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

生产数据安全管理标准

Pro. Data Security Mgt. Standard

批注 [u1]: 科道芯国 官网上并没有明确给出公司的英文名称。
我们在官网【对外生产与制造】版块找到至少两种不同的说法：
1. Sichuan precision intelligent technology Limited by Share Ltd
此为官网【质量管理】版块的译法。
2. Jing King Technology Holdings Ltd.
此为官网【资质】版块的译法。

但是这两种说法都与科道芯国的商标“KEYDOM”不相符，所以无法确定该公司的正式英文名称，暂时以商标为准，译为：Sichuan Keydom Smart Technology Co., Ltd

文 件 编 号: KD-MSC-02

Doc. No.:

编 制:

Prepared by:

审 核:

Reviewed by:

批 准:

Approved by:

版本 /修订状态: A1

Rev./Revision status:

受 控 状 态:

Controlled status:

2020 年 1 月 1 日发布　　2020 年 1 月 1 日实施

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

修订历史记录 Document Changes

序号 No.	日期 Date	修订内容 Description of Change	版本 Version	编制 Made by	审核 Reviewed by	批准 Approved by
01	2019.9.2	初版制定 First edition	A0	胡廷军	唐联果	陈为明
02	2019.12.29	更改文件格式	A1	胡廷军	唐联果	陈为明
03						
04						
05						
06						
07						
08						

目　录 Table of Content

1. 目的 Purpose

为保证公司生产中心个人化系统中各类数据文件的安全，并规范此类数据文件的管理，特制定本管理标准。

Specially make this standard to ensure the security and management of all kind data and document within personalization system of Production Center .

2. 范围 Scope

本标准规定了公司生产中心个人化系统中各类数据文件分类和安全管理相关的职责、管理内容与要求 ，适用于 2 级预个人化网络和 3 级个人化。（以下简称本标准）。

It defines the responsibility, management procedures and requirements related to all kinds of data doc. classification and security mgt. used for Level 2 pre-personalization network and Level 3 personalization network.

3. 术语和定义 Definition

3. 1. 数据密级 Data Classification

上述网络中涉及的信息/数据等级具体如下：The information/data classification involved in the above network is as follows:

- Level 0：公共数据。Public Data
- Level1：内部数据，仅能对公司内部员工发布，可以在生产工作中查看的数据，如生产计划安排等。Internal Data: only can be available to internal employees, and data that can be viewed in production, such as production scheduling, etc.
- Level2：秘密数据，有限人员可获得，且在传输过程中需加密。涉及公司和客户生产经营安全的数据，只允许授权人员访问和使用，一旦泄露会给公司和客户带来经

济上的损失和企业形象的负面影响，如涉及客户的报表、商务合同等。Secret Data: it is limited to some personnel and must be encrypted during transmission. Data that related to production and business of company and customer is only allowed authorized personnel to access and use, once the leak can bring economic loss and negative effects to company and customer, such as involving the report and business contract of customer.

- Level3：机密数据，仅文件使用者可获得，或任何人都不能单独掌握。加密存储使用，使用完毕后，必须被安全销毁。涉及公司和客户重大利益关系的数据，只允许少数授权人员在双人双控的情况下访问和使用，一旦泄露将会给公司和客户带来较大的经济损失和负面影响，如持卡人数据等。Confidential Data: it is limited to the personnel needing to use and subjected to knowledge split, it will be securely destroyed after use. Data that related to major interests of company and customer is only allowed a handful of authorized personnel access and use in the case of double control, once the leak will bring large economic loss and negative effects to company and customer, such as cardholder data.

- Level4：绝密数据，仅工作相关人员可获取，加密传输、存储使用，需销毁时使用安全销毁措施。涉及公司经营层面的关键信息，如公司主要投资、项目重组等关系到股价变动的重大信息，仅限董事会成员、高管及工作相关人员获取。Top-secret Data: It is limited to related working personnel; it should be encrypted during storage and transmission and securely destroyed after use. Key information related to the company's operation level, such as major investment, project restructuring and other important information related to share price changes, is only restricted to board members, executives and relevant personnel.

3. 2. 存储介质 Storage Media

用于存储数据的媒介。如：磁盘、移动硬盘、刻录光盘等。

It refers to the media which is use for data storage. Such as: disc, removable media and so on.

3. 3. 卡组织 Card Organization (shortened as CO)

指 GSMA、中国银联、VISA 国际组织、JCB 国际组织，美国运通，万事达国际组织。

It refers to GSMA, China Union Pay, Visa International Organization, MasterCard International Organization, Amex, JCB etc.

4. 管理职责 Mgt. Responsibilities

4. 1. 安全策略部 IT 职责 IT of Security Policy Dept.

- 协助本标准的制修订。To assist to revise this standard.
- 负责按照卡组织要求，严格执行本管理标准，并提供技术实施层面的保障。Be responsible for executing this standard and provide safeguard on technology level according to COs' requirements.
- 负责搭建维护个人化网络和 IT 设备，提供安全的数据接收、使用、存储环境。Be responsible for personalization network, IT equipment construction and maintenance and safeguarding the security environment for data receipt, using and storage.
- 负责确保日常工作记录与本标准的符合性。To ensure that all the daily work records are compliance with this standard.

4. 2. 安全策略部逻辑职责 Logical Security Officer (shortened as LSO) of Security Policy Dept.

