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

存储介质管理标准

Storage Medium Management Standard

文件种类：管制文件 File Type: controlled document

文 件 编 号: **KD-MLJ-02**

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: **A5**

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**

文件种类：管制文件 File Type: controlled document   2

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	李永量 Li Yongliang
4.3.5, 4.4	A/1	1.格式调整 1.Format adjustment 2.删除 4.3.5 项笔记本管理 2. Delete 4.3.5 laptop management	2016/03/11	曹良攀 Cao Liangpan	刘劲松 Liu Jinsong	李永量 Li Yongliang
4.3.6-4.3.9	A/2	新增办公区域移动存储介质管理条例 New management regulations on removable storage medium in office area	2016/06/21	徐锐 Xu Rui	刘劲松 Liu Jinsong	李永量 Li Yongliang
4.3.7-8 4.2	A/3	新增涉密介质条例 New confidential medium regulations	2017/2/24	徐锐 Xu Rui	刘劲松 Liu Jinsong	崔云峰 Cui Yunfeng
/	A/4	更换 log 及公司名称 Change log and company name	2018/7/25	王建勋 Wang Jianxun	刘劲松 Liu Jinsong	崔云峰 Cui Yunfeng
All	A/5	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

文件种类：管制文件 File Type: controlled document

1 目的

1 Purpose

为加强数据信息的安全管理，保证数据信息的可用性、完整性、机密性依据 PCI 及 GSMA 要求及生产中心实际情况，特制定以下《存储介质管理程序》,完善逻辑安全管理。

To strengthen the security management of data information and ensure its availability, integrity, confidentiality, the *Storage Medium Management Program* is hereby formulated to improve the logical security management based on the requirements of the PCI and GSMA

2 适用范围

2 Application Scope

这项政策适用于生产中心所有的可移动存储设备，并适用于资料、数据的储存，公司数据及生产中心数据机房、个人化数据相关作业过程。

This policy applies to the related operation process such as all portable storage devices in the production center, data storage, corporate data, production center's data machine room and personalized data.

3 职能职责

3 Duties and Responsibilities

逻辑安全管理员：负责所有可移动存储介质统一管控、分配，监督可移动存储介质的使用，制定修改存储介质管理程序。

Logic Security Administrator: Responsible for uniformly managing and distributing all removable storage media, monitoring the use of removable storage media, and formulating and modifying storage media management program.

文件种类：管制文件 File Type: controlled document

密级: 1 级 内部

安全策略部总监：负责监督及授权可移动存储介质的使用，定时对移动介质的使用记录审查。

Security Policy Director: Responsible for supervising and authorizing removable storage medium use, and regularly reviewing the usage record of removable medium

4 可移动存储介质管理

4 Removable Storage Medium Management

4.1 定义

4.1 Definition

包括便携硬盘、软盘、笔记本电脑、手机、光盘、存储卡、USB 存储设备等所有可移动存储设备。特殊情况下因工作必须使用须填写《媒介及 Psam 卡使用申请表》，必须清晰地标识。

Removable storage devices include portable hard disk, floppy disk, laptop, cell phone, CD, storage card and USB storage devices.

4.2 可移动存储介质编号

4.2 Removable storage medium number

公司数据及生产中心禁止任何人员使用未受控可移动存储设备，所有的可移动存储设备在采购或调配后，由逻辑安全管理员统一编号保存管理，逻辑安全管理员更新《IT 固定资产统计表》，移动介质编号中必须包括安全等级。

Any usage of uncontrolled removable devices is prohibited by the data and production center of the company. All removable devices shall be numbered by the logical security administrator after being purchased or deployed. The logical security administrator shall update the IT Fixed Asset Statistic Form, and the security level must be involved.

编号表示方式：如 CDJK-S01-05-012-001（LV1）

Numbering representation: e.g. CDJK-S01-05-012-001 (LV1)

保密等级分级：

Security level classification:

LV0：公开（所有人均可访问和知晓）

LV0: Public (permit access and knowledgement of anyone)

LV1：内部（仅公司内部员工可以知晓）

LV1: Internal (only exposed to internal staff of the company)

LV2 秘密：（仅公司少数授权人员可以知晓）

LV2: Secret (exposed to an authorized staffs)

LV3：机密（与机密内容有直接关系的工作岗位人员）

LV3: Confidential Direct connection to this confidential Normal Asset.

