
4.2	A/6	新增服务器访问控制 Adding server access control	2017/10/13	王建勋 黄伟 Wang Jianxun Huang Wei	刘劲松 Liu Jinsong	杜强林 Du Qianglin
9.2.1	A/7	修改申请账号规范 Modifying the application of account specification	2018/05/14	王建勋 Wang Jianxun 黄伟 Huang Wei	刘劲松 Liu Jinsong	杜强林 Du Qianglin
/	A/8	更换 log 及公司名称 Change log and company name	2018/7/25	王建勋 Wang Jianxun 黄伟 Huang Wei	刘劲松 Liu Jinsong	杜强林 Du Qianglin
9.2.2	A/9	更新复杂密码具体化 Updating materialization of complex password	2018/12/10	王建勋 Wang Jianxun 黄伟 Huang Wei	刘劲松 Liu Jinsong	杜强林 Du Qianglin

All	A/10	修改与实际情况不相符的规则	2020.1.1	黄伟 Huang Wei	刘劲松 Liu Jinsong	陈为明

目　　录

Contents

1 目的

1 Purpose

为了保障公司系统安全可靠运行，规范系统管理和作操作流程，保证卡片生产的正常运行，生产中心依据《PCI-GSMA》要求，结合生产中心生产和运营流程，形成生产中心的《系统安全程序》。

In order to ensure the safe and reliable operation of the company's system, standardize the system management and operation process, and ensure the normal operation of card production, the Production Center forms the *System Safety Procedure* of the Production Center according to the requirements of the PCI-GSMA and in combination with the production and operation process of the Production Center.

2 适用范围

2 Application Scope

本程序适用于公司生产中心系统、网络及软硬件管理，所有网络、IT 设备、软件相关的管理工作。

This procedure is applicable to the management of the company's Production Center system, the management of network and software and hardware, as well as all management works related to the network, IT equipment and software.

3 职能职责

3 Duties and Responsibilities

首席信息安全官：审批的最高权限在首席信息安全官，所有的核心配置和网络结构要得到批准、授权，并定期进行审查、更新。负责设计和监督实施所有网络结构设计、配置设计、更改审查、维护的审查、生产记录的审查和必要的现场见证。

Chief Information Security Officer: The highest authority for approval rests with

the Chief Information Security Officer. All core configurations and network structures shall be approved, authorized, reviewed and updated regularly. Be responsible for designing and supervising the implementation of all network structure design, configuration design, change review, maintenance review, production record review and necessary on-site witness.

安全策略部安全总监：受首席安全官授权负责生产中心日常安全管理，负责监督实施所有网络结构变更、配置变更；审查各种日常记录和报表；必要的现场见证。

Security Director of Security Policy Department: Authorized by the Chief Security Officer, he/she is responsible for the daily security management of the Production Center, and is responsible for supervising the implementation of all network structure changes and configuration changes; reviewing various daily records and statements; necessary on-site witness.

逻辑安全管理员：受安全总监管理和监督，所有的 IT 设备、软件、网络的更改都要由逻辑安全管理员执行。负责所有 IT 设备、软件、网络的维护并记录，检查个人化数据在生产过程中的所有记录，保证生产网络稳定、安全运行。

Logical Security Administrator: Under the management and supervision of the Chief Security Officer, all changes to the IT equipment, software and network shall be performed by the Logical Security Administrator. Be responsible for the maintenance and recording of all IT equipment, software and networks, checking all records of personalized data in the production process to ensure the stable and safe operation of the production network.

4 网络安全

4 Network Architecture

4.1 网络拓扑图及配置标准

Network Topology and Configuration Standard

生产网络拓扑图见《网络配置授权书》，物理架构符合以下要求：

The topology diagram of the production network is shown in the *Network Configuration Authorization Letter*, and the physical architecture meets the following requirements:

- 形成独立的安全区，办公网络不在其内。

  Form the independent safety zone, and the office network is not included.
- 在个人化网络和 DMZ 网络之间部署 H3C F100 防火墙

  Deploy H3C F100 firewall between personalized network and DMZ network
- 在 DMZ 网络与 Internet 之间部署 H3C F1000 防火墙

  Deploy H3C F1000 firewall between DMZ network and Internet
- 生产网络线缆敷设与办公网络必须独立。

  Cable laying of the production network must be independent from that of the office network.
- 在生产车间、个人化数据处理室、数据机房禁止存在办公网络节点。

  Office network nodes are prohibited in the production workshops, personalized data processing rooms and data rooms.
- 所有网络线缆在未经安全总监授权下，禁止任何变动及更改。

  All network cables are not allowed to change without the authorization of the Chief Information Security Officer.

4.2 网络设备及防火墙 Network equipment and firewall

a．网络设备和网络协议的全部更改，必须通过正式的文件授权方可执行。

All changes to network equipment and network protocols must be authorized by a formal document.

b．通过三级文件《网络配置授权书》列出所有防火墙策略。

List all firewall policies through the three-level file network configuration authorization.

c．在任何变更前，需进行网络设备配置备份并存储相应的服务器内。

Before any changes are made, the network device configuration should be backed up and stored in the corresponding server.

d．在个人化和数据准备网络与互联网之间部署防火墙。

Deploy a firewall between the personalization and data preparation network and the Internet.

e．每月检查防火墙规则设置并验证配套业务的正确性，并记录确保防火墙配置的完整性。

Check firewall rule setup monthly and verify the correctness of supporting business, and record to ensure the integrity of firewall configuration.

f．防火墙规则只开通需要的端口，禁止所有未授权的端口。

Firewall rules only open required ports and prohibit all unauthorized ports.

g．防火墙必须遵循双人双控原则，由 IT 人员负责执行，逻辑安全员负责监督。

Firewall must follow the principle of double and double control, by the IT personnel responsible for implementation, logic security officer responsible for supervision.

h．在防火墙手动添加必要的静态路由。

Manually add the necessary static routes to the firewall.

