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

安防控制管理标准

Security Control Management Standard

文件种类：管制文件 File Type: controlled document   1

文 件 编 号: KD-MWL-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	郭明	刘劲松	陈为明
02	2019.12.30	更改文件格式	A1	郭明	刘劲松	陈为明
03						
04						
05						
06						
07						
08						
09						
10						

目 录 Table of Content

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

密级：1 级 内部

1. 目的 Purpose

　　为确保公司经营场所的物理安全控制，满足各卡组织、客户，及公司自身的安全防范需求，特制订本标准。本标准参照中国银联、PCI、JCB、美国运通、GSMA 协会相关安全规定，结合公司自身安防控制要求而制定，所有员工必须了解并遵守安防控制规范和安防设施使用要求。

　　To specify physical security control of Tianyu to satisfy security requirements of card organization and customers, we made this standard referring security standards of Union Pay, PCI, JCB, Amex and GSMA. All employees should understand and follow its items appropriately.

2. 适用范围 Scope

　　本标准适用于四川科道（含生产中心、研发中心），所有生产、办公建筑及其安防设施的管理。

　　This standard applies to management of security controls of Tianyu, including Production Center and R&D Center.

3. 术语定义 Definitions

　　无。None.

4. 职责 Responsibility

4.1. 安全策略部 Security Policy Dept.

➢ 负责安防设施（如：安防报警系统、门禁系统、CCTV 系统、监控照明等）的控制需求、施工验收、日常使用维护工作，及时进行安防设施档案的更新。

Be responsible for reconstruction requests control, projects acceptance and daily

密级：1 级　内部

maintenance of security devices, such as alarm systems, badge access system, CCTV and illumination etc. Security devices files should also be maintained appropriately.

➢ 负责安防零星工程的技术指导、图纸确认及安防功能验收。

Be responsible for providing technical guidance, confirming reconstruction drawings and acceptance checking security functions for security construction projects.

4.2. 设备管理部 Equipment mgt. Dept.

➢ 负责协助安防设施维修及维护。

Assist maintenance of security devices.

➢ 负责安防零星工程项目的核价、项目布局设计的管理。

Price security project and manage project.

➢ 负责施工现场管理，如施工访客人员入厂手续办理、施工陪同等。

Manage construction, such as handling access process for constructors etc.

➢ 负责安防零星工程项目的非安防功能类的验收工作。

Check non-access-control functions.

4.3. 行政办公室 Administration Office

➢ 负责授权手机的购置、实名制的手续办理及通讯费用的结算。

Buy and settle communication fee for authorized mobile phones.

4.4. 各区域前台 Front Desk Staff

核实来访人员身份、登记、发放访客临时门禁卡，并通知被访人员或其代理人员，至前台接待访客；在访客离开时，回收并妥善保存访客临时门禁卡。

Verify visitors' identification. Notify employees visited to receive visitors and make registration and issue visitor badges. Retrieve visitor badges when they left.

4.5. 门岗保安 Guards on Gate

厂区授权人员身份识别和安防管控，外来人员身份识别和安防管控。

Manage with identification verification of authorized and unauthorized personnel.

4.6. 监控室保安 Guards in SCR

➢ CCTV 的日常检查、门禁系统、安防报警系统的日常处理、记录，及关键报警的紧急确认和处理。

Conduct CCTV daily checks. Deal with and record daily affairs of access system and alarm system and immediately confirm and manage important alarms.

➢ 7*24 小时*365 天不间断监控厂区内外安全情况，及时记录并汇报各类安全异常情况，并进行现场处理。

Ensure permanent (7*24) control of security of site. Deal with and record any abnormities timely.

5. 工作流程 Working Procedure

5.1. 厂房安全级别及管理要求系统 Site Security Levels and Management Requirement.

5.1.1. 厂区共分为 3 个安全级别 Three security levels

3 个安全级别的区域中，分别用颜色区分为不同的种类。Differentiate security levels of areas by different colors.