LV4：绝密（与绝密内容有直接关系的工作岗位人员）

LV4：Top-secret Direct connection to this top-secret Normal Asset.

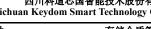# 4.3 可移动存储介质的管理

4.3 Removable storage medium management

4.3.1 在生产区及高级安全区禁止使用任何未受控的可移动存储设备。

4.3.1 Usage of any uncontrolled removable storage device in the production area and advanced security zone is prohibited.

4.3.2 若因工作或业务需要，在生产区或高安全区使用笔记本、可移动存储设备（U 盘、光盘、硬盘）、加密狗、Psam 卡时，使用人必须向安全策略部申请并填写《媒介/PSAM 卡使用申请表》，经部门负责人、逻辑安全管理员和安全策略部总监审批通过后，由逻辑安全管理员分配专用可移动存储介质。

4.3.2 When using the laptop, removable storage devices (U disk, CD-ROM, hard disk), dongle, Psam card in the production area or a high security zone if they are required by the work or business, the user must apply to Security Policy Department and fill the *Media/ PSAM Card Application Form*. On approval of the head of the department, logical security administrator and director of Security

文件种类：管制文件 File Type: controlled document

Policy Department, logical security administrator assign the dedicated removable storage media.

4.3.3 在使用介质前，逻辑安全管理员必须先检查介质中有无数据，使用人确认无误后立刻进入存储介质使用程序，逻辑安全员须全程监督移动介质的使用情况，再有需要使用移动介质时交由其使用。

4.3.3 Before the medium is used, logical security administrator must first check whether it contains data. After confirmation, the user can access to the storage medium under full supervision of the logical security administrator who can hand over the removable device to the user again when necessary.

4.3.4 在可移动存储介质使用完毕后由安全策略部收回，收回后的存储介质，逻辑安全管理员必须使用删除软件执行不可恢复删除操作（包括 U 盘中的隐藏文件，删除后必须格式化介质，整改过程由两名逻辑安全员双控完成并填写《存储介质数据删除及销毁记录表》。

4.3.4 The removable storage medium needs to be returned to the Security Policy Department. For the used medium, the logical security administrator must use the deletion software to permanently delete data including hiding files in the USB, after which the medium shall be formatted. The whole process is operated by two logical security administrators who fill in the Record on Deletion and Destruction of Storage Medium Data when accomplished.

4.3.5 若可存储介质中的敏感或机密数据无法删除，应完全粉碎销毁设备，确保数据无法恢复，整个过程由两名逻辑安全管理员双控完成，并检查填写《存储介质数据删除及销毁记录表》

4.3.5 If the storage medium contains sensitive or confidential data that cannot be deleted, destroy the device by completely shattering it to ensure that the data cannot be recovered. The entire process is operated by two logical security administrators who fill in the Record on Deletion and Destruction of Storage Medium Data when accomplished.

4.3.6 所有涉密移动介质由安全策略部保管，空闲的涉密移动介质放置在保险柜

中，每次访问移动介质必须填写《媒介/PSAM 卡使用申请表》。

4.3.6 All classified removable media must be kept by the Security Policy Department with available classified removable media being placed in the safe. Each access to a removable medium must be recorded in the *Removable Medium Usage Registration Form*.

4.3.7 所有涉密移动介质只能在本单位的涉密计算机或涉密信息系统中使用，严禁借给外单位或转借他人使用。

4.3.7 All classified media can only be used in confidential computers or confidential information system within the company. lending them to other units or person is prohibited.

4.3.8 在生产区及高级安全区禁止使用外来 U 盘，若因工作或业务需要时，可以按照上述流程向安全策略部申请专用的保密 U 盘，将需要的数据导入保密 U 盘即可。

4.3.8 External USB Flash Drive is not allowed to use in production areas and advanced security areas. A specific confidential USB Flash Drive can be applied in accordance with the above procedure from the Security Policy Department. You may import the data needed to the confidential USB Flash Drive.

