

**澄天伟业（宁波）芯片技术有限公司**

|  |
| --- |
| **Physical Security Policy**  **物理及环境安全政策** |

Document Number文件编号:SCT-SP020

版本 V1.0

**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** |
| 1.0 | 2019/10/14 | First Issue首发 | 曹海翠 | 毛正锋 | 梅昌刚 |
|  | / / |  |  |  |  |
|  | / / |  |  |  |  |
|  | / / |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**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 PURPOSE AND SCOPE目的和范围

Physical Security measures are the primary means of defense against theft or misuse of products and services supplied by the company and are required to protect company know how. They are also a protection for the company personnel.

物理安全措施是防止公司产品和服务被盗窃或滥用的主要手段，他们指示公司如何防止事件发生，也包括对公司人员的保护。

This standard is applicable to all Chengtian Weiye (Ningbo) Chip Technology Co., Ltd must comply with the minimal security features as described in this standard in accordance with their domains of activity and the identified risks of their processes. Also refer to Organizational Security Standard.

本标准是适用于所有澄天伟业（宁波）芯片技术有限公司，它严格遵守根据员工活动区域和其流程识别出的风险制定的标准中的最小安全功能。也指组织安全标准。

# 2 PHYSICAL SECURITY STANDARD物理安全标准

All Chengtian Weiye (Ningbo) Chip Technology Co., Ltd domains of activity must apply the minimal physical security features as described in this document. The document “Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Premises Physical and Logical Security Zones” should be referred to for ensuring consistency between physical and logical security features.

所有澄天伟业（宁波）芯片技术有限公司活动必须应用本文档中所述的最小物理安全功能。"澄天伟业（宁波）芯片技术有限公司公司物理和逻辑安全区域"文档应确保物理和逻辑安全功能之间的一致性。

## 2.1 Zone Level Organisation 区级组织

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd activities include several domains that generate and have access to information of different classification levels.

澄天伟业（宁波）芯片技术有限公司活动包括生成和获得不同分类级别

#### 2.1.1Normal Zone (NZ)正常区域

Offices that do not host any form of production equipment or details of research or which are not used for development purposes is in Normal Zone.

办事处(办公室)，不承载任何形式的生产设备或研究的详细信息或不用于发展目的的是在正常区域中。

The type of protection depends on what is to be held, the number of persons who will be using the office, who requires access to it and its location within the building.

保护类型取决于将发生的项目，将会使用办公室的人员数目，需要访问它或其地点的大楼内的人员数目。

Normal Zone can be open spaces or separated closed areas with access control. According to the sensitivity of the handled information, separated areas are recommended for Headquarter, Human Resources, Legal and Finance departments.

正常区域可以是开放空间或需要访问控制的隔离的封闭区域。根据处理信息的敏感性，被分离的区域，建议为综合办公室、人力资源、法律和财务部门。

#### 2.1.2 Security Zone (SZ)　　安全区域

Any entity dealing