4.2.1 根据防火墙管理要求，用于对所有的外部网络连接和防火墙配置变更进行批准和测试，并保存配置变更的详细记录。

Use to approve and test all external network connection and firewall configuration changes according to firewall management requirements, and keep detailed records of configuration changes.

4.2.2 防火墙设备通过用户密码方式进入配置，通过双控方式管理，在修改防火墙配置时需通过安全策略部负责人进行审批后方可进行，并且详细记录变更信息。

Firewall devices enter the configuration by means of user password and are managed by dual-control mode. The modification of firewall configuration shall be approved by the person in charge of security policy department, and the change information shall be recorded in detail.

4.2.3 每周对防火墙的运行配置进行备份，并在每月对防火墙配置进行恢复测试，

以确保备份的可靠性。

Backup the running configuration of the firewall every week and restore the firewall configuration every month to ensure the reliability of the backup.

4.2.4 及时对网络及网络安全设备的补丁安装和版本升级，及时更新入侵检测（防御）系统的特征库。

Timely patch installation and version upgrade of network and network security equipment, and timely update the feature library of intrusion detection (defense) system.

a. 在进行升级前做好相关更新计划并通知相关部门做好准备工作；

Make relevant update plan before upgrading and inform relevant departments to make preparations;

b. 在进行升级更新前对设备配置进行备份；

Backup equipment configuration before upgrading;

c. 升级更新完成后验证其可用性并做好相关记录；

Verify the availability of the upgrade and update after it is completed and make relevant records;

4.2.5 根据防火墙等网络设备配置备份，以便在系统崩溃时数据、配置文件可以及时恢复。备份数据和文件保存至专用服务器，以确保安全性，并且只有授权的人员接触。

Configure backup according to firewall and other network devices, so that data and configuration files can be recovered in time in case of system crash.Backup data and files are saved to a dedicated server to ensure security and are accessed only by authorized personnel.

4.2.6 个人化网络是采用专业硬件防火墙保护整个网络，对应任何进入个人化网络的文件、软件或数据进入都会被检查并记录。

The personalization network adopts professional hardware firewall to protect the whole network, and any files, software or data entering the personalization network will be checked and recorded.

4.3 访问控制

4.3 Access Control

逻辑安全管理人员访问机房服务器应符合以下要求：

The Logical Security Administrator shall meet the following requirements when accessing the machine room server:

- 访问服务器必须采取双人双控原则

  Access to the server must be based on the principle of double control by double persons.

- 访问密码应由两位安全管理人员各执一段

  Each security administrator shall keep one section of the access password

- 防火墙变更通过审核后由 IT 人员执行，在逻辑安全员监督下实施

  Firewall changes are approved and then executed by the IT staff under the supervision of the logical security officer

个人化网络中的所有设备都禁止访问互联网，配置域间策略，限制所有不必要连接，应符合以下要求：

All equipment in the personalized network are prohibited from accessing the Internet, the inter-domain policies are configured, and all unnecessary connections are restricted. The following requirements shall be met:

- 所有的网络连接必须使用受保护的网络传递方式

  All network connections must adopt the protected network delivery method

- 控制必要的访问，仅允许建立有需要的连接

  Control necessary access and allow only necessary connections to be established

- 控制访问协议及端口，仅允许开通有使用需求的端口及协议

  Control the access protocols and ports, and only allow the ports and protocols with usage demand to be opened

- 随时对可能的攻击做出反应，并对影响进行评估

  Respond to possible attacks at any time and evaluate the impact

4.4 远程访问

4.4Remote Access

连接的建立必须满足以下要求：

The establishment of the connection must meet the following requirements:

- VPN 通道的建立必须基于 CA 证书认证

  The establishment of VPN tunnel must be based on CA certificate authentication

- 仅允许远端设备通过 VPN 访问数据接收服务器

  Only remote devices are allowed to access the data receiving server through VPN

- 任何实施设备管理操作的远程连接必须在生产网络以内进行

  Any remote connection to implement equipment management operations must be made within the production network

- 禁止任何远程连接，如果需要使用远程连接必须有首席信息安全官的授权

  Disable any remote connections, which must be authorized by the chief information security officer if needed

- 仅允许逻辑安全管理员管理设备

  Only Logical Security Administrators are allowed to management devices

4.5 安全测试和监控

4.5 Security Testing

4.5.1 安全隐患

安全测试包括内部与外部弱点、漏洞的扫描，应满足以下要求：

Security testing includes scanning of internal and external weaknesses and vulnerabilities, and shall meet the following requirements:

- 逻辑安全管理员每年系扫描服务商扫描一次内外部安全隐患；
  The Logical Security Administrator contacts the scanning service provider to scan the internal and external security risks once every year;
- 当网络架构发生变更后，逻辑安全管理员应进行一次内外部安全隐患扫描；
  When the network architecture changes, the Logical Security Administrator shall conduct a scan of the internal and external security risks;
- 扫描完成后，逻辑安全管理员应及时分析弱点报告、提出优化建议，经首席信息安全官审批后执行修补工作；
  After the scan is completed, the Logical Security Administrator shall analyze the vulnerability report and put forward the optimization suggestions within timely, and perform the repair operation after it is reviewed by Chief Information Security Officer；
- 在漏洞修补前，逻辑安全管理员不得以任何方式透露给他人；
  Before the vulnerability is fixed, the Logical Security Administrator shall not disclose it to others in any way；

4.5.2 入侵

a. 建立防火墙的管理和配置标准，在个人化生产线中三个区域通过防火墙进行隔离，用来拒绝来自不可信网络和主机的所有通讯，并且在整个过程中，加入了专业的硬件 IPS 入侵攻击，已确保个人化网络的安全。
b. 在重要的基础设施变更后，每年开展一次内部和外部入侵检验。
c. 内部入侵检验必须处于本局域网内。
d. 通过使用 IPS 入侵防御系统监督数据准备和个人化网络的通信量以及异常情况。
e. 定期对 IPS 系统日志报告进行分析，上报异常情况。

