

**上海诚天智能卡有限公司**

|  |
| --- |
| **Data Security Management Process**  **数据安全管理流程** |

Document Number文件编号: WI-MIE-013

版本 V5.0

**Distribution Controls 发行管制**

This distribution of this plan is controlled to authorize control leaders of each organizational function who are active members. The Dept Director manages updates and replacement of this plan. Plan recipients who cease to be responsible for the scope of this plan must surrender all copies of the plan to the Dept Director.

此文件仅限于在职能范围内人员中发布。部门主管负责文件的更新、更换。文件接收人不再履行职责时应将此文件所有复印件交还部门主管。

**Document History 文件历史记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version**  **版本** | **Date**  **日期** | **Update Details**  **更新资讯** | **Author**  **主办** | **Censorship**  **审查** | **Approbation**  **核准** |
| V 1.0 | 2015 /11/01 | First Issue首发 | 尤长峰 | 李乾凯 | 梅昌刚 |
| V 2.0 | 2016 /07/16 | Add detailed security actions  增加详细安全活动 | 尤长峰 | 李乾凯 | 梅昌刚 |
| V3.0 | 2017/02/15 | 部分文字修改  Partial Text Modification | 雷浪 | 李乾凯 | 梅昌刚 |
| V4.0 | 2018/ 06 /13 | 数据流程更新  Data Flow Update | 闫成玲 | 雷浪 | 景在军 |
| V5.0 | 2020/05 /11 | 重新定义数据存储周期  Redefining data storage cycle | 闫成玲 | 雷浪 | 景在军 |
|  | / / |  |  |  |  |

**This version supersedes all previous versions issued prior to the date indicated above**

此版本取代上述发布日期之前的所有版本。

1. **目的Purpose**

对公司内所有涉及到个人化生产的相关数据进行安全有效的管理，在数据的接收、存储、内部传输、处理、生成、交付和销毁等一系列过程都建立相应的安全保护机制，保障数据的安全。

To effectively and safely manage the personalization production data of company, establish corresponding security & protection mechanism for the data’s receiving, storage, internal transfer, handling, generation, submitting and destruction etc., and guarantee the security of the data.

1. **范围Scope**

适用于公司内所有涉及到个人化生产的相关数据的安全管理，包括客户原始数据、生产数据和回复客户数据等。

Be suitable for the security management of corresponding personalization data of Shanghai Chengtian Smart Card Co.,Ltd, including the customer’s raw data, production data and output data etc.

1. **职责Responsibility**

## 数据工程师 Data engineer

### 接收外来数据文件

### Receiving of incoming data

### 执行数据处理并生成导入数据文件

### Implementation of data handling and generation of input data

### 备份和销毁数据

### Backup and destruction of data

### 储存外来数据

### Storage of incoming data

## 数据主管/经理 Data Leader/manager

## 3.2.1 在数据下载、数据销毁等需要“四眼”控制时参与数据的管理活动

Take part in data management activities when need “4 eyes” control, such as data download, data destruction, ect.

1. **参考文件Reference: /**

4.1 SCT-SM01 安全管理手册 Security Manual

4.2 SCT-SP-001 资产分类控制程序 Assets Classification Control Procedure

4.3 IT-P-001 IT安全政策 IT Security Policy

1. **程序Procedure**

## 定义 Definition

### 原始数据：由客户提供的卡片特定机密信息的数据。原始数据以特定格式的原始数据文件的形式提供给公司。

### Raw data: The card data with specific confidential information supplied by the customer. The raw data is provided to Shanghai Chengtian Smart Card Co., Ltd in the form of raw data files with specific format.

### 生产数据：数据生成过程产生的用于个人化生产、包括卡片特定机密信息的数据，生产数据以特定格式的生产数据文件的形式存在于生产服务器的特定区域，供个人化系统和设备生产卡片使用。

### Production data: The data produced during data generation process and used for personalization production, including specific confidential information of the card. The production data exists in the specific area of production server in the form of production data file with specific format, and is used for personalization system to personalize the card.

## 描述Description

### 数据的生命周期Data lifecycle

### 数据的生命周期主要分为以下六个阶段，分别是数据的接收、数据的处理、数据的上传、数据的存档、数据的销毁。

### The data lifecycle is mainly divided into the six phases, data receiving, data handling, data generation, data submitting, data archiving and data destruction.

### 数据的接收Data receiving

### 数据的接收是指公司从客户处接收有关个人化生产的原始数据文件，并传递到生产网内。

### It means that the data files related with personalization are received from the customer, and then transferred them to the production network.