- 安全策略部是逻辑安全的管理职责部门。Security Policy Dept. is logical security responsible dept.
- 负责按照卡组织的要求，组织数据组、安全策略部制（修）定本管理标准，并监督

检查本标准各环节内容的执行情况。To organize IT and data team to revise this standard according to requirements of Cos and supervise the implementation of this standard.

- 对涉及个人化数据文件的安全管理工作的监督和检查。To supervise and inspect security management work of data files related to personalization system.
- 包含监督个人化数据存储介质的物理销毁。To physical destruct data storage medium that contains supervision of personalization system.

4.3. 数据组职责 Data Team ofPersonalization Dept. of Pro. Center

- 负责个人化系统中各类数据文件分类保护的实施或执行。To execute or implement all the protective measures related to data and doc classification within personalization systems.
- 数据主管负责，监督检查本部门对本标准的执行情况，并建立检查记录；确保个人化系统内，数据流程与记录的合规性。Data Supervisor should check the performance of the implementation of this standard and maintain records to ensure the compliance of data processes and records within personalization systems.
- 负责在双控环境下，对各类个人化数据进行销毁和删除。To delete and destroy personalization data under dual control.

4.4. 其他部门职责 Other Depts.

- 各部门负责部门内文件的管理与安全控制。To implement internal doc mgt. and security control.

5. 管理内容与要求 Mgt. Processes and Requirements

5.1. 数据文件的存在形式 Data Form

个人化系统内各类数据文件，可以电子形式或纸质形式存在：

All kinds of data could be in electronic file or paper file within personalization system:

- 电子形式的文件包括：个人化数据、服务器系统日志、证书/密钥组件、操作系统备份和各类工具软件等。Data in electronic file includes: personalization data, server system logs, certificate/key components, operation system back-ups and all kinds of tool software etc.
- 纸质文件包括：卡组织的安全标准、技术文件（卡片设计指南）、发卡机构的商业文件（打卡通知单、生产通知单、订单数据）、公司的凭证文件（产品交接单、生产过程记录单、产品发票、管理标准）、供应商的机密数据（PIN 信封）等。Data in paper file includes: security standards from COs, technology docs (card design guide), business docs of card issuers (notices of sample request, card production and order), Tianyu's certificating docs (product interchange receipts, pro records, product invoices and mgt. standards), vendor secret data (PIN mailer) etc.

5. 2. 数据文件的安全控制 Security Control for Data

5.2.1. 总要求: General Requirements

- 个人化系统内所使用和产生的一切数据文件都必须参照公司分类标准对其进行安全等级的定义并标记。The data used and generated within personalization system must be labeled with security level according to classification standard.
- 第三方访问支付组织或发卡机构的涉密数据文件，必须经过相应的安全评估，参见《数据访问申请表》，并获得支付组织或发卡机构的书面授权。All third party accesses to limited data belonging to COs or card issuers is not allowed until relevant security assessment by Data Access Applicant is completed and get written approval from COs or card issuer.

- 数据组必须将备份的数据文件保存在安全的位置，并采取适当措施防止非授权访问。Data team must store the data back-up in security place and take measure to prevent unauthorized access.
- 公司所有员工必须签订并遵守《保密协议》。All employees must sign and comply with the Employee Confidential Agreement.

5.2.2. 文件的备份和标注 Backup and Labelling of Doc

- 个人化网络系统中需进行备份的数据包括：各类系统数据、客户要求备份的个人化数据、传输系统日志、密钥管理系统日志、及各类日志等。The data needing to be backed-up within personalization network system includes: all kinds of system data, transmission system logs, KMS logs and other logs etc. Back up personalization data if customer requires.
- 所有备份的个人化数据应进行加密，且在规定的时间内安全删除。Encrypt all the bake-up of personalization data, and safely delete the data within specified time..
- 异地备份数据的销毁和使用，应遵循相关批准手续，如实保留记录。Destruction and use of all the off-site data backup should be subjected to relevant approving procedure, and keep destruction and use record.
- 所有与个人化生产相关的数据备份活动，由数据组在《数据转移处理进度表》上作好记录。数据组对数据进行备份，应按照随时可以重建的方式进行，所备份文件必须确保安全，未授权人员不能访问。Data team should record all the back-up activities related to personalization production system on Data Backing-up Record. Data team should back up data by method guaranteeing recovery. Ensure the security of all the backup and limit all the backup to authorized personnel only.
- 备份的数据文件若安全等级发生变化时，保管部门应对数据文件的安全标记进行更新。To update the security level identifier of data document backups according to

changes of security level.

- 2 级或 2 级以上数据的备份工作，应由双人控制执行。It is must under dual control to back up the data above level 2.
- 数据组应对所备份的个人化数据和日志进行清晰的标注和分类。Data team should clearly label and classify the backup of personalization data and log.
- 数据的存储介质应该设置防篡改。The storage media with data should be tamper proofing.

5.2.3. 文件标记与处理 Doc. Labelling and Processing

- 数据组负责对所保存的个人化系统内的所有数据文件进行分类和标记并归档。Data team is responsible for classifying, labeling and filing all data docs stored within personalization systems.
- 存储的所有三级安全数据，需添加额外的保护措施，以防止数据遭到未经授权的篡改。To take additional measures to prevent data from unauthorized tempering for all level 3 security data should taking.
- 与客户进行往来的纸质凭证应标记相应分类等级。To label all paper certificate related to exchange with customer to indicate security level.