4.6 网络线缆管理

4.56Network Cable Management

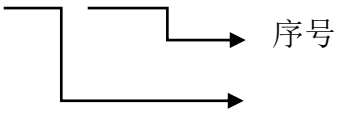
4.6.1 网络布线标准

4.6.1 Network Cabling Standard

所有网络线缆必须有明确的编号，编号标准如下：

All network cables must be clearly numbered, and the numbering standard is as follows:

KD-□□-□□□



网络编号

Network number

序号：从 001 开始依次递增

Serial number: increasing in sequence from 001

网络编号：01 生产网络 02 办公网络 03 宿舍网络

Network Number: 01 Production network 02 Office network 03 Dormitory network

4.6.2 网络线缆变更

4.6.2 Network Cable Change

若生产网络中网络线缆需要更改其连接状态、设备或端口，逻辑安全管理员应填写《IT 设备安装及变更申请表》且经安全总监签字授权后才能更改，逻辑安全管理员应每周检查生产区中网络线缆是否有异常，检查应记录在《IT 日常检查记录表》中。

If the network cable in the production network needs to change its connection status, equipment or port, the Logical Security Administrator shall fill in the *Application Form for Installation and Change of IT Equipment* and can only change it after being signed and authorized by the Security Director. The Logical Security Administrator shall

check whether there is any abnormality in the network cable in the production area twice a week, and the check results shall be recorded in the *IT Routine Inspection Record Form*.

4.7 无线网络管理

4.7 Wireless Network Management

在生产网络中，确保生产网络中无任何无线传输设备。逻辑安全管理员应每月扫描一次无线热点，并在《无线热点扫描统计表》中记录扫描时间等内容，逻辑安全管理员应保存每一张截图，截图中应包括右下角系统时间， In the production network, ensure that there is no wireless transmission equipment in the production network. The Logical Security Administrator shall scan the wireless hotspot once a month and record the scanning time and other contents in the *Wireless Hotspot Scanning Statistics Table*. The Logical Security Administrator shall save each screenshot, which shall include the system time in the lower right corner.

扫描范围包括个人化生产车间、仓库、生产机房，扫描方式如下：

The scanning range includes all high-security areas. The scanning method is as follows:

- 使用笔记本电脑连接 RTL 8187L USB 无线网卡以支持扫描

  Connect the RTL 8187L USB wireless network card with a laptop to support scanning
- 扫描软件使用 RTL 自带无线网络管理程序

  The scanning software uses RTL's own wireless network management program
- 扫描过程必须由逻辑安全管理员执行，并满足双人四眼原则

  The scanning process must be performed by the Logical Security Administrator and witnessed by two people.

5 系统管理

5 System Management

5.1 系统分类

5.1 System Classification

生产中心系统分为生产系统和办公系统，生产系统主要由补丁自动更新系统、杀毒系统、加密系统、安全监控系统和生产设备系统构成；办公系统主要由办公软件系统、文件共享系统和行政财务系统构成。

The Production Center system is divided into the production system and office system. The production system mainly consists of the patch automatic updating system, antivirus system, encryption system, security monitoring system and production equipment system. The office system mainly consists of the office software system, file sharing system and administrative finance system.

5.2 系统管理方针

5.2 System Management Policy

生产中心系统管理由权限管理、备份管理、容量管理、监控管理有机组成，权限管理主要涉及系统访问控制和权限审批，备份管理涉及系统数据和配置安全备份，容量管理涉及系统环境容量和性能管理，监控管理涉及系统操作过程和数据的安全监控管理。

The Production Center system management consists of the authority management, backup management, capacity management and monitoring management. The authority management mainly involves the system access control and authority approval. The backup management involves the system data and configuration security backup. The capacity management involves the system environment capacity and performance

management. The monitoring management involves the system operation process and data security monitoring management.

5.2.1 权限管理

5.2.1 Authority Management

根据相关要求，系统最高权限应由在首席安全官负责管理，授权逻辑安全管理员管理员权限管理各类系统，普通用户不能有系统管理员权限。

According to relevant requirements, the highest authority of the system shall be managed by the Chief Security Officer, and the Logical Security Administrator shall be authorized to manage all kinds of systems. Ordinary users shall not have authority of the system administrator.

5.2.2 备份管理

5.2.2Backup Management

逻辑安全管理员负责系统备份实施和审计，首席安全官负责备份的审查工作。

The Logical Security Administrator is responsible for the implementation and audit of the system backup, and the Chief Security Officer is responsible for the review of the backup.

5.2.3 容量管理

5.2.3 Capacity Management

逻辑安全管理员负责系统容量的监控和日常审计，首席安全官不在容量的规划和性能提升。

The Logical Security Administrator is responsible for the monitoring and daily audit of the system capacity. The Chief Security Officer is not responsible for the capacity planning and performance improvement.

5.2.4 配置和补丁管理

5.2.4 configuration and patch management

1.每周对系统和设备进行补丁查证更新是否可用并做记录。

Patch and verify the availability of updates to the system and equipment on weekly basis and keep records.

2. 通过检查发现有更新补丁并通过测试后，30 日内为全部系统环境安装最新补丁。

Install the latest patch for all system environments within 30 days after the update patch is found through inspection and passed the test.

3. 每月检查授权的设备配置，验证所有系统组件的配置均可通过标准。

Check the authorized equipment configuration every month to verify that all system components can pass the standard.

4. 在应用任何补丁前对即将变更的系统进行备份。

Make a backup of the system that will change before applying any patches.

5. 在两个工作日内不可能实施的高危补丁情况下，CISO、安全经理、IT 主管必须明确记录知晓需要在最多七日内授权完成高危补丁的更新安装。

In the case of high-risk patches that cannot be implemented within two working days, CISO, security manager and IT supervisor must clearly record that they need to authorize the update and installation of high-risk patches within a maximum of seven days

5.2.5 杀毒软件管理

1) 在个人化网络部署病毒升级服务器，病毒库自动分发到各客户端进行每日升级，并保证最新的病毒库文件被使用。To deploy virus upgrade server in personalization and connection management system network. The virus reservoir server will automatically make distribution to each clients for daily virus reservoir upgrade to ensure virus reservoir used is the newest.