安全级别 Sec Level	物理保护措施 Physical Security Controls	范围 Scope

LV 1 普通区域 绿色区域标识 LV 1 Normal Area Identified by Green	**物理保护**：2.5M 钢制围栏分布在厂区四周 **CCTV 系统**：CCTV24 小时不间断录像覆盖全区域 **报警系统**：安装在四周围栏、人员出入闸门、建筑厂房四周高安全区域的窗户上，当有物体穿过则发生报警讯号，并传递到监控室 **Physical Protection Device:** Deploy steel fence with 2.5m height at periphery of plant. **CCTV System:** Deploy CCTVs fully cover the area and working 24 hours a day. **Alarm System:** Be deployed at fences, barrier gate for personnel, windows of HSAs. It will activate alarm signals to SCR for unauthorized across.	栅栏内、建筑厂房外墙 Fences, external wall
LV 2 受控区域 黄色区域标识 LV 2 Controlled Area Identified by Yellow	**CCTV 系统**：CCTV24 小时不间断录像覆盖全区域 **门禁系统**：仅限授权人员进出 **特点**：在建筑内部，无外围护栏等周界报警 **CCTV System:** Deploy CCTVs fully cover the area and working 24 hours a day. **Access System:** Only for authorized personnel to access. **Characters:** Within the building, without perimeter alarm systems such as fences.	一楼前厅及办公室、楼梯、卫生间 二楼办公室、维修室、更衣室、储物间、楼梯、卫生间 三楼、收发货区中外门区域 The first floor: front desk, office and staircase, toilet. Second floor: office, maintenance room, dressing room, storage room, staircase, toilet All of the third floor. The area of middle door to outside door in the loadiing bay.
LV 2 受控区域 橙色区域标识 LV 2 Controlled Area Identified by Orange	**CCTV 系统**：CCTV24 小时不间断录像覆盖全区域 **门禁系统**：门开启后超过 3 分钟门未关闭将产生报警讯号，仅限授权人员进出，防折返功能 **报警系统**：触发报警器后，将产生报警信号 **特点**：有移动侦测报警 **CCTV System:** Deploy CCTVs fully cover the area and working 24 hours a day. **Access System:** Only for authorized personnel to access. Opening for more than 3minutes will activate an alarm. Anti-pass-back function. **Alarm System:** Generate alarm signals once alertors activated. **Characters:** With Motion Detection Alarm	监控室 SCR
LV 3 高安全区域 红色区域标识 LV 3 HSAs Identified by Red	**单人通道门**：一次只能通过一人，双门互锁，刷卡匹配成功后，门才开启（两边入口都是 Mantrap） **CCTV 系统**：CCTV24 小时不间断录像覆盖全生产区域 **门禁系统**：单卡刷门。门开启后超过 3 分钟门未关闭将产生报警讯号，仅限授权人员进出，防折返功能 **报警系统**：触发报警器后，将产生报警信号，信号直通监控室 **特点**：通过单人通道门和货闸，隔离生产区域与办公区域 **Man-trap:** enforce One-by-One and interlock function technically. Accessed by successful card authentication. **CCTV System:** Deploy CCTVs fully cover the area and working 24 hours a day. **Access System:** Only for authorized personnel to access by single Cards. Opening for more than 3minutes will activate an alarm. Anti-pass-back function. **Alarm System:** Generate alarm signals to SCR once alertors activated. **Characters:** Isolate pro area and Office by Man-trap and Good-trap.	A-B 门内所有区域 HSAs within Man-trap.

区域	说明	位置
LV3 高安全区域内特殊区域 浅紫区域标识 LV 3 Special area of HSAs Identified by Light Purple	**单人通道门**：一次只能通过一人，双门互锁，刷卡 匹配成功后，门才开启（两边入口都是 Mantrap） **CCTV 系统**：CCTV24 小时不间断录像覆盖全生产区域 **门禁系统**：单卡+密码。门开启后超过 3 分钟门未关闭将产生报警讯号，仅限授权人员进出，防折返功能 **报警系统**：触发报警器后，将产生报警信号，信号直通监控室 **特点**：通过单人通道门和货闸，隔离生产区域与办公区域 **Man-trap:** enforce One-by-One and interlock function technically. Accessed by successful card + password authentication. **CCTV System**: Deploy CCTVs fully cover the area and working 24 hours a day. **Access System:** Only for authorized personnel to access by single Cards+passord. Opening for more than 3minutes will activate an alarm. Anti-pass-back function. **Alarm System:** Generate alarm signals to SCR once alertors activated **Characters:** Isolate pro area and Office by Man-trap and Good-trap.	GMSA 车间 GMSA room
LV 3 高安全区域内特殊区域 深紫区域标识 LV 3 Special area of HSAs Identified by Dark Purple	**CCTV 系统**：CCTV24 小时不间断录像覆盖全生产区域 **门禁系统**：双卡 开启后超过 3 分钟秒门未关闭将产生报警讯号，仅限授权人员进出，防折返功能 **报警系统**：触发报警器后，将产生报警信号，信号直通监控室 **特点**：需双人刷卡 **CCTV System**: Deploy CCTVs fully cover the area and working 24 hours a day. **Access System:** Only for authorized personnel to access by dual Cards. Opening for more than 3minutes will activate an alarm. Anti-pass-back function. **Alarm System:** Generate alarm signals to SCR once alertors activated. **Characters:** 2 Cards are needed while accessing at least.	数据机房、金库 Data and server room、Vault

5.1.2. 安防技术工程师应根据实际的各区域位置，制定《厂房安全级别平面图》，并需实时更新，且至少每 90 天变更一次，交由部门领导审核。Sec. Technical Engineer should make The Layout of Plant Security Level on base of actual site deployment and update it in real time or at least every 90-days. Dept. leader's review is also needed.

5.2. 厂房安防设施的运作 Security Devices Operation of Site

5.2.1. 安防报警系统 Alarm System

5.2.1.1. 电子围栏：在厂区外围围墙都设有电子围栏。处于 24 小时运作状态，若发生非法侵入，位于监控室的报警器会报警，并显示侵入的防区。

Electronic Fence: Be deployed on the fence of site periphery and be on for 24*7 hours.

Unauthorized across will activate alarm signal to SCR popping with a picture showing the area.

5.2.1.2. 红外光栅：在人员出入闸门、建筑厂房四周高安全区域的闸门、窗户外都设有红外光栅，处于 24 小时运作状态，若发生非法侵入，位于监控室的报警器会报警，并显示侵入的防区。

Echelette Grating: Be deployed above low barrier gate for personnel and outside of windows of HSAs and be on for 24*7 hours. Unauthorized across will activate alarm signal to SCR popping with a picture showing the area.

5.2.1.3. 红外对射探测器：在厂区外围伸缩门、铁门处设有红外对射探测器。处于 24 小时运作状态，若发生非法侵入，位于监控室的报警器会报警，并显示侵入的区域。

Infrared Beam Detector: Be deployed above retractable door and steel door of site and be on for 24*7 hours. Unauthorized across will activate alarm signal to SCR popping with a picture showing the area.