### 数据的处理Data handling

### 数据的处理是指通过特定的数据处理软件对原始数据文件进行解密。

### It means that the raw data files are decrypted and converted by specific data handling software.

### 数据的上传Data loading

### 数据的上传是指将生产数据文件上传至生产服务器的生产区域供个人化系统和设备生产卡片使用。

### It means the transit of the production data files from the working area to the production area on the production server for personalization system.

### 数据的存档Data archiving

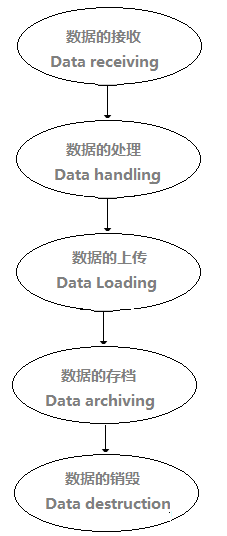
### 数据的存档是指将相关客户的原始数据文件和相应的已交付的生产数据文件等在生产服务器进行相应的存档，以便客户追溯返查。

### It means the archiving of raw data files from the related customers and relevant data files on the production server ,in order to serve the customer long-term tracing.

### 数据的销毁Data destruction

### 数据的销毁是指将生产服务器上已完成生产的相关数据文件进行永久性的擦除和对客户原始数据进行销毁。

### It means the securely shredding of the relevant data files on the production server and the raw data from the customer.



## 原则和方法Principles and methods

1. “四眼”原则 “4 eyes” Principle

在数据安全管理的各个环节和各个阶段从始至终必须严格贯彻和执行“四眼”原则，在任何情况下都必须要有双人在场，同时操作并确认。

The “4-eye Principle” must be strictly carried out during every phases of the data security management, and in any case, two persons should be on site for operating and confirmation simultaneously.

1. “绝对必要”原则 “Need to know” Principle

在数据安全管理中只有在绝对必要的情况下才能够对数据做相应的操作，除此之外任何多余的操作和干涉是不允许发生的，要在“四眼”原则的基础上严格贯彻和执行“绝对必要”原则。

During the data security management, the data can be accessed only under absolutely necessary circumstance according to “need to know” principle, and then it is not allowed to have any redundant operation and interference. The “Need to know” principle must be strictly carried out based on the “4-eye Principle”.

1. “操作记录”方法 “Audit trail” method

在数据安全管理中的任何“绝对必要”的操作必须有操作记录可以追踪和审查，操作记录至少要包含以下信息：日期和时间，操作的行为，操作的责任人和见证人的签字确认，要在“四眼”原则的基础上严格贯彻和执行“操作记录”原则。

Any operation of “Need to know” during the data security management must be trailed and audited with “Audit trail” method, and the “Audit trail” at least includes the following information: date, time, operation behavior, signature of the operator and the witness of the operation. The “Audit trail” principle must be strictly carried out based on the “4-eye Principle”.

## 数据的接收Data receiving

1. 数据的接收只能在个人化数据中心指定的PC上，由双人在场同时进行，不允许在其它任何区域和PC上进行数据的接收。

从SFTP服务器上接收数据的PC用户密码分两段由两个保管，必须两个同时在场才能登录，保障数据的安全性。

Data receiving only can be done in the specific computers in data center by two persons in place simultaneously, while not permitted in any other area and computers.

The password of user account of computer used for receiving data from SFTP server separated two phase and save by two authorized data engineers, and only them in place simultaneously can logon, which guarantee the security of the data.

1. 接收机密数据只能通过以下唯一方式：固定IP的专线，SFTP和通知论证用户，不能通过其它不安全的方式，如电子邮件、ICQ等方式接收机密数据。为了保护机密数据的安全性，客户一般采用PGP软件对数据进行加密保护。若客户要求使用不安全的数据接收方式或未用PGP加密的数据文件，客户服务部门应正式书面通知客户由此可能带来的安全漏洞和风险。

Confidential data is only received via fix IP address private line by SFTP with authorization ID, not via other insecure ways like E-mail and ICQ etc .In order to secure confidential data, the customer to protect the data with PGP encryption usually. If the customer requires the unsecure data transfer mechanism, the Sales department should inform the customer of the security weakness and risk potential in formal written document.

1. 接收完成后，用专业杀毒软件进行杀毒。查毒正常后将数据上传到生产网络中的SFTP 服务器。然后数据工程师从生产服务器将数据从生产网络中的SFTP服务器中下载下来。

After receiving, scanning the data with the professional Anti virus software, If it ok, uploading the data to production network SFTP server. Then, the data engineer will download the data from the production network SFTP server at the production server.