4.3.9 办公区域存储介质必须有独立编号，并在《IT 固定资产统计表》中作出详细记录，个人的存储介质不属于公司财产。

4.3.9 The storage media of office areas must be individually numbered and recorded in detail in the *IT Fixed Asset Statistic Form*. And personal storage media do not belong to the company.

4.3.10 个人需要在办公区域首次使用的可移动存储介质，必须经过安全策略部检查并登记更新到《存储介质信息记录表》，安全策略部有权利对已获得许可的员工个人电脑在内的存储介质不定时检查，所属人应当配合工作。

4.3.10 If a removable storage medium is used for the first time in the office area due to personal need, it must be inspected by the Security Policy Department and recorded in the *Storage Medium Information Record*. The Security Policy

Department has the right to conduct unscheduled inspection on the storage medium and the medium owner shall be cooperative.

4.3.11 员工个人可移动存储介质中与公司有关的文档资料、技术秘密、经营秘密、或其他商业秘密等其所有权均属于公司，申请人应严格遵守公司有关保密制度和协议的规定，不得向任何第三方泄露。

4.3.11 For personal removable storage media, the data related to the company such as documents, technology secrets, business operation secrets, and other trade secrets belong to the company. The applicant shall strictly comply with the provisions and agreements on secrecy and must not disclose to any third party.

4.3.12 员工个人可移动存储介质由个人自行保管与维护，丢失和损坏责任自负。且不能由于个人使用或其他客观原因影响工作，出现故障时应及时维修，日常维护维修及增加配置的费用须由个人承担。

4.3.12 The employees should keep and maintain their personal removable storage media. and liable for loss and damage. The device shall be immediately maintained due to personal usage or other objective factors retarding the work. The cost of routine maintenance and additional configuration is borne personally.

4.4 纸质介质

Paper Medium

a. 所有在高级安全区域机密或极机密资料、文档禁止外出 For the classification of confidential or extremely confidential information and document in the advanced security zone which cannot be sent out, please see the Data Grade Classification.

b. 若在业务必须情况下，进出或访问前必须有授权人士的同意签字，并记录过程。

If they must be accessed due to business demands, it must be approved and signed by the authorized person and the whole process shall be recorded.

c. 纸质介质销毁必须在双控下粉碎，并详细记录。

Paper medium must be destroyed under dual control, and recorded in detail.

4.5 外来的存储介质

Foreign Storage Medium

a. 外来的存储介质必须记录，若因工作的需要进入生产区域的，必须检查并得到批准通过后方可进入，且需安全人员陪同并全程监督。

The Foreign storage media must be recorded, checked and approved if it needs to enter the production area due to work demands, and accompanied and supervised by the security officer in the whole process.

b. 安全人员必须确保介质不会接触到敏感信息。

The security officer must make sure that the medium will not contact with any sensitive information.

c. 出安全区域后安全人员必须对介质进行检查，是否有可能被泄密的可能。

The security officer must check the medium after it leaves the security zone for the possibility of disclosure of confidentiality.

d. 外来的存储介质包括所有可移动介质。（如笔记本、平板电脑）

Foreign storage medium includes all mobile media. (such as laptop computer, tablet computer)

e. 外来介质管理必须遵循以上的要求。

The management of foreign medium must meet above requirements.

f. 以上的管理必须有清晰的程序进行控制，必须有书面的记录证明符合该项要求。

Above management must be controlled by a clear program, and a written record must be provided to prove it meets the requirement.

5 相关表格

Related Forms

《媒介/PSAM 卡使用申请表》

Media/ PSAM Card Application Form

《存储介质数据删除及销毁记录表》

Record on Deletion and destruction of Storage Medium Data

《生产区域 IT 设备清单》

IT Fixed Assets Statistics Form

文件种类：管制文件 File Type: controlled document

密级:1 级 内部