5.2.4. 登记制度 Registration

- 数据组负责对经批准的备份数据的使用进行登记，并填写《数据转移处理进度表》。Data team is responsible for registering all the use of data backup approved and make record on Data Backup Use Record.
- 安全策略部负责统计生产网络所有存储介质数量，内容，建立《存储介质管理日志记录》形成台账进行管控；安全策略部负责监督记录的一致性，并协助进行介质销毁的双控。Security Policy dept. is responsible for maintaining a clear inventory for all

storage medias within pro network and making record on Storage Media Management Log Record.Security Policy dept. also should verify the accuracy and authenticity of the record and supervising the process of media destruction.

6. 个人化数据流转要求 Requirement for the Flowing of Personalization Data

6.1. 数据传输 Data Transmission

- 数据传输按照客户安全要求建立，安全要求不能低于卡组织的规定。To establish data transmission according to customer's requirements which should not be looser than the requirements of Cos.
- 使用数据共享服务，须遵循安全加密及数据完整性的原则，除 SIM 卡外，禁止使用 FTP 数据传输方式，应使用安全的 SFTP 数据传输方式。It is the basic principle to follow the security encryption and data integrity for using data sharing service. Do use SFTP but not FTP for data transmission except sim card.
- 数据传输过程中，必须保证线路的冗余性和安全性，传输数据必须进行加密。 To ensure the redundancy and security of data transmission line used for data transmission. All the data transmitted must be encrypted.
- 用 PGP/GPG 加解密数据文件前，与发卡商之间必须进行公钥交换。一般来说，PGP/GPG 用于数据包加密。Public keys must be exchanged with issuer before encrypt the data document by PGP/GPG. Generally, the PGP/GPG is used for data encryption.
- 可采取以下数据传输协议应用于数据传输：Below data transmission protocols could be used for data transmission:

a. 安全文件传输协议 Security File Transfer Protocol

b. 带 IPSec 的虚拟私网 Virtual private network with IPSec

c. 其他安全协议例如 SSH Other security protocols such as SSH

- 生产中心应与客户之间协商数据传输方式，建立专线或 VPN 等数据传输方式，或者由专人双控取送；所有数据以密文形式通过加密的链路或安全的渠道进行传输。Pro Center should negotiate with customer about the data transmission methods, such as establishing private line, VPN or dual personnel. All the data should be cipher text and be transmitted through encrypted lines or other security channels.
- 生产中心应设置单独的数据收发服务器，用于同客户之间的数据传输，其与外部传输网络和内部生产网络之间均必须通过防火墙隔离。Pro Center should set separate data receive and dispatch servers for data transmission between different customers. Separate it from external transmission network and internal pro network by firewalls.
- 如果通过拨号方式，需要客户提供书面需求文档。客户端要求文件数据传输活动时，拨号调制解调器才能打开。数据文件传输完成后，调制解调器将关闭。Dial mode is prohibited unless provide written request doc customer. Turn on the dial modern only when client request to transmit data. Turn off it once data transmission completed.
- 接收加密的持卡人数据文件或存储媒介后，必须检查数据或媒介完整性，保证数据文件或媒介没有被篡改。Verify the integrity of the data or media after received encrypted card holder data or media to ensure that data documents or media have not been tampered.
- 建立确保数据传输和接收真实性、完整性的验证机制。对于持卡人数据文件完整性的检查，必须验证以下项目，保证文件完整性：To establish mechanism for verifying the authenticity and integrity of data transmission and receipt. Below information must be verified to ensure the integrity of card holder data docs.

a. 文件日期和时间戳 Doc date and time

b. 文件名 Doc name

c. 文件大小 Doc size

d. 接受的文件数量 Quantity of doc received

- 根据发卡商要求校验文件完整性，如：MD5、SHA 或由 PGP 数据包自带的完整性功能来校验。To verify doc authenticity according to issuer's requirements, such as MD5 or SHA.
- 生产中心接收数据的来源必须确保安全，传输账户的建立必须经过批准，并定期审核。传输账户应有 IP 地址绑定等安全控制措施，以确保数据源的真实性。In order to ensure that the source of data received by Pro Center is security, the creation of transmission accounts must be approved and audited regularly. Take security control measures for transmission accounts to ensure the authentication of data source, such as IP address binding.
- 如果文件没有成功传输，或只有部分的数据被接收，接受者务必联系项目信息反馈接口人。当文件没有成功被接收时，应尽快地通知银行或授权的信息处理人员。任何接收的不完整的数据，必须在双控条件下安全删除 The recipients must contact with the project info feedback personnel if transmission is failure or only partial data is been received. To notify issuer or authorized responsible info treatment while docs are not be received successfully. Delete all incomplete data received under dual control.
- 个人化生产系统内部的，持卡人数据传输和使用，必须以密文形式进行，使用完毕后后立即删除该数据。The card-holder's info (including eSim platform data) must be cipher text during transmission and used within personalization pro system of Pro Center. Delete the data immediately after used.
- 对于远程加密传输系统与生产内部加密体制不一致的客户，需建立数据文件加密体制转换平台。两加密系统之间的加密体制的转换必须在同台机器中进行，文件解密

与加密动作必须在同一台设备中连续进行，不允许有人为中断的操作，以实现明文数据不落地、不露明。处理过的数据应在数据处理完成后立即删除。Establish encryption mechanism conversion platform for the customers whose remote encryption transmission systems are different with pro center's internal encryption mechanisms. The conversion for different encryption mechanism of two encryption systems must be on the same machine dedicated. The decryption and encryption activities must happen within the same machine continuously, no interruption is permitted to achieve a goal of no clear data fell. The data processed should be deleted immediately after the process.