5.2.1.4. 红外移动探测器：在工厂车间、仓库、金库、碎卡室等高安全区域内的每个房间都设有红外移动探测器。正常上班时间，红外移动探测器是关闭的，安防技术工程师会根据生产排班计划，在公司放假/没有生产排班时进行设防和撤防设置，并通知保安。设防时一旦检测到有物体移动，会立即报警并显示报警区域。

Infrared Movement Detector: Be deployed in HSAs such as workshop, warehouse etc. Security Technical Engineer should set be protection or removal according to production schedule. It should be removal during working time and be turned on during company holiday or no production.

5.2.1.5. 震动探测器：在厂区金库内设有震动探测器，处于 24 小时运作状态。若墙体、天花板或地面受到强烈震动时，将产生报警讯号，讯号直通监控室。地面的震动传感器在有人工作时会撤防，无人时布防。

Vibration Detector: Be deployed in Vaults and be on for 24*7 hours. Wall, ceiling or floor vibrating will activate alarm signal to SCR. Vibration detector of floor are disarmed during working hours.

5.2.1.6. 胁迫按钮：厂房内各区域均设有胁迫按钮，供紧急情况下报警使用。Be deployed

to cover every area of site for emergency alarming.

➢ 当胁迫按钮被激活后，监控室将会有报警声，且实时监控画面会显示相应区域的监控画面，保安应立即确认是否发生了紧急事件（如胁持、侵入、火灾、地震等）。若确认为有紧急情况发生，应立即按下位于监控室的胁迫按钮（监控室内不会产生本地报警声），该胁迫按钮与警方 110 直接相连，并回答 110 的询问，以便在紧急情况下警方能迅速、准确到达公司处理异常。无论是否有紧急情况发生，保安根据《监控室紧急联络窗口》立即联络第一联络人，同时应立即向安全策略部报告，以得到进一步的指示，并做好记录。为避免 110 来电时正被挟持，会造成不必要的人身伤害。与 110 约定"今日几月几号"作为正在被挟持中的暗号。

Pressing duress button will activate alarm to SCR popping with popping with a picture showing the position. Guards in SCR will check and confirm if it is true emergency (kidnap incursion, fire, earthquake etc.). To press duress button located at SCR to call police appropriately once an emergency is confirmed. To avoid unnecessary personnel injury caused by SCR guards is kidnapped, a code word 'What's the date today' should be communicated to responsible Police Station in advance. Then notify related person according to Emergency Contact Information in SCR and Security Policy Dept. Make record appropriately.

➢ 对于因误按触发的胁迫按钮报警，保安必须填写《胁迫按钮纠正行动记录表》，详细记录触发原因，涉及人员，处置方法等信息，由部门领导签字确认。

Guards must complete the Duress Button Corrective Actions Form for the accidental duress button activation; detail the reason, personnel involved, action etc., supervisor of security dept. should sign to make confirmation.

➢ 安防技术工程师需要定期（每三个月一次）对胁迫按钮进行测试，并记录在《胁迫按钮测试清单》中，测试过程保留在《胁迫按钮纠正行动记录表》中。

Security Technical Engineer should test the duress button quarterly and maintain Duress Button Test List and Duress Button Corrective Actions Form.

5.2.1.7. 无人报警：处于 24 小时运作状态。当监控室内无人或检测到监控内十分钟没有人员走动的时候，监控室内将会产生本地报警声。保安需将报警时间记录在《无人系统报警处理表》中，安防控制工程师在正常工作日对报警条数及报警原因进行确认。

Dead-man Alarm: Be on for 24*7 hours. A local alarm will be activated if no movement is detected while system registered that at least one person has entered for more than 10 minutes. Guards should record the alarm time in Alarm Processing Records of Dead-man System, Security Control Engineer will confirm the quantity and reason of the alarms.

5.2.1.8. 开门报警：处于 24 小时运作状态。所有的消防安全门都有开门报警功能。消防安全门只有在紧急情况下才能打开；若在非紧急情况下，需要开启消防安全门，需要向安全策略部部门领导申请，待部门领导批准后方可打开。消防安全门打开时，产品安全员需要全程陪同，仅限经批准的目的使用，并记录在《紧急门异常开启记录表》中。安防技术工程师在做月度检查时，测试开门报警功能时，不需产品安全员陪同。

Alarm for door opening: Be deployed for all fire doors and be on for 24*7 hours. Fire door only can be opened for emergency. For opening fire door for non-emergency, should contact with Security Policy Dept. leader to approve. Security Officers should supervise the fire door opening and maintain the Emergency Door Abnormal Opening Record. It needn't be supervised during monthly fire door test performed by Security Technical Engineer.

5.2.1.9. 货闸有人报警：处于 24 小时运作状态。当货闸关闭时，检测到有人站在货闸中间时，将产生本地报警声及监控室报警，此时双门锁定且刷卡无法开门。待监控室保安确认该报警后，授权人员只能刷员工所进的那个卷帘门，才能刷开。此为原进原出功能。

Goods-trap Occupation Alarm: Be on for 24 hours a day. If someone is detected to be in the loading area while the doors are closed, local audible alarm will be activated and alarm signal will be sent to SCR. The doors will be interlocked. Only the door employee opened to access can be opened by authorized personnel after SCR guard confirmed. This is the function of interlock doors to control personnel to exit from where they enter.