2) 对所有的系统安装防毒软件，防止恶意软件的攻击（如 PC 和服务器）。To

deploy anti-virus software on all computers and systems to prevent from attack of malicious software.

3) 确保所有的杀毒软件被监测、避免被删除，免受各种恶意软件的攻击。Ensure that all the anti-virus software could detect, remove and protect against all known types of malicious software

4) 确保所有反病毒机制是最新的（至少 7 天以内），且能够产生审核日志。Ensure that all the anti-virus mechanism is current (within seven days) and able to generate audit log.

5) 发现病毒感染必须有处理记录，从发现到病毒清除完毕应有详细日志。To keep detailed record for handling virus infection from discovery to elimination.

6) 对于任何进入个人化网络的文件、软件或数据在进入前都要用防病毒软件进行检测。To test all the docs, software or data by anti-virus software before they enter into personalization network.

7) 制定必要策略定期对生产网络进行扫描。Necessary policies should be defined to enforce regular scanning for pro network.

5.2.6 监控管理

5.2.6 Monitoring Management

逻辑安全管理员负责系统日常监控和问题汇报，首席安全官评估问题和风险控制。

The Logical Security Administrator is responsible for the daily monitoring and problem reporting of the system, and the Chief Security Officer evaluates the problems and carries out risk control.

6 IT 设备管理

6 IT Equipment Management

6.1 IT 设备申请

6.1 IT Equipment Application

各部门申购 IT 设备机器配件等需填写《IT 设备安装及变更申请表》，逻辑安全管理员确认是否必需添置，若无法调配设备，逻辑安全管理员应对所有申购设备提出配置及选型意见，进入采购程序，方可采购设备或配件。

Each department shall fill in the *Application Form for Installation and Change of IT Equipment* when purchasing IT equipment and machine accessories. The Logical Security Administrator shall confirm whether it is necessary to purchase the equipment. If the equipment cannot be allocated, the Logical Security Administrator shall put forward the configuration and selection opinions for all equipment to be purchased and enter the procurement procedure before purchasing the equipment or accessories.

6.2 IT 设备编号标准

6.2 IT Equipment Numbering Standard

逻辑安全管理员须对 IT 设备进行编号以规范管理，设备的编号及相关信息应记录在《IT 固定资产统计表》,IT 设备编号标准依照《生产中心固定资产管理制度》。

The Logical Security Administrator shall number the IT equipment to standardize management. The number of the equipment and relevant information shall be recorded in *IT Fixed Asset Statistic Form*. The numbering standard of IT equipment shall be in accordance with the *Fixed Assets Management System of the Production Center*.

编码规则如下表：

The numbering rules are as follows:

名称 Item	编码规则 Numbering rules:	说明 Description
服务器 Server	CDJK-S01-05-001-xxx	服务器 Server
固定座机 Fixed landline	CDJK-S01-04-002-xxxx	固定电话、传真 Fixed-line telephone, fax
台式电脑主机 Desktop computer mainframe	CDJK-S01-05-003-xxx	台式电脑主机、品牌机 Desktop computer mainframe, brand-name computer
液晶显示器 Liquid Crystal Display	CDJK-S01-05-004-xxx	液晶显示器 Liquid Crystal Display
打印机扫描仪 Printer, scanner	CDJK-S01-05-005-xxx	打印机、扫描仪、复印机 Printer, scanner, copying machine
投影仪、幕布 Projector, curtain	CDJK-S01-05-006-xxx	投影仪、幕布 Projector, curtain
软件 Software	CDJK-S01-05-009-xxx	软件、操作系统 Software, operating system
网络设备 Network device	CDJK-S01-05-010-xxx	路由器、交换机、防火墙、加密机、安全设备等… Router, switch, firewall, HSM, security device, etc.
移动存储介质	CDJK-S01-05-012-xxx(LV[X])	U 盘、移动硬盘、加密狗,保密

Removable storage medium		等级 1-3 USB Flash Drive, mobile hard disk, dongle, security level 1-3
其他 Other	CDJK-S01-05-011-xxx	其他 Other

6.3 设备安装及检查

6.3 Equipment Installation and Check

6.3.1 安全来源检查

6.3.1 Security Source Check

所有 IT 设备必须确保其来源安全（包括供应商及设备本身），采购部必须要求合作商（供应商、运输商）向生产中心报备企业各项信息并建立基本档案，档案信息记录到《IT 固定资产统计表》中。

All IT equipment must ensure its source security (including suppliers and equipment itself). The Purchasing Department must require the partners (suppliers and carriers) to report all information of the enterprise to the Production Center and establish the basic files. The file information shall be recorded in *IT Fixed Asset Statistic Form*.

合作商信息应至少包括：

Partner information shall include at least:

- 供应商名称

  Supplier name
- 供应商联系人及电话

  Contact person and telephone number of the supplier
- 设备生产商名称

Name of equipment manufacturer

- 设备售后服务联系人及电话

  Contact person and telephone number of equipment after-sales service

- 设备名称及型号

  Equipment name/model

- 设备唯一编码，如序列号或串号

  Unique code of equipment, such as serial number or identification number

6.3.2 安装前检查

6.3.2 Check before Installation

为保证网络及数据安全，至少应检查以下内容：

In order to ensure the network and data security, the following contents shall be checked at least:

- 检查设备是否满足 IT 设备安装标准并协助验收，逻辑安全管理员填写《IT 设备检查报告》，保证设备符合使用需求。

  Check whether the equipment meets the IT equipment installation standards and assist in acceptance. The Logical Security Administrator shall fill in the *IT Equipment Inspection Report* to ensure that the equipment meets the use requirements.

- 逻辑安全管理员在安装时应做好对设备的调试。

  The Logical Security Administrator shall carry out equipment commissioning properly during installation.