- 数据加密体制转换和传输应由专人负责，设备应专机专用。To designate one employee to be responsible for data encryption system transfer or transmission. Machine must be dedicated.
- 妥善保管电子日志，确因业务需要从生产环境中获取电子日志的，必须办理审批手续，由两名以上员工共同操作，并在专有指定环境中安全使用电子日志。所有日志不得带离现场，应保存至少两年。To keep electronic log appropriately. All access to electronic loges within pro. environment for business need should be approved and under dual control. Use electronic logs in dedicated secure environment. Log is retained for at least two year and is prohibited to be taken away.
- 数据组对数据的接收活动，必须保留数据处理日志，至少包括接受日期、接收时间、数据文件所有人（客户或发卡商）、文件名、文件大小。Data team should keep data process logs for data receipt activities. Logs should include received date and time, data owner (customer or issuer), name and size at least.

6.2. 数据处理 Data Processing

- 数据处理必须由授权的专人负责，在指定的数据室进行。分别设置数据生成人员和审核人员，处理过程双重控制由系统自动完成。处理系统应专机专用，除系统自动

产生监控日志外，操作人员必须填写数据生成日志表，包括姓名、处理时间等信息。Data must be processed by authorized and dedicated employees and within dedicated data room. To designate data generating personnel and checking personnel for data processing. System will enforce dual-control automatically. Except monitoring loges generated by system, manual logs should be maintained including name, time and so on.

- 金融卡数据使用分配前，需确认分配数量后才可进行分配处理。如需匹配照片项目需核实照片是否符合写卡要求容量标准，保证照片数量与待分配数据相符。To confirm the allocation quantity prior to the banking card data processing allocation. Verify that if the photos compliance with the card writing capacity standard for the program needing photography matching to ensure that the photography quantity is matched with the data waiting for allocation.

- 数据加密应使用符合国家商密管理的要求，或满足 FIPS140-II 以上要求的加密产品，用于交付客户的数据文件，应使用客户统一要求的加密产品，对数据文件进行加密。Data must be encrypted with encryption product at least satisfying with requirement of national cipher mgt. or FIPS140-II. To encrypt the data document needing to be delivered to customer by use encryption product as customer required.

- 安全策略部和数据组应使用技术手段，保障数据生成过程中的数据源的可靠性、生成程序的符合性和数据的完整性。Security Policy dept. and data team should use technology method to ensure reliability of data source, compliance to generation procedure and integrity of data during data generation processes.

- 数据处理和生成系统必须从通过设计合理的机制，从技术上保证避免出现重复生产的情况。Data processing and generating system should be design with reasonable mechanism to prevent duplication production.

- 如有特殊原因必须手动对数据进行处理，或更改已使用过的数据状态时，必须经审批，处理过程须保证双人操作、各自复核，并留存处理记录。零星的数据状态更改

需要当班班长和质检双控执行，按照补卡流程操作。批量的数据状态更改需要得到逻辑安全员批准后，由生产主管和质检按补卡流程操作。eSim 平台 profile 的重复使用，必须在系统中确认，被成功下载的该 profile，通过系统成功在设备中删除后，方可通过系统授权用户再次使用。All manual data processing or data status change for special reason should be approved. Processing and checking should be under dual control and be recorded. Sporadic data status changes should be under dual control by on-duty monitor and QC according to card supplement procedure. Bulk data status change should be approved by LSO and performed by production supervisor and QC according to card supplement procedure. The re-use of eSim platform profiles could only be re-used by authorized system users after successful deletion of profile.

- 在生产的全过程当中，应有完整的、自动化的日志跟踪记录，记录数据操作过程当中的所有变化和活动。There should be integrate and automatic tracking logs to record all changes and activities related to data processing within the whole pro period.
- 定期对跟踪记录进行审查，确定其完整性。若有不正常操作和未经授权的活动，应立即汇报，同时在职责上应使用双控机制，保证操作和使用活动有跟踪记录。Audit the tracking logs regularly to ensure integrity. Report all abnormal operations and unauthorized activities discovered immediately. Enforce dual control and ensure that all operations and using activities are with tracking logs.
- SIM 卡数据处理特殊要求：Special requirements of SIM card data processing:

生产中心电信智能卡生产过程中，使用的随机数发生器应为符合国家商密管理要求或满足 GSMA/SAS 要求的随机数生成器。Special requirement for SIM card data processing: Random number generators used during SIM card pro should satisfy with the requirement of national cipher mgt. or GSMA/SAS.

- 数据处理人员及其他要求：Data processing personnel and other requirements:

a. 对于生产提请的，处理持卡人数据文件的员工，必须由人事部门和安全策略部门评估后，授权批准；数据处理员必须单独签署保密承诺书，承诺严守秘密，妥善处理客户数据，绝不将数据泄露给其他人。All employees responsible for processing data docs should be authorized and approved. Data processing employees must sign confidential agreement to make promise to keep secret of all data and process data appropriately.

b. 必须对处理持卡人数据文件的各用户创建受控制的域账户，专人专用。Create unique domain control account for each data processing user.

c. 各用户对持卡人数据文件的处理权限，必须基于工作需要对权限分配严格管理，且符合最小权限原则。Provide right for processing card-holder data for each user should be on a work-needing basis and compliance with least privilege principle.

d. 第三方访问敏感持卡人数据文件，必须经评估和客户书面同意，并签署保密协议。All third party access to limited data belonging to COs or card issuers is not allowed until relevant security assessment is completed and get written approval from COs or card issuer. Confidential agreement signed by them is needed as well.

e. 调整报告及生产记录上的卡片账号，必须进行掩盖处理，除非有客户的书面同意或基于必须的业务需求，方可显示全部卡号。Mask the card accounts on reports or production records. Whole accounts are prohibited to be visual unless getting written approval from customers or business requirements based on necessity.