5.2.1.10. 卸货区缓冲区有人报警：处于 24 小时运作状态。当卸货区中卷帘门与内卷帘门关闭时，检测到有人站在缓冲区，将产生本地报警声及监控室报警，此时双门锁定且刷卡无法开门。待监控室保安确认该报警后，授权人员只能刷员工所进的那个卷帘门，才能刷开。此为原进原出功能。

Loading Area Occupation Alarm: be on for 24 hours a day. If someone is detected to be in the inner area while the inner and intermediate doors are both closed, local audible alarm will be activated and alarm signal will be sent to SCR. The door been opened lately can only be opened after guard within security control room has confirmed the alarm event. The doors will be interlocked. Only the door employee opened to access can be opened by authorized personnel after SCR guard confirmed. This is the function of interlock doors to control personnel to exit from where they enter.

5.2.1.11. 安防技术工程师应根据实际的各报警器位置制定《CCTV 报警系统厂房平面分布图》，并需实时更新，且至少每 90 天变更一次，交由部门领导审核。

Security Technical Engineer should make and update the Plant Layout of CCTV/Alarm System according the actual alarm location in-real time or at least every 90 days. The layout should be reviewed by dept. leader.

5.2.2. 门禁系统 Badge Access System

5.2.2.1. 公司各区域入口处均设有门禁系统，处于 24 小时运行状态。门禁控制系统设置在监控室，与 Internet 和公司内部网物理隔离，由安全策略部进行管理，任何人未经安全策略部授权，不得调整、设置、变更用途。保安对门禁系统的实时信息进行监控，对异常情况进行及时处理，并向门禁系统管理员进行报告。

Entrances are equipped with badge access controls which are working for 24 hours a day. The Badge Access System is in SCR, physically separated from Internet and internal network. Security Policy Dept. leaders and authorized employees are responsible for its management. Nobody could change its configuration without Security Policy Dept.'s authorization. SCR guard is responsible for supervising access information in real time, handling emergency events and report it to Security Control Engineer.

a) 门禁权限 Access Right

➢ 公司员工的门禁权限是根据权限最小化原则，针对《岗位权限对照表》中的岗位，在门禁系统中进行权限设置。The principle of access right allocation is 'need to be there'. Allocate access rights to employees' access badge according to the Position Access Right Reference List.

➢ 公司员工确因工作需要有权限新增或权限删除时，需要使用纸质或在协同办公 OA

平台上填写《人员权限变更/补卡申请单》进行申请、审批、权限变更。Any access right change for work needs should submit a Personnel Access to Change/Re-make Card Application Form to make request.

➢ 安全策略部结合各岗位的实际工作需求，而进行的权限变更，需要使用《门禁权限变更申请操作表》进行申请、审批、权限变更。Security Policy Dept. should change the access right considering actual request of each position. Make application and request by Access right changing application form.

➢ 门禁系统的具体操作内容都需要记录在《门禁系统操作记录表》上。Operation details of Badge Access System should be recorded on Access right changing application form.

➢ 门禁卡 90 天没有任何刷卡记录，将会自动失效。Access badge will be de-active automatically if no activity happened for more than 90 days.

b) 系统权限 System Privilege

➢ 系统权限由安全策略部部门领导授权，通常仅授权给门禁系统管理员，并记录在《密码权限一览表》中（含变更记录）。System privilege is generally authorized to Security Control Engineer by Security Policy Dept. leaders. The authorization will be recorded in List of Password Permissions being accompany with change history.

➢ 经授权的门禁系统管理员，使用各自的用户名和密码登陆，且登陆密码必须至少每 90 天变更一次。Security Control Engineer authorized should use his own ID and password to log in. Password should be changed every 90 days at least.

➢ 只有安全策略部部门领导和经授权的人员，才可以对门禁系统进行设置变更，每次设置完成后应退出门禁系统。Only Security Policy Dept. leader and authorized employees could change the Badge Access System configuration. Log off the system after configured every time.

➢ 门禁系统采用双人登陆，登录密码分为 2 段，由 2 名已授权的门禁系统管理员分别持有。登陆时必须由 2 人分别输入密码方可登陆系统进行操作。操作过程中，一人实际操作，一人现场监督。The password for administrator account is split into 2 components held by two administrators respectively. They key in his own passwords respectively to log in the system. During the operation, one administrator is responsible operation and another one is responsible for supervision.

c) 系统日志：门禁系统会生成每日日志，且日志必须每周备份。

System log: Badge Access System will generate daily logs. Logs must be backed up weekly.

d) 安防技术工程师应根据实际的各门禁位置制定《门禁系统厂房平面分布图》，并需实时更新，且至少每 90 天变更一次，交由部门领导审核。

Security Technical Engineer should make The Plant Layout of Badge Access System according to the actual access controller location. Update the layout in real time and submit it to security manager to review every 90 days.

5.2.2.1. 门禁卡的管理 Access Badge Management

a) 所有的空白门禁卡保存在监控室的保险箱里，并使用《空白门禁卡数量控制表》进行双控管理，实时记录使用数量。安防主管需每月对空白卡数量进行盘点，并记录在《安防控制检查表》中。

All access badges must be stored in the safe within SCR. Dually control them by Blank Access Badge Control Table and record the quantity used in real time. Security Access Control Supervisor should make inventory for all the blank access badges monthly and document on Security Access Control Checklist.

➢ 新员工临时卡：新员工入职当天，门禁卡管理员根据新员工的岗位设置相应的门禁权限。临时卡的发放记录需记录在《新员工临时卡发放回收登记表》中，发放正式员工卡时需要回收此临时卡。长期供应商采取与普通员工相同的要求进行管理。具体操作流程参考《人员安全管理标准》。New Employee Temporary Card: Issue temporary card to new employee on the day they entry, the temporary card will be set with the access right according to his position. Issue will be recorded on the Temporary Cards Use Registration Form. Surrender the temporary card after issue formal employee ID card. Management requirement for Long-term supplier is same as general employee. Refer Personnel Security Management Procedure for detail operation procedure.