- 检查是否有使用痕迹及数据并填写《IT 设备检查报告》，若有使用痕迹或数据，逻辑安全管理员应在删除前备份数据并记录在《IT 设备检查报告》中。

  Check whether there are traces of use and data and fill in t*he IT Equipment Inspection Report*. If there are traces of use or data, the Logical Security

Administrator shall back up the data and record it in the *IT Equipment Inspection Report* before deleting it.

6.3.3 设备安装

6.3.3 *Equipment Installation*

设备的安装必须由申请人填写《IT 设备安装及变更申请表》，经逻辑安全管理员检查确认符合安装要求后，由逻辑安全管理员按设备安装标准安装并调试设备，安装完成后申请人需在该表中签字确认，逻辑安全管理员必须立即更新《计算机档案记录表》、《IT 固定资产统计表中》该设备的相关信息（如：责任人、IP 地址、设备位置等）。

The applicant must fill in the *Application Form for Installation and Change of IT Equipment* when installing the equipment. After checking and confirming that the equipment meets the installation requirements, the Logical Security Administrator shall install and commission the equipment according to the equipment installation standards. After the installation is completed, the applicant shall sign and confirm the form. The Logical Security Administrator must immediately update the relevant information (such as responsible person, IP address, equipment location, etc.) of the equipment in the *Computer Archives Record Form* and *IT Fixed Asset Statistic Form*.

6.3.4 运行状态检查

6.3.4 Check the Operating Status

6.3.4.1 设备状态检查

6.3.4.1 Check Equipment Status

逻辑安全管理员的所有检查由首席信息安全官授权。

All checks by the Logical Security Administrators are authorized by the Chief Information Security Officer.

逻辑安全管理员必须对运行状况日常监控，包括设备的运行状态、环境，在《IT

日常检查记录表》中记录检查结果。

The Logical Security Administrator must monitor the operation status on a daily basis, including the operation status and environment of the equipment, and record the inspection results in the *IT Routine Inspection Record*.

每周检查两次生产区终端设备硬件状况，包括机箱柜上锁状态、IT 设备或配件位置变动。

Check the hardware status of the terminal equipment in the production area twice a week, including the locking status of the cabinet and changes in the location of IT equipment or accessories.

每月检查机房中防火墙及服务器配置以免受篡改，在《关键设备审查记录》表中记录检查结果。

Check the firewall and server configuration in the machine room monthly to avoid tampering, and record the inspection results in the *IT Routine Inspection Record*.

6.3.4.2 设备日志管理

6.3.4.2 Equipment Log Management

a) 日志检查

a) Log Check

逻辑安全管理员需每周检查一次设备日志，检查结果应记录在《IT 日常检查记录表》，设备日志管理遵循 11 日志管理检查应包括以下内容

The Logical Security Administrator shall check the equipment log a week, and the inspection results shall be recorded in the *IT Routine Inspection Record*. The equipment log management shall follow 11. Log Management. The check shall include the following contents.

- CA 证书及 WSUS 服务器日志

  CA certificate and WSUS server logs

- IPS 日志

  IPS logs

- 管理、杀毒及子 WSUS 服务器日志

  Management, antivirus and sub-WSUS server logs

- 生产机台终端日志

  Production machine terminal logs

- 防火墙日志

  Firewall logs

- 数据接收服务器日志

  Data receiving server logs

- 数据准备服务器日志

  Data preparation server logs

- 数据处理服务器日志

  Data processing server logs

- SAS 数据准备服务器日志

6.4 设备备份管理

6.4 Equipment Backup Management

日志、数据、配置的备份应按照《数据备份策略》的各项要求准确实施。

The backup of logs, data and configuration shall be implemented accurately according to the requirements of the *Data Backup Policy*.

防火墙日志、防火墙配置、IPS 日志、IPS 配置、数据接收日志、数据准备日志，SAS 数据准备服务器由逻辑安全管理员备份，备份完成后填写《数据备份记录表》。

Firewall logs, firewall configuration, IPS logs, IPS configuration, data receiving logs and data preparation logs and CPS database data shall be backed up by the Logical Security Administrator, and the *Data Backup Record* shall be filled in after the backup is completed.

所有设备定期备份，所有设备在更改之前备份。

All equipment shall be backed up regularly and all equipment shall be backed up before changes are made.

6.5 设备变更管理

6.5 Equipment Change Management

6.5.1 设备回收与转移

6.5.1 Equipment Recovery and Transfer

逻辑安全管理员应每周检查是否存在任何闲置的 IT 设备,闲置设备必须回收，IT 设备必须回收后才能再次分配，回收后逻辑安全管理员应根据《IT 设备检查报告》检查设备并更新《IT 固定资产统计表》。

The Logical Security Administrator shall check every week whether there is any idle IT equipment. The idle equipment must be recovered and can be redistributed only after recovery. After recovery, the Logical Security Administrator shall check the equipment according to the *IT Equipment Inspection Report* and update the *IT Fixed Asset Statistic Form*.

6.5.2 硬件变更

6.5.2 Hardware Change

任何 IT 设备的硬件变更都必须由使用人或负责人提出申请，申请人必须填写《IT 设备安装及变更申请表》，经安全总监签字后，逻辑安全管理员才能更改硬件并更新《计算机档案记录表》、《IT 固定资产统计表》和《IT 设备变更记录表》。

Any hardware change of the IT equipment must be applied by the user or the person in charge. The applicant must fill in the *Application Form for Installation and Change of IT Equipment*. After being signed by the Chief Security Officer, the Logical Security Administrator can change the hardware and update the *Computer File Record,*

IT Fixed Asset Statistic Form and *IT Equipment Change Record*.