6.3. 数据调度与生产 Data Allocation and Production

- 允许在高安全区内个人化网络中，数据处理组使用共享机制调用个人化数据，并设置共享文件夹的安全属性为仅允许特定的域控账户访问。需处理的数据统一放置于数据处理人员账号相对应的目录，数据处理人员只能以指定的方式取得该数据。

- 数据处理工作在固定区域内完成，数据处理完毕后，入库至指定数据库服务器中，

以便车间访问生产数据并进行调度生产。Data processing should be within fixed area. To put the processed data in dedicated data server to convenient pro dept. to access and produce.

- 生产主管为生产机台及人员分配生产任务。Pro supervisors allocate pro tasks to pro equipment and employees.
- 根据任务分配，生产人员使用本人账户登录设备，开始生产操作。Pro employees log in equipment by using self-accounts and start pro. on basis of allocation.
- 对于需要在生产设备 PC 上落地存储的磁条卡数据，需要经授权的人员通过实名制账户登录进行数据装载，装载完毕后，应立即登出账户，生产人员再登录实名制账户开始生产。For magnetic stripe card data needing to be stored on the pro equipment PC, authorized employees should log in by their own account to load data and logoff immediately after loading and log off the system.

6.4. 废品补号控制 Card Re-produce Control

本条规定了个人化生产过程中废品补号过程的安全控制要求。

This section defines the security control requirements for card re-make for reject during personalization production.

- 各机台在生产过程中产生的废品，均要作详细的补号记录，填写补号清单并及时向当班班长报告，当班班长必须依据各机台的废品记录，对产生的废品一一进行核对，确认后在补号清单上签名。To maintain detail records of all re-make of the reject during pro. Complete re-make list and report it to on-duty monitor timely. On-duty monitor must check the reject with the reject record of each equipment and sign on the re-make list after verification.
- 补号应在当班班长和操作人员双人双密码控制下登陆发卡软件，生成补卡索引后方

可补号。补号完毕操作者必须将补号卡片与原废品卡片核对无误后方可放回原组产品中，废品立即进行打孔处理。当班班长和操作人员的补号登陆密码均不能互相告诉对方和其他人员。Re-make should be under dual control that on-duty monitor and operator log in the issue software by use their own passwords and generate re-make index. Re-make operator must put back to original product patch after verified re-make card with reject card and securely treat the reject immediately, such as punch on the reject. Re-make logging-in passwords are unique belong to on-duty monitor and operator must not be known to each other.

- 对于数据在生产设备本机中存储进行生产的情况，应由指定的具有数据装载/调度权限的人员生成补号文件，仅具有发卡权限的操作工进行双人复核。To designate an employee with data loading/ dispatching right to generate re-making doc for status of data stored on local equipment to produce. Operator with issue right only to perform re-check.

- 补卡所需的卡片应在指定的带有《补卡记录表》的产品中拿取，并在该表上作补号记录。For pick the card for re-make from designated product team with re-make record and make registration on it.

- 对于批量产品返工，生产部门必须下达正式返工任务订单，并且说明原因。逻辑安全员必须检查返工任务订单的真实性和必要性，其次要确认原卡基是否需要销毁。如需要销毁，则应参考《生产中心卡及敏感组件安全管理标准》中单片卡废品的销毁流程进行销毁，销毁后重新下达生产订单。逻辑安全员确认无误后，在返工任务订单上签字。数据组必须见到逻辑安全员的签字确认后，才可以将返工订单批次数据重置。Pro dept. must submit official re-work order for bulk re-works and detail the reasons. LSO must check the authenticity and necessity of the re-work order and confirm that whether the original card bodies need to be destroyed. If needed, the destruction should be carried out following the Card and Sensitive Component Security

Mgt. Standard, and submit re-work order after destruction. LSO should sign on the re-work order after confirmation. Data team will reset data for the re-work patch only after seen the signature confirmation of LSO.

6.5. 数据删除和破坏 Data Deletion and Destruction

- 生产设备、生产数据调度服务器中的数据，数据处理电脑中的“中间数据”在生产/处理完毕后必须立即删除。因客户需求或原因，需要在数据处理区域暂存的“中间数据”，必须加密存放，且仅限授权处理的人员访问。Delete data stored in pro equipment and dispatch servers and “Internal Data” stored in data processing computers once after the completion of production or processing. If customers require us to store “Internal Data” temporarily on the data processing area, the data should be encrypted and limited to authorized personnel.
- 数据组应客户要求的数据备份活动必须在双控下完成。一旦客户方面的问题解决，所有形式的数据文件必须被安全性删除。数据库以及订单数据应采用异地备份，进行双重保护。定期的数据文件销毁应在逻辑安全员监督下完成，并填写《数据删除销毁记录表》。所有备份的数据应进行加密保存。Data team should complete the data backup under dual control according to customers’ requirements. All data docs must be deleted securely once customers had resolved their problem. Data base and order info should be backed-up off-site, encrypted and under dual control always. The regular destruction of docs should be performed under supervision of LSOs. Destruction record should be maintained.
- 金融卡数据（原始银行数据）必须在接收到后，按照客户要求，或在订单完工后 30 日之内被彻底删除。删除时需双控核对，进行自检和互检确认，确认完工数据范围并记录删除数据的范围，然后再删除金融卡数据（原始银行数据）。金融卡发卡数据库生产完工后 30 天之内由数据员双控从发卡服务器中删除。备份数据的删除每月由数据组提出，在逻辑安全员的监督下完成并登记。客户要求不能在 30 天