1. 生产服务器上存放客户原始数据文件的工作区域只有数据工程师有权限访问，其它人员都无权访问。

Only Data engineers have the right to access the working area storing the raw data files on the production server, while other person have no right to access.

1. 相应的操作人员必须填写数据接收的相关操作记录文件并签字确认。

Corresponding engineers must fill in the relevant working record of the data receiving and sign.

## 数据的处理 Data handling

1. 数据的处理只能在数据中心内生产服务器上处理，由双人在场同时进行，不允许在其它任何区域和PC上进行数据的处理。

Data handling only can be done in the production server at data center by two engineers in place simultaneously, while not permitted in any other area and computers.

1. 运行专用的数据处理软件对接收的客户原始数据文件进行处理，软件自动直接将其生成在生产服务器上存放导入文件的工作区域。

The Data engineers utilize the specific data handling software to hand the input data files. The input data files are automatically created on the working area on the production serer by data handling software.

1. 导入文件只能存储在生产服务器上的工作区域，在任何情况下不得将其存储在执行处理操作的PC本地硬盘，该区域只有数据工程师有权限访问，其它人员都无权访问。

The input data files can only be stored in the working area on the production server, and in any case may not be stored into the local hard disk of the computer implementing data handling. This area can only be accessed by Data engineer not by any other personnel.

1. 数据处理若需要使用相应客户的传输密钥卡进行文件的解密，需由双人操作打开数据中心的保险柜，取出对应的密钥卡，密钥卡必须受控使用并有操作记录，使用完后需要立即归还存入保险柜。

If the transport key card of the corresponding customer is required for the decryption of the raw data, it must to open the locked cabinet of data center room by two persons and take out the key card. The key card should be accessed under dual controls via a detailed tracking record, and after usage it should be immediately returned back the cabinet.

## 数据的上传 Data Loading

* + 1. 数据的上传只能由数据工程师来完成，将需要生产的数据从服务器上传到对应的个性化机器。

Data loading can only be done by data engineers, and the data needed to be produced can be uploaded from the server to the corresponding personalized machine..

* + 1. 相应的数据人员与操作人员必须填写数据上传的相关操作记录文件并签字确认。

Corresponding engineers must fill in relevant working record of data submitting and sign.

## 数据的存档 Data archiving

* 1. 数据的存档只能在数据中心室内备份服务器上，由双人在场同时进行，不允许在其它任何区域和PC上进行数据的生成。

Data archiving only can be done in the backup server in data center by two data engineers in place simultaneously, while not permitted in any other area and computers.

* 1. 为了防止客户长期的追溯，存储加密后的客户原始数据和相关配置文件至备份服务器上6个月, 如果不同客户对数据存储时间有更严谨的要求，需按照户要求来存储。

Archiving the raw data and relevant configuration files which encrypted by PGP function to the backup server for 6 months in order to serve the customer long-term tracing., If different customers have more stringent requirements on data storage time, we need to store data according to the requirements of customers

* 1. 相应的操作人员必须填写数据存档的相关操作记录文件并签字确认。

Corresponding engineers must fill in relevant working record of data archiving and sign.

## 数据的销毁 Data destruction

* 1. 电子数据的销毁只能在数据中心，由双人在场同时进行，不允许在其它任何区域和PC上进行数据的生成。

The destruction of data with the electronic format only can be done in data center by two data engineers in place simultaneously, while not permitted in any other area and computers.

* 1. 生产区域内相关配置和文件的销毁在产品出货后在24小时内完成，备份的数据需按照客户要求的存储期限来删除，文件的销毁采用PGP的Wipe或Shred功能安全擦除。

The script and relevant files in the production area should be erased by Data engineers ，backup data shall be deleted according to the storage period required by the customer， manually via the Wipe or Shred function of PGP after the shipment within 24 hours.

* 1. 相应的操作人员必须填写数据销毁的相关操作记录文件并签字确认。

Corresponding engineers must fill in relevant working record of data destruction and sign.

1. **相关文件及表格Relevant documents**

## MIE-003 个性化批次分配表 Personalization Batch Distribution Sheet V1.0

## MIE-004 数据存档与销毁记录表 Data Storage & Data Destruction Sheet V1.0

## MIE-005 数据销毁记录表 Data Destruction Sheet V1.0

## MIE-06 数据下载记录表 Data Download Record V1.0版