6.5.3 配置管理

6.5.3 Configuration Management

6.5.3.1 配置变更及申请

6.5.3.1 Configuration Change and Application

所有 IT 设备的系统软件、应用软件设置的修改需由申请人填写《IT 设备安装变更申请表》，经首席信息安全官签字授权后，逻辑安全管理员变更配置并在《IT 设备变更记录表》中记录，在变更配置时应满足以下要求：

The applicant must fill in the *Application Form for Apply and Change of IT Equipment* when modifying the settings of the system software and application software of all equipment. After it is signed and authorized by the Chief Information Security Officer, the Logical Security Administrator shall change the configuration and record it in the *IT Equipment Change Record Form*. The following requirements shall be met when changing the configuration:

- 所有配置变更应满足双人四眼原则操作

  All configuration changes shall be under the witness of two people

- 设备在配置变更前必须备份

  Equipment must be backed up before configuration changes

6.6 设备维修与报废

6.6 Equipment Maintenance and Scrapping

a) 当 IT 设备故障需维修时，设备使用人应告知逻辑安全管理员并填写《IT 故障报修申请表》，逻辑安全管理员应检查设备状况，填写《IT 设备检查报告》以确认维修必要并给予维修意见，经部门领导和安全总监授权后可外出维修。

a) When the IT equipment fails and needs repair, the equipment user shall inform

the Logical Security Administrator and fill in the *Application Form for repairing IT faults*. The Logical Security Administrator shall check the equipment condition and fill in the *IT Equipment Inspection Report* to confirm the repair necessity and give repair advice. The equipment user can go out for repair after being authorized by the department leader and Security Director.

b) 逻辑安全管理员在检查机房 IT 设备时一旦发现设备故障，应立即告知安全总监并进入逻辑安全应急预案，检查故障情况并记录在《IT 日常检查记录表》中。

b) When checking the IT equipment in the machine room, the Logical Security Administrator shall immediately inform the Security Director and start the contingency plans for logical security, check the failure and record it in the *IT Routine Inspection Record*.

c) IT 设备若需要委外维修，申请人必须填写《IT 设备运输申请表》，运输详细流程详见《IT 设备进出流程》。

c) If the IT equipment needs outsourcing maintenance, the applicant must fill in the *Application Form for Transportation of IT Equipment*. For detailed transportation procedures, please refer to *IT Device Access Process*.

d)设备维修完毕，接收时必须进行设备检查并填写《IT 设备检查报告》。确认无问题后方可重新使用。

d) Upon completion of equipment maintenance, equipment inspection must be carried out and the *IT Equipment Inspection Report* must be filled in upon reception. Only after confirming that there is no problem can it be reused.

e)设备报废处理流程如下：

①.由逻辑安全管理员进行设备检查检查并填写《IT 设备检查报告》确认；

②.对于重要的数据存储介质确认损毁后，在安全经理的监督下进行物理破坏，并拍照取证；

③.将进行破坏后的物体在安全员的监督下暂存金库内储物柜存储；

④.暂存金库报废设备一周内集中国家涉密单位销毁中心，统一销毁；

⑤. 报废完成后由逻辑安全管理员更新《IT 固定资产统计表》；

e) Equipment scrapping process is as follows:

①.The logical security administrator shall conduct equipment inspection and fill in the "IT equipment inspection report" for confirmation;

②. After confirming the damage of important data storage media, conduct physical damage under the supervision of the security manager, and take photos for evidence;

③. The damaged object is temporarily stored in the storage cabinet of the Treasury under the supervision of the security officer;

④. The scrapped equipment temporarily stored in the Treasury shall be centralized in the destruction center of national secret-related units within one week for unified destruction;

⑤. After the completion of scrapping, the logical security administrator shall update the statistical table of IT fixed assets;

7 软件管理

7 Software Management

7.1 系统软件

7.1 System Software

逻辑安全管理员需每周检查一次操作系统更新，将检查结果记录在《IT 日常检查记录表》中，若发现更新，逻辑安全管理员在对更新做完安全测试及评估后，应在 2 天内更新所有 IT 设备操作系统，并填写《补丁及病毒库更新记录表》。

The Logical Security Administrator shall check the operating system update once a week and record the inspection results in the *IT Routine Inspection Record*. If an update

is found, the Logical Security Administrator shall update the operating system of all IT equipment within 2 days after completing the security test and evaluation of the update, and fill in the *Patch and Virus Database Update Record*.

7.2 应用软件

7.2 Application Software

所有 IT 设备的应用软件安装、卸载、升级必须填写《软件安装及变更申请表》，经由申请人部门负责人、逻辑安全管理员、安全总监审核通过后，由逻辑安全管理员安装并调试。逻辑安全管理员每周检查一次所有 IT 设备的应用软件安装情况，并将检查结果记录在《IT 日常检查记录表》中。

The *Application Form for Software Installation and Change* must be filled in for installation, uninstallation and upgrade of the application software of all IT equipment. After it is reviewed and approved by the head of the applicant's department, the Logical Security Administrator and Security Director, the installation and debugging shall be carried out by the Logical Security Administrator. The Logical Security Administrator shall check the application software installation of all IT equipment twice a week, and record the inspection results in the *IT Routine Inspection Record*.

8 机房进出管理

8 Room Access Management

8.1 人员进出管理

8.1 Personnel Access Management

■ 逻辑安全管理员进出机房必须以首席信息安全官的授权书为基础

The access to the machine room by the Logical Security Administrator shall be

based on the authorization of the Chief Information Security Officer.

- 逻辑安全管理员进出机房必须双人双控

  The access to the machine room by the Logical Security Administrator shall be controlled by two people.

- 任何外来人员进出机房都必须填写《机房进出申请表》

  Any visitor access to the machine room shall fill in the *Room Access Application Form*.

- 任何外来人员进出必须有两位或以上逻辑安全管理员陪同

  Any visitor access to the machine room shall be accompanied by two or more Logical Security Administrators.

- 外来人员进出机房必须填写《机房进出记录表》

  Visitors access to the machine room shall fill in the *Room Access Record Form*.

- 出机房时逻辑安全管理员必须将密码报警系统布防

  When leaving the computer room, the logical security administrator must deploy the password alarm system.