删除的数据文件，应要求客户提供书面授权，保留期限最长不得超过 6 个月，其书面授权有效期不能超过 2 年。若客户有其他的删除时间要求，则以客户要求为准。如：备份发卡日志保存一年之后删除；SIM 卡个人化数据库在生产完工后 7 天之内从发卡服务器中删除；非银行制卡数据保存一年之后删除。VISA 和 MasterCard 的制卡数据，客户要求保留的时间不能超过 6 个月。Delete cardholder data according to customers' requirements within 30 days from the time the order completed. Do self-check and cross-check and record the scope of data for completed pro prior to deletion of banking data (original). Data processing employee should delete the banking card data inside the card issuing server under dual control within 30 days after completion of the order. Data team submit data backup deletion request monthly and delete data backup under supervision of LSOs and make registration. To require customer to provide written approval if they need us to retain data for more than 30 days. This authorization is valid for retaining data no longer than 2 years. For other retention time, customers' requirements will be as the criterion. Such as, card issuing log database should be retained for at least one year after pro completion, SIM card personalization data should be deleted from card issuing server within 7 days after pro completion. Non-bank card data backups should be deleted after be retained for one year. Visa and MasterCard card pro data should be retained for less than 6 months.

- 客户直接提供的存储介质的破坏和销毁，由数据组填写《存储介质销毁表》并及时与相关客户联系，如客户要求公司退还，则由安全策略部负责监督数据安全删除后，数据组办理手续退还客户；如客户要求在公司原地销毁，安全策略部签字确认后，按照规定的数据破坏删除程序，与数据组双控处理。 Data team should fill Personalization Data Destruction Applicant and contact with customers before destroy the storage media provided by customers. While customers need to retrieve the storage media, data team is responsible for handle procedure of the return of storage media to customer after deleted data stored under supervision of security dept. While customers

need us to destroy them on-site, data team should destroy them under dual control according to data destroy and deletion processes afterSecurity Policy dept. signed to confirm.

- 印有客户非敏感信息的纸质文件，由打印需求部门负责存档保存；每年提交一次销毁申请，安全策略部负责监督双人销毁。Paper docs being with customer's non-sensitive information are retained by printing request dept. and these docs should be destroyed monthly under dual control.Security Policy dept. is responsible for supervision.
- 安全策略部每月进行一次内部审计，检查数据销毁落实情况，确保超过数据保留时间段的数据已经被安全删除。Security Policy dept. conduct internal audit monthly. Check the destruction situation to ensure the data is deleted as retain time requirements.

6. 6. 敏感数据 Sensitive Data

- 敏感数据在整个生命周期必须加密，防止非授权人员直接查看敏感数据。Sensitive data should be encrypted during its whole life cycle to prevent unauthorized access.
- 敏感数据是需要受到妥善保护并防止非授权公开，修改或销毁的客户资产。特别是明文 PINS 和加解密密钥，包含特征，状态等信息。 Sensitive data refers to the customer assets needing to be carefully safeguarded to prevent unauthorized disclosure, modification or destruction, especially for PINs in clear text and encryption and decryption key contained with info such as identification and status.
- 金融卡敏感数据通常分为持卡人数据和敏感验证数据。Banking card sensitive data is usually divided into cardholder data and sensitive verification data.

a. 持卡人数据包括：主账户（PAN）、持卡人姓名、失效日、业务码。Card holder data includes: PAN, card holder name, invalid data and business code.

b. 敏感验证数据包括：全磁道数据（磁条数据或芯片上的等效数据）、卡片验证码和验证值 CAV2/CVC2/CVV2/CID、PIN 等。 Sensitive verification data includes: full magnetic track data (Equivalent data on chip or magnetic track data), card verification code and verification value (CAV2/CVC2/CVV2/CID) and PIN, etc.

- 对于敏感数据进行分级管理，举例阐述如下：The classification mgt. for sensitive data is detailed as below:

a. 二级数据：有限人员可获得，且在传输过程中需加密。例如：PAN 的有效期，服务编码 ，持卡人姓名。SSL 密钥、保持数据的卡商证据等。Level 2 data: is limited to access and encrypted during transmission. Such as: expiry date of PAN, service code, card holder name, SSL key, evidence for data maintenance etc.

b. 三级数据：任何人都不能单独掌握，使用完毕后，必须被安全销毁。例如：芯片个人化密钥、PIN 密钥和用于生成 CVVs 的密钥或 CVCs、PINs、全磁道数据（磁条数据或芯片上的等效数据）等。Level 3 data which is subjected to knowledge split and must be secure destroyed after use. Such as: personalization key for chip, PIN key, key for CVVs generation, CVCs, PINs, full magnetic data (equivalent data on chip or magnetic track data) etc.

c. 对于通讯卡敏感信息分级参照《信息资产安全管理标准》GSM 卡资产安全控制。The classification requirements for communication card sensitive data can be found in Section 5.3.2.7 GSMA Asset Control in Info. Asset Security Mgt. Standard.