➢ 正式员工卡：需要办理时，门禁卡管理员两人双控打开保险柜领取新的空白门禁卡，并需在《开柜记录表》上登记。正式员工卡办理完成后，需要员工在《门禁卡发放登记表》上签收。具体操作流程参考《人员安全管理标准》。ID Badge: Security Control Engineer should open the safe under dual control to pick the un-programed access badge and register on the Safe Cabinet Open Record. Formal employee should sign for the ID Badge on the Badge Access Issue Registration Form.

> 生产区域临时卡：各生产区域均有临时卡使用 Temporary Card for Production Area: Make temporary card for every production area.

  ✧ 非生产区域授权员工（含四川科道信息各子公司员工）确因工作需要临时到某一生产区域，需要所进区域的主管及以上级别的领导到监控室，在《临时卡使用登记表》现场签字确认后，再使用自己的员工卡在监控室更换相应区域的临时卡；临时卡必须当天下班前归还到监控室，并换回自己的员工卡。生产区域临时卡权限不包含金库、机房、碎卡室等双人刷卡进出的区域权限。For person needs to access production area of facility who is Tianyu's employee but not Pro Centre's employee, should exchange appropriate temporary card by his own ID badge after relevant leaders of production area sign to confirm his visit on Temporary Card Using Registration Form at the SCR. Temporary card must be returned before leaving to get back his own ID badge. This temporary cards do not with access to area need dual control access, such as vault, server room, destruction room etc.

  ✧ 若员工在此生产区域上班，其员工卡丢失、损坏或忘带时，可找上一级领导到监控室签字确认，换 0 号临时卡进入。待拿到员工本人的员工卡后，换回该临时卡。 Employee could exchange the temporary card to where he works after his direct leader's confirmation if forget to bring with own access badge. All the temporary card must be returned to SCR when get off work on the day.

> 访客卡：所有的访客进入生产区域前，均需要提前办理访客入厂手续，到达工厂时，在陪同人的带领下，使用自己的有效证件在监控室登记，并领取访客卡。离开时归还访客卡。Visitor Card: Deal with visiting procedure for visitors needing to access production area in advance. Receptionists accompany with visitor to show his own valid documentation and make registration at SCR and must return the visitor card to SCR before leaving.

> 应急卡：每个监控室均备有 2 张应急卡，保管在监控室的卡片柜中。不使用时，应急卡包在锡箔纸内，并在封口处粘贴有带编号的易碎标签。若有紧急情况需要使用时，需要安全策略部领导确认后使用，并在《应急卡使用记录表》上记录；使用完毕后，需要重新用带编号的易损标签封口，并在《应急卡使用记录表》上记录。Emergency Card: There are two emergency cards stored in safe in each SCR. The emergency card is packaged in silver paper and sealed with tamper-proofing label numbered during storage. The using for the emergency card should be recorded on the

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

密级：1 级 内部

Emergency Cards Use Record. Repackage them with new tamper-proofing label numbered and make record on the Emergency Cards Use Record after used.

b) 门禁卡的回收：当有员工辞职、解雇时，门禁卡管理员负责回收其门禁卡，在 24 小时内取消门禁权限，并执行销毁动作。记录需要保存在《门禁卡回收/销毁登记表》中。

ID badge Retrieval: Security Control Engineer is responsible for retrieve departure and dismissal employee's ID badge. Deactivate the ID badge within 24 hours and destroy them and make record on Badge Access Recycling/Destruction Registration Form.

c) 门禁卡的丢失/损坏：当员工、保安或其他人员发现门禁卡（包括员工卡、临时卡、访客卡、应急卡）丢失或损坏时，须立即报告安全策略部。门禁卡管理员应将丢失/损坏门禁卡在系统中立即删除，信息记录在《丢失/损坏门禁卡清单》中。丢失/损坏门禁卡需要补办时，需要使用纸质或在协同办公 OA 平台上填写《人员权限变更/补卡申请单》进行申请。

Damage and Loss of Access Badge: Report to the Security Policy Dept. of the access card's damage or loss discovered by employee, guards or others, including ID badge, temporary card, visitor card, emergency card. Security Control Engineer should deactivate the card damaged or missed in the system immediately. Keep record on the List of Lost/Damaged Badge Access. The re-make of access badge should be recorded on Personnel Access to Change/Re-make Card Application Form.

d) 所有已设置权限的门禁卡（含：临时卡、访客卡、应急卡）均需在《门禁卡核对表》中留下记录，且帐物一致，定期季度（每三个月）由安防控制工程师审核。已发放给员工的员工卡不在此范围内。

All the access badges be programmed with right should be recorded on Badge Access Check Form and cards should be consistent with the Form, including temporary card, visitor card, emergency card. Security Control Engineer should check the Badge Access Check Form and card programing quarterly, not including ID badge issued to employee.

5.2.3. CCTV 系统 CCTV System

5.2.3.1. CCTV 监控系统在厂房外围、内部各区域均设有摄像头。监控室的监控器显示固定摄像头图像，保安每天都必须根据《保安员作业指导书》，针对所有摄像图象

检查，发现任何问题，应立即报告。

Cameras are deployed at site exterior periphery and everywhere within site. The monitors within SCR are showing the fixed camera's video. SCR guards must check images of all cameras according to the Security Guard Work Instruction, and immediately report any issue discovered.