8.2 物品进出管理

8.2 Article Access Management

- 除安全总监授权以外，禁止任何 IT 设备进出机房

  No IT equipment is allowed to access to the machine room except as authorized by the Security Director.

- 除安全总监授权以外，禁止任何纸张带出机房

  No paper shall be taken out of the machine room except as authorized by the Security Director.

- 经授权的 IT 设备必须由逻辑安全管理员检查，确认无误后方可带入机房，详细流程见 IT 设备进出流程。

Authorized IT equipment must be checked by the Logical Security Administrator and can be brought into the machine room only after being confirmed. For the detailed process, see the IT Dvice Access Process.

- 任何 IT 设备及纸张进出机房必须记录，由物品携带人在《机房进出记录表》中填写详细信息。

  Any IT equipment and paper entering or leaving the machine room must be recorded, and the goods carrier shall fill in the detailed information in the *Room Access Record*.

9 账号及密码管理

9 Account and Password Management

9.1 账号命名标准

9.1 Account Naming Standard

9.1.1 员工账号

9.1.1 Employee Account No.

□□□

↳ 姓名代码

Name code

姓名代码：姓拼音+名拼音首字母。如：王学谦，代码为 wangxq。

Name code: last name in Pinyin +initial letter of first name in Pinyin. For example, Wang Xueqian, whose code is wangxq.

9.1.2 客户账号

9.1.2 Customer Account No.

客户账号命名规范详见《客户账号创建规范》

Please refer to the *Customer Account Creation Specification* for the naming specification of customer accounts.

9.2 账号申请及创建

9.2 Account Application and Creation

9.2.1 申请账号

9.2.1 Applying for an Account

员工在填写《IT 账号开通及变更申请表》后，经由申请人部门负责人、逻辑安全管理员、安全总监审核通过后，逻辑安全管理员才能创建员工账号并启用，客户账号由计划管理部客户服务组提出账号申请。数据接收服务器不允许申请个人账户，保证个人账户和客户账户严格隔离。

After the employee fills in the *Application Form for IT Account Opening and Change*, the Logical Security Administrator can create and activate the employee account only after it is approved by the head of the applicant's department, logical security administrator and security director. The customer account is applied for by the Customer Service Group of the Planning and Management Department. The data receiving server is not allowed to apply for personal accounts to ensure strict isolation between personal accounts and customer accounts.

9.2.2 创建账号

9.2.2 Create an Account

逻辑安全管理员创建账号时应填写《IT 账号管理记录表》，账号必须设置以下内容：

The logical security administrator shall fill in the *IT Account Management Record Form* when creating an account. The account number must be set with the following contents:

- 密码长度必须为 8 个字符或以上

  Password length must be 8 characters or more

- 账号并发登录数为 1

  The number of concurrent login accounts is 1

- 密码必须设置为复杂密码（包含大小写字母、数字、特殊符号中的三种）

  The password must be complex (including three types, upper and lower case letters, numbers and special symbols)

- 首次登陆必须修改初始密码

  The initial password must be changed for the first login

- 密码有效期为 90 天

  The password is valid for 90 days

- 生产网络个人化区与 DMZ 区之间的防火墙管理密码必须独一无二

  The firewall management password between the personalization area and DMZ area of the production network must be unique

- 客户账号登录 6 次错误则自动锁定账号

  The account will be locked automatically if the customer's account is incorrectly logged in for 6 times

- 客户账号登录后五分钟内未操作将自动连接超时

  If the customer account is not operated within five minutes after logging in, the automatic connection will timeout

9.2.3 IT 设备账号

9.2.3 IT Equipment Account

a) 所有 IT 设备的 Administrator 账号密码必须由两位逻辑安全管理员按双控原则设置。

a）The administrator account of all IT equipment is forbidden to use in management and daily operation. The administrator account password must be set by two Logical

Security Administrators according to double control principle.

b) 任何 IT 设备账号创建前需填写《IT 账号开通/变更申请表》，经申请者部门负责人逻辑安全管理员、安全总监授权后由逻辑安全管理员创建账号，使用者首次登陆后必须更改账号初始密码。

b) Before any IT equipment account is created, the *Application Form for IT Account Opening and Change* must be filled in. The account shall be created by the Logical Security Administrator after authorized by the Logical Security Administrator, head of the applicant's department, and Security Director. Users must change the initial password of the account after logging in for the first time.

9.3 账号及密码变更

9.3 Account and Password Change

9.3.1 账号变更

9.3.1 Account Change

当公司员工职务发生变动或客户账号信息需要修改时，员工应填写《IT 账号开通/变更申请表》，客户账号的变更申请由计划管理部提出并填写。

When the position of the company's employees changes or the customer account information needs to be modified, the employees shall fill in the *Application Form for IT Account Opening and Change*, and the change application for the customer account shall be submitted and filled in by the Plan Management Department.

员工发生职务变动或离职时，人力资源管理部必须在 1 天内通知逻辑安全管理员，逻辑安全管理员在收到通知后必须在 1 天内锁定该员工账号并填写《IT 账号管理记录表》。

When an employee changes his/her position or leaves his/her job, the Human Resources Management Department must notify the Logical Security Administrator

within 1 day. The Logical Security Administrator must lock the employee's account and fill in the *IT Account Management Record Form* within 1 day after receiving the notification.

经锁定的账号必须填写《IT 账号开通/变更申请表》并经授权后，逻辑安全管理员才能执行变更操作。

For the locked account, the *Application Form for IT Account Opening/Change* shall be filled in and being authorized before the Logical Security Administrator performing the change operation.

9.3.2 密码变更

9.3.2 Password Change

账号使用者必须妥善保管账号密码，允许账号使用者更改密码，密码修改必须和前四次使用密码不一致，若使用者账号密码忘记或遭泄露、篡改，密码的重置按以下流程执行：

The account user must properly keep the account password and is allowed to change the password. The password change must be inconsistent with the previous four passwords. If the user's account password is forgotten or leaked or tampered with, the password reset shall be carried out according to the following procedures:

- 申请者填写《IT 账号开通/变更申请表》且经签字授权

  The applicant fills in the *Application Form for IT Account Opening/Change* which is authorized by signature.