- 敏感数据存储、使用均须以密文形式存在，密文数据与密钥须分别进行控制，确保不存在明文数据、密钥可被同一人获得的情况。 The sensitive data stored or used must be in cipher text. Control cipher text data and keys separately to ensure that nobody can get the cipher text data and decryption-key by themselves.

- 如果由于业务需要，必须由第三方访问数据，应经客户书面同意，同时必须满足以

下要求：Third party access to data is not allowed unless get a written approval from customer and satisfy below requirements at the same time.

a. 任何必须访问数据的第三方，必须建立在承诺遵守安全制度和标准的正式合同基础上； Any third-party needing access must have established a formal contract with items of applicable security policies and standards.

b. 执行适当的控制并签订规定的访问条款后，才能允许访问相关数据和处理工具；Appropriate access controls must been implemented and a contract defining terms for access has been signed before access.

c. 在同意第三方任何访问之前必须进行风险评估。 To conduct risk assessment before third-party access authorization.

d. 在访问敏感数据之前，需建立用户身份核实机制。核实是否产生审计追踪的日志。Establish user identification verification mechanism before accessing sensitive data to verify if audit tracking log will be generated.

- 当基于业务需要，卡号需要打印或展示出来时，确保卡号是被隐藏的，除非有客户书面通知授权。当卡号被隐藏时，卡号数字最多只能允许看前 6 个数字和后 4 个数字。Card accounts must be masked when displayed or printed unless there is a written issuer authorization regarding it. When card accounts are masked, only a maximum of the first 6 digitals and last 4 digitals of the card account can be visible.

6.7. 测试数据 Test Data

- 正式数据严禁用于测试开发目的，在测试或开发环境中，仅允许使用事先制作的测试数据。测试数据原则上不在正式环境中运行，除非客户的特殊需求（例如打样数据），应由客户出具书面说明。对于客户要求将正式数据用于测试开发目的，必须出具书面说明，安全策略部进行风险评估之后才被允许。It is prohibited to use formal data for test and development where is only for pre-made test data. Testing data is

prohibited to be used in live mode unless with customers' written docs for special requests. Formal data is prohibited to be used for test and development unless written approval is provided andSecurity Policy dept. has conduct risk assessment for it.

- 必须严格选择测试数据，并对测试数据加以适当的保护和控制。Test data should be chosen rigorously and secure and control them appropriately.
- 针对不同的客户和项目，应制作对应的测试数据并归类存档，以便于使用。 Test data should be dedicated for each customer and program and have them classified and on file for further use.

7. 存储介质 Storage Media

- 安全策略部负责检查数据文件被彻底销毁的情况。如：纸质文件应彻底粉碎或焚烧，一次性数据存储介质（CD-R）应彻底粉碎，可重复使用存储介质（磁带）应对数据进行破坏后删除等。Security Policy dept. is responsible for verifying the data doc destruction. Such as: paper with data should be smashed or fired thoroughly, disposable CD-R should be smashed thoroughly and data on the reusable storage media (tape) should be destroyed and deleted securely.
- 所有经过数据删除处理的可重复使用存储介质，由安全策略部统一回收进行管理。安全策略部人员应定期汇同数据组相关人员对存储介质进行检查，以防止可能发生的数据遗留。经过检查之后的存储介质，标记为可用状态，方可重复使用。Security Policy dept. is responsible for recycling the reusable storage media to ensure that there is not data docs within it.Security Policy dept. should check the storage media with data team regularly to prevent data from left over. The storage media can be re-used only after has been checked and labeled usable.
- 安全策略部负责检查所有重复使用的存储介质中，只包含指定实际接收人的信息，任何其它数据应彻底清除。Security Policy dept. is responsible for checking all the

reusable storage media to ensure that it only contains with actual receipt info and any other data should be deleted thoroughly.

- 安全策略部负责所有缺损的存储介质的销毁，并在数据组提交的销毁申请单上签字确认。Security Policy dept. is responsible for the destruction of all the deficient storage media and signing on the destruction applicant submitted by data team to make confirmation.

- 对于检查存储媒介的完整性，必须进行以下程序：Below procedure should be implemented for integrity verification of storage media:

a. 检查存储媒介的包装。To check the package of storage media.

b. 如果包装完整性有差异，必须立即通知个人化部门经理或数据组主管和 CISO。Report any discrepancy of package integrity to personalization dept. manager or data team supervisor and CISO.

c. 必须立即终止全部的数据处理流程。To terminate all the data process immediately.

d. 必须立即将该事件通知数据所有人（发卡商）。To report the incident to data owner (card issuer) immediately.

e. 对于该事件将启动数据泄漏程序。To activate the data compromise procedure for the incident.

- 安全策略部负责统计生产网络所有电子存储介质数量，内容，建立《存储介质管理日志记录》形成台账进行管控。Security Policy dept. is responsible for statistic of electronic storage media within pro network and establishing Storage Media Management Log to implementing control.

8. 数据安全应急处理 Data Security Emergency Process

1) 如果发生数据泄漏（已知的或怀疑的），必须通知个人化部门经理、eSim 连接管

理系统项目经理、CISO、分管领导和数据所有人，必须在 24 小时内通知支付卡机构、GSMA 等卡组织。 To report any confirmed or suspicious data reveal to personalization dept. manager, project manager of eSim connection management system, CISO, branched general manager and data owner immediately and to COs, such as GSMA etc. within 24 hours.