5.2.3.2. CCTV 应确保敏感区域被全覆盖，画面清楚，没有明显的信号干扰。CCTV 系统与报警系统和门禁系统关联，当报警系统和门禁系统关联报警时，应立即弹出关联画面，以及时确认异常情况。CCTV 系统与门禁系统时间、报警系统时间、北京时间必须同步，误差在 2 秒以内。

Keep CCTV to fully cover sensitive areas, be with clear image and without any obvious signal interference. CCTV system could communicate with alarm system and access control system. Any alarms generated from alarm system and access control system should be popped with relevant CCTV video. The time synchronization between CCTV system and access control system should be within 2s.

5.2.3.3. 安防技术工程师应根据实际的摄像头位置制定《CCTV 报警系统厂房平面分布图》，并需实时更新，且至少每 90 天变更一次，交由部门领导审核。

Security Technical Engineer should make and update The Plant Layout of CCTV/Alarm System according to the actual location of camera. Submit it to dept. leaders for review every 90 days at least

5.2.3.4. 安防技术工程师应根据实际的摄像头画面制定《CCTV 画面对照图》，并需实时更新，且至少每 90 天变更一次，交由部门领导审核。

Security Technical Engineer should make CCTV Image Contrast Figure according to actual camera image and update it in real time, and submit it to dept. leaders for review every 90 days at least.

5.2.3.5. 所有 CCTV 监控画面至少保存 90 天以上，且需每日异地备份。

All the CCTV monitoring videos should be retained for at least 90 days and be backed up off-site every day.

5.2.4. 监控照明 Illumination for Monitoring

公司外围及内部各区域设有监控用照明，厂房外围照明灯的开关由光敏开关自动控制，具体开启时间依据外部环境亮度而定。

Equip illumination for monitoring for all the area within company and exterior periphery. Illumination is controlled by light activated switch. The turn-on period is based on the sunrise and sunset time.

5.2.5. 钥匙管理 Physical Key Management

5.2.5.1. 重要钥匙 Important Key

a) 重要钥匙是指公司高安全区（如金库密码锁工具、…等）或公司公共区域（如外围栅栏门、阳台等）的钥匙，保管在监控室专用的钥匙柜中，由保安进行发放，并在 CCTV 的监控之下。

Important keys are the keys to HSAs such as key combination for vault etc. and the keys to public area such as fire door or balcony etc. They are stored in the special key box within SCR. SCR guards will issue the important key under CCTV monitoring

b) 《重要钥匙领用权限审批表》粘贴在重要钥匙的钥匙柜旁。授权可领用重要钥匙的人员名单，由部门领导提报、安全策略部审核批准，并每季度审核。

Important Keys Use Permissions Approval Form is pasted beside the key box stored with important keys. The list of authorized personnel to pick important keys is submitted by dept. leader and approved by Security Policy Dept. leader. It will be reviewed quarterly.

c) 授权员工提出需领用某一把钥匙时，保安要求员工出示员工自己的门禁卡，并核对该员工是否有该把钥匙的领用权限。

SCR guard should require personnel to show his own ID badge when they want to pick a key and verify their authorized right to pick key.

➤ 若员工没有该把钥匙的领用权限，申请人需要在《钥匙领用申请表》上进行该钥匙的申请，由提出部门领导审批，安全策略部审核批准后，方可领用。

Key applicant should make application for the key on Keys Use Application which

should be approved by his leader and security manager or his authorized backup if he does not has been authorized to pick the key.

➢ 若员工有该把钥匙的领用权限，保安要求领用人在《钥匙领用登记表》上，记录领用日期、领用时间、钥匙名称、钥匙编号、领用人、预计归还时间，保安发放相应的钥匙，并签名。

If the key applicant has been authorized to pick the key, SCR guard should require him to record the apply date and time, key name, key number, personnel name and return time planed on the Keys Use Registration Form. Sign to confirm after SCR guard issued the key.

d) 重要钥匙必须当天归还。使用完毕后，由领用钥匙的人立即将钥匙归还监控室，归还人及保安在《钥匙领用登记表》记录归还时间，并签字确认。

Important key must be returned on the day picked. Key applicant should immediately return to SCR after used. Key applicant and SCR guard should record the return time and sign to confirm on the Keys Use Registration Form.

e) 安全策略部部门领导或其授权人员每季度定期审核《钥匙领用登记表》。

IT & Security Dept. leader or authorized employee should check the Keys Use Registration Form quarterly.

f) 安防技术工程师应根据实际的各重要钥匙位置制定《重要钥匙厂房平面分布图》，并需实时更新，且定期季度（每三个月）由部门领导审核。

Security Technical Engineer must make The Plant Layout of Important Keys on the basis of the actual location of the important key and updated it in real time and submit it to dept. leaders for review every 90 days at least.

5.2.5.2. 一般钥匙 General Physical Key

a) 一般钥匙是指办公区内，办公室的钥匙；生产区各部门在日常工作过程中需要长期使用的钥匙。

General physical keys are the keys to offices in official area and the keys to be used for long-term by production dept. in daily work.

b) 所有保管一般钥匙的员工，均应在该钥匙发放清单上签名，承诺确保此钥匙不会被其他未授权的人员使用。实时更新《钥匙授权发放清单》，且定期季度（每三个月）

由部门领导审核。

All the employee holding general key should sign on the Authorization Key Issue List to promise not provide the key other unauthorized employee. Update the Authorization Key Issue List timely and submit it to dept. leaders for review every 90 days at least.