- 逻辑安全管理员按申请变更内容操作，并填写《IT 账号管理记录表》

  The Logical Security Administrator shall operate according to the content of the change application and fill in the *IT Account Management Record*.

9.4 账号锁定及撤销

9.4 Account Locking and Cancellation

9.4.1 锁定账号

9.4.1 Account Locking

- 若已知公司员工将休假、出差或其他原因未使用账号超过一个月，人力资源管理部必须在 2 天内通知逻辑安全管理员。

  If it is known that the account of an employee of the company is not used for more than one month due to that he/she will be on vacation, on business trips or for other reasons, the Human Resources Management Department must notify the Logical Security Administrator within 2 days.

- 若客户将暂停业务合作或超过一个月未使用账号，计划管理部必须在 2 天内通知逻辑安全管理员。

  If the customer will suspend business cooperation or has not used the account for more than one month, the Plan Management Department must notify the Logical Security Administrator within 2 days.

- 逻辑安全管理员收到通知后应在 1 天内锁定该使用者所有账号并填写《IT 账号管理记录表》。

  After receiving the notification, the Logical Security Administrator shall lock all accounts of the user and fill in the *IT Account Management Record* within 1 day.

- 逻辑安全管理员必须每周检查一次账号使用情况并填写《IT 日常检查记录表》，若发现超过 90 天未活动账号，必须立即锁定该账号并填写《IT 账号管理记录表》。

  The Logical Security Administrator must check the account usage once a week and fill in the *IT Routine Inspection Record*. If it is found that the account has not been active for more than 90 days, the account must be locked immediately and the *IT Account Management Record* must be filled in.

9.4.2 撤销账号

9.4.2 Account Cancellation

- 若与客户的业务合作停止或员工辞职离开公司，人力资源管理部必须在 2 天内通知逻辑安全管理员

  If the business cooperation with the customer stops or the employee resigns and leaves the company, the Human Resources Management Department must notify the Logical Security Administrator within 2 days.
- 逻辑安全管理员在收到通知后必须在 1 天之内完成账号的撤销工作。

  The Logical Security Administrator must complete the account cancellation within 1 day after receiving the notification.
- 逻辑安全管理员每周检查账号使用情况时，若发现超过 90 天未活动，必须立即注销该账号并填写《IT 账号管理记录表》。

  When the Logical Security Administrator checks the usage of the account every week, if he/she finds that the account has not been active for more than 90 days, he/she must immediately cancel the account and fill in the *IT Account Management Record*.

10 审查管理

10 Review Management

逻辑安全管理员应每周对关键设备审查一次，包括访问控制、变更记录等。

The Logical Security Administrator shall review the key equipment once a week, including access control, change records, etc.

- 防火墙配置及日志

  Firewall configuration and log
- 服务器配置及日志

Server configuration and log

- 数据处理记录

  Data processing record

- 数据接收记录

  Data receiving record

- 数据删除记录

  Data deletion record

- 机台终端数据操作记录

  Machine terminal data operation record

首席信息安全官应每季度检查一次所有的记录文件是否达到记录要求。

The Chief Information Security Officer shall check every quarter whether all records meet the recording requirements.

11 日志管理

11 Log Management

- 日志管理主要由日志服务器和日志备份完成

  Log management is mainly completed by the log server and log backup.

- 所有日志能在线访问前 3 个月内，通过文件能查询到至少 1 年的日志

  All logs within 3 months can be accessed online, and the logs of at least 1 year can be searched through files.

- 日志的保存期限为 1 年，1 年前的日志文件没有特别说明、没有人员提出查询，将做删除处理并填写《日志销毁记录表》；

  The storage period of the backup files of remote disaster recovery is 1 year. For the files of 1 year ago, if there are no special notes, or no one has proposed to use, the files will be deleted and the *Log Destruction Record* should be filled.

- 所有日志实时由日志服务器管理和存储

  All logs are managed and stored by the log server in real time

- 所有日志每周自动备份至日志备份服务器

  All logs are manually backed up weekly

- 仅日志管理员可审计日志，非授权人员禁止访问任何日志

  Only log administrators can audit the logs, and unauthorized personnel are prohibited from accessing any log

a)日志审计

a) Log audit

日志管理员每周审计以下日志：

The log administrators audit the following logs weekly:

- 数据活动审查：数据接收、数据准备、数据删除

  Review of data activities: data reception, data preparation and data deletion

- 网络状态日志审查：网络阻塞记录

  Log review for network status: network blocking records

- 系统登录日志：设备登录日志、FTP 登录日志、VPN 连接日志

  System login log: device login log, FTP log, VPN connection log

- 变更日志：包括系统、设备配置变动记录

  Change log: including change records of system and equipment configuration

12 相关/支持性文件

12 Related/Supportive Documents

《存储介质管理程序》

Storage Medium Management Program

《网络配置授权书》

Network Configuration Authorization

《IT 设备进出流程》

IT Device Access Process

13 表单

13 Forms

《无线热点扫描统计表》

Wireless Hotspot Scanning Statistics

《IT 日常检查记录表》

IT Routine Inspection Record

《IT 设备安装及变更申请表》

Application Form for Installation and Change of IT Equipment

《IT 固定资产统计表》

IT Fixed Assets Statistics Form

《IT 设备检查报告》

IT Device Inspection Report

《计算机档案记录表》

Computer File Record

《数据备份记录表》

Data Backup Record

《IT 故障报修申请表》

Application Form for repairing IT faults

《IT 设备运输申请表》

IT Device Transportation Application Form

《补丁及病毒库更新记录表》

Patch and Virus Database Update Record

《机房进出申请表》

Room Access Application Form

《机房进出记录表》

Room Access Record

《IT 账号开通及变更申请表》

Application Form for Opening and Changing IT Account

《IT 账号管理记录表》

IT Account Management Record

《日志销毁记录表》

Log Destruction Record