2) 如果此数据正在生产，应立即停止。对已生产的卡应立即封存，直到数据泄漏事件已解决。Immediately terminate the pro related the divulged data. Seal to store the produced card until the reveal incident is resolved.

3) IT 工程师、逻辑安全员将对泄漏事件执行详细的调查，并在个人化部门经理、eSim 项目经理和 CISO 的帮助下确认所有可能受影响的数据文件。IT engineer and LSOs will look through the incident and verify all data docs maybe affected with the help of personalization department, eSim project manager and CISO.

4) 一旦确认了怀疑被泄露的数据文件，所有怀疑的数据文件和对应的文件将禁止用于下一步流程。 Data and docs are prohibited to be used for next process immediately if the data is known or suspicious of being divulged.

5) 泄漏的敏感数据应在 4 小时内被封存保管、限制访问，直至客户允许时，方能彻底删除。个人化部门经理、eSim 项目经理和分管领导，将通知所有相关管理方和发卡商对所有受影响的或怀疑的数据文件进行销毁和再生成。 Divulged sensitive data should be stored sealed and access limited within 4 hours. Delete them thoroughly if customer approves. Personalization department, eSim project manager and general manager should inform interested party and issuer of destroying and re-generating all data document being effected or suspicious.

6) 怀疑的或泄漏的数据文件已个人化的卡片，必须销毁或彻底删除清零。To destroy and delete thoroughly the card personalized with data known or suspicious of being divulged.

7) 启动恢复程序前，CISO 必须确认，纠正所有可能的安全违规情况，验证所有措施的可用性、有效性。Security Policy manager must verify that all violation to security requirements has been corrected effectively before recovery program activation.

8) 对发生泄漏的原因应检查和分析，对泄漏造成的危害和损失应进行评估，形成分析评估报告及整改方案。CISO 必须准备关于数据泄漏事件的事件调查报告。必须至少包括以下项：To analysis the reason of divulge and assess the damage resulting from reveal and to formulate analysis assessment report and corrective plan. CISO must make incident investigation report for the data reveal incident concerning for below information:

a. 数据泄漏的根本原因 Root reason of data reveal

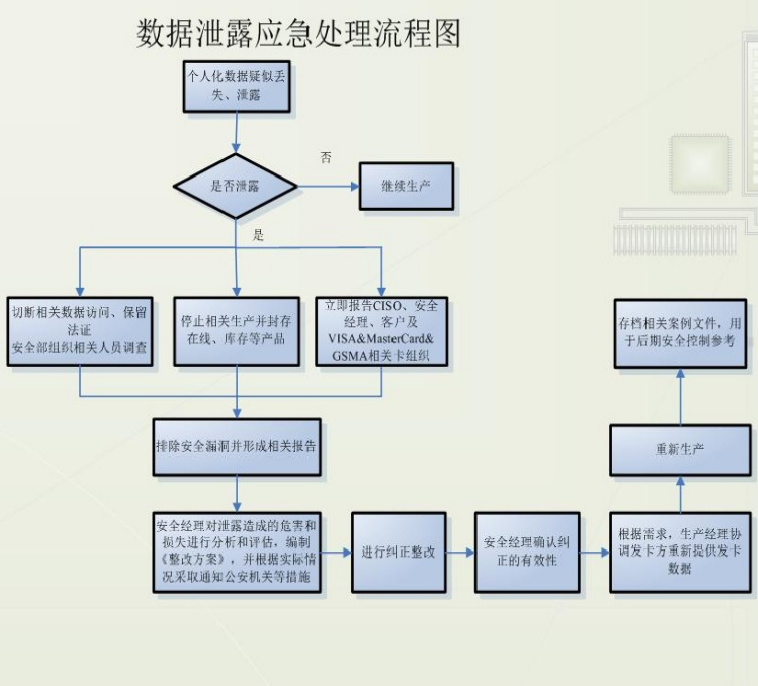
b. 损害的原因和范围 Reason and scope of damage

c. 纠正行动 Corrective Measure

d. 预防行动 Preventive Measure

9) 个人化部门经理必要通知发卡商再次生成持卡人数据文件。 Personalization dept. manager must require issuer to re-generate card holder data doc.

10) 安全策略部应制定数据安全控制的应急方案，安全策略部、个人化部门汇同安全管部一起，定期维护和演练，并保留相关记录。Security Policy dept. should make emergency plan for data security control.Security Policy dept. and personalization dept. should maintain and drill regularly and keep relevant record.



9. 引用相关文件 Doc Referred

- 信息资产安全管理标准 Info. Asset Security Mgt. Standard

10. 引用相关记录 Record Referred

- 数据访问申请表 Card Re-make Record
- 数据转移处理进度表 Data Transfer Processing Schedule
- 数据删除销毁记录表 Data Delete Destruction Record Table
- 存储介质数据删除及销毁记录表 Storage Media Destruction Table
- 数据接收登记表 Data Receiving Registration Form

11. 附加说明 Additional Remark

- 本标准由安全策略部归口并解释。Security Policy dept. has the right of interpretation of this standard.
- 本标准由安全策略部负责检查与考核。Security Policy dept. is responsible for checking and assessing this standard.
- 如有违反本标准规定的，对责任人或部门处以《生产中心员工奖惩管理实施细则》进行考核。Any breach to this standard will be punished according to the Punishment and Awarding Mgt. Rules of Pro Center.