5.2.5.3. 备份钥匙 Key Backups

a) 所有的备份钥匙都保存在监控室的保险箱里，并通过《备份钥匙清单》进行管控。且由安全策略部部门领导或其授权人员每季度审核。

All key backups should be retained in the safe within SCR and be controlled by List of Backup Keys. Security Policy Dept. leaders or authorized employees should review the list quarterly.

b) 钥匙发生遗失时，相关责任人应立即以书面形式或电邮形式报告安全策略部，由安全策略部进行调查/确认后，通知综合管理部更换新的锁具。原有钥匙和对应的备份钥匙立即作废，由新锁具的钥匙替换原有钥匙和备份钥匙。

Relevant responsible should immediately report to Security Policy Dept. in written or e-mail when key is discovered to be missing. Security Policy Dept. should ask Administrator dept. to change the lock after investigation and confirmation. Previous keys and their backups should be destroyed immediately and be replaced by the new keys and key backups.

c) 备用钥匙主要在正常钥匙断裂，扭曲损坏等不能开锁的紧急情况时使用，由安全策略部的人员放置在位于监控室的保险柜中，并受 CCTV 的监控。

Key backup is only using for the emergency such as key is not useful for damage. Security dept. is responsible for storing it into the safe within security control room under CCTV monitoring.

5.2.5.4. 定期每季度对每把重要钥匙及锁孔进行匹配，并记录在《钥匙锁孔匹配核对表》中。若钥匙与锁孔不匹配，则需要立刻向安全策略部报告。

Re-match the key with the lock quarterly and make record on Key & Lock Match Checklist. Any mismatching should be reported to Security Policy Dept. immediately.

5.2.5.5. 当因员工离职、岗位变动等原因导致钥匙权限变更时，由安全策略部审核后，发布新的《重要钥匙领用权限审批表》。

Security Policy Dept. should review all the key authorization change for employee departure and position change and update Important Keys Use Permissions Approval Form as necessary.

5.2.6. UPS 管理 UPS Management

5.2.6.1. 所有的安防设施（监控照明除外）都由 UPS 提供电源。市电停电后，UPS 自动供电，柴油发电机将会在 1min 内自动启动，保证在停电时所有安防系统可维持 48 小时以上。

All the security and protection devices are powered by UPS. The diesel generator will start to supply power automatically within one minute after power failure to ensure the security and protection system could work for more than 48 hours.

5.2.6.2. 工程与设备部定期（每周）对柴油发电机检查/调试记录是否符合要求，并留下记录。

Equipment dept. should inspect the availability of UPS weekly and maintain record.

5.2.6.3. 定期季度（每三个月）对柴油发电机的可用性进行测试。安防技术工程师协调工程与设备部、安全策略部 IT 组、综合管理部相关人员，测试完成后留下记录。

Test the availability of diesel generator every three months. Security Technical Engineer is responsible for organizing Equipment Dept., IT team and Administration Dept. Test record should be maintained.

5.2.6.4. UPS 电源应定期检测其可用性，并测试 UPS 电源的实际功率以及负荷是否超载。

Test the availability of UPS regularly, including if the actual capacity and power is within the range.

5.3. 安防设施的检查 Security Devices Inspection

5.3.1. 日常检查 Daily Check

保安每日对 CCTV 系统进行日常检查。检查内容记录在《CCTV 日常检查记录表》中

Guard should conduct daily check for the CCTV system. Check details should be recorded on the Inspection Records of CCTV System.

5.3.1.1. 日志保存期：录像日志是否正常保存。

Log Retention Period: To check if the monitoring log is OK

5.3.1.2. 设备故障：对于设备中警告、错误、严重错误的判断和及时处理。

Equipment Failure: To verify and confirm the warming, error, serious error.

5.3.1.3. 设备状态：是否在正常录像中。

Equipment Status: To check if video recording is OK.

5.3.1.4. 时间同步：录像存储时间、CCTV 显示时间、远程客户端 PC 电脑时间误差是否在 2 秒内；CCTV 时间与门禁系统时间误差在 2 秒以内。

Time synchronization: To check if the time synchronization error is within 2s between video time, CCTV show time and remote client PC time, and if the time synchronization error between CCTV time and access control system time is within 2s.

5.3.1.5. 比照《CCTV 画面对照图》，查看各摄像头的方位及覆盖范围。

To look at the position and scope of camera against the CCTV Image Contrast Figure.

5.3.1.6. 图像质量问题（白天/夜晚）：图像的清晰度、明亮度、图像信号的干扰、是否有噪点、是否被镜边框遮挡、录像是否正常。

Image quality (day/night): To check the sharpness and brightness of images, and confirm if there is signal interference to video, if there is noise, if the image is blocked by the camera frame, if the CCTV system operates normally.

5.3.1.7. 保存期限：是否正常回放 90 天的录像。

Retention Period: could the video of last 90 days be replayed.

5.3.2. 周检查 Weekly Check

5.3.2.1. 系统管理员每周导出上周异常刷卡事件，进行评估，针对 10 次以上的违规情况进行跟踪检查，确定是否存在异常，并记录在《门禁系统记录异常报告》中，由违规的人员自行填写纠正预防改善措施，交由安全策略部部门领导或授权人员

审核。

Security Control Engineer should export abnormal access incidents of last week and analysis it. To make verification of violation incidents for more than 10 times. Make record on Access System Record Abnormal Report.

5.3.2.2. 安防主管应每周检查门禁系统中的配置变更的完整性及正确性，并记录在《门禁系统日志检查表》中。

Security Control Supervisor will check the integrity and validity of access system configuration weekly, and make record on Access System Log Inspection Records.

5.3.3. 月度检查 Monthly Check

5.3.3.1. 安防技术工程师每月对安防设施进行检查，检查内容记录在《厂房安防设施月度检查表》中，记录保存 3 年。

Security Technical Engineer should inspect the security devices monthly. Inspection detail should be recorded on the Security and Protection Facility Monthly Checklist which should be retained for three years.

a) 门禁系统检查：门禁系统日志、权限变更日志。Access control system check: access control system log, right change log.

b) 厂房门及安全通道检查：各门的物理结构无损坏、读卡器无脱落/无破损、电锁无损坏、闭门器无松动/无脱落、互锁功能完好、防折返功能完好、开门报警完好、25 秒延时报警完好、消防安全门锁闭正常。Door and Security Passageway Check: To check if the physical structure is OK, such as card reader, electric lock, door shutter and door's seal. To check if the required function is OK, such as interlock, anti-pass-back, alarm for door kept opening or open more than 25s is OK.

c) 外部灯光及四周围墙检查：外围灯光开启关闭时间、灯具无故障、配套的安防设施支架无倾斜、四周围墙无破损、外部安防设施控制盒保持上锁状态。Exterior Illumination and Fence Check: To check the turn-on and turn-off time of the illumination, the illumination equipment status, if the security and protection facility stand is slant, if the fence is integrate, if the exterior security and protection control box is locked.

d) 报警系统检查：电子围栏、红外光栅、红外对射探测器、红外移动探测器、胁迫按钮、震动报警、无人系统、货闸有人报警、卸货区缓冲区有人报警、UPS 功能正

常。Alarm System Check: To check if the alarm system function is OK, such as electronic fence, infrared grating, infrared radiation detector, infrared movement detector, duress button, movement detector, dead-man system, and data room man-trap, infrared movement detector in load and unload area, UPS.

e) 检查中发现异常的，填写《安防设施异常处理表》，并联系相关方进行维修。Any abnormity discovered during check should be recorded on Security Facilities Exception Handling Form and ask related party to repair.

5.3.3.2. 安防主管需每月对安全控制内容进行定期检查，检查内容包括但不仅限于：钥匙管控、密码管控、门禁卡管控、高安全区域访问清单、授权清单、报警系统、安全设施平面图更新、安防设施完好性及功能等进行定期检查，并需记录在《安防控制检查表》中，记录保存 3 年。检查过程中发现异常的，需开具《纠正、预防措施处理单》，并追踪整改效果。

Security Control Supervisor conducts monthly check for security controls, include but not limited to key control, password control, access card control, authorization list, alarm system, HSA accessing list, security and protection facility layout, regular security and protection etc. All the check detail should be maintained on Security Control Quarterly Checklist which should be retained for 3 years at least. Issue Corrective and Preventive Action Request to responsible employees for any non-conformities.

5.3.4. 半年度检查 Semi-annually Check

每半年由安防人员联系外部有资质的机构对工厂的安防系统进行功能完好性检测，并记录检测情况，检查报告至少保留 18 个月。

Security Control Engineer should ask external qualified organization to conduct function testing for security control systems and maintained testing detail semi-annually. The test report should be retained for 18 months at least.

6. 相关文件 Relevant Document

➢ 内部安全检查作业指导书 Security Audit Mgt. Standard

➢ 人员安全管理标准 Personnel Security Mgt. Standard

> 保安员作业指导书 Work Instruction for Security Guards

7. 相关记录 Relevant Record

> 密码权限一览表 List of Password Permissions

> 空白门禁卡数量控制表 Blank Access Badge Control Table

> 开柜记录表 The Safe Cabinet Open Record

> 新员工临时卡发放回收登记表 New Employee Temporary Card Issuance/Recycling Registration Form

> 门禁卡发放登记表 Badge Access Issuance Registration Form

> 门禁卡回收/销毁登记表 Badge Access Recycling/Destruction Registration Form

> 应急卡使用记录表 Emergency Cards Use Record

> 丢失/损坏门禁卡清单 List of Lost/Damaged Badge Access

> 门禁卡核对表 Badge Access Check Form

> 门禁系统记录异常报告 Access System Record Abnormal Report

> 门禁系统日志检查表 Access System Log Inspection Records

> 门禁权限变更申请操作表 Access Rights Change Applying and Operating Record

> 门禁系统操作记录表 Access System Operating Record

> 重要钥匙领用权限审批表 Important Keys Use Permissions Approval Form

> 钥匙领用申请表 Keys Use Application

> 钥匙领用登记表 Keys Use Registration Form

> 钥匙授权发放清单 Authorization Key Issue List

> 备份钥匙清单 List of Backup Keys

> 钥匙锁孔匹配核对表 Key & Lock Match Checklist

- 厂房安全级别平面图 The Layout of Plant Security Level

- CCTV 画面对照图 CCTV Image Contrast Figure

- CCTV 报警系统厂房平面分布图 The Plant Layout of CCTV/Alarm System

- 门禁系统厂房平面分布图 The Plant Layout of Badge Access System

- 重要钥匙厂房平面分布图 The Plant Layout of Important Keys

- CCTV 日常检查记录表 Inspection Records of CCTV System

- 厂房安防设施月度检查表 Inspection Record of Security Control System

- 安防设施异常处理表 Security Facilities Exception Handling Form

- 胁迫按钮测试清单 Duress Button Test List

- 胁迫按钮纠正行动记录表 Duress Button Corrective Actions Form

- 安防控制检查表 Inspection Records of Security Control

- 无人系统报警处理表 Alarm Processing Records of Dead-man System

- 紧急门异常开启记录表 Emergency Door Abnormal Opening Record

- 时间同步操作记录表 Time Synchronization Operation Record

- 授权手机使用清单 Authorized Phone Use List

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

密级：1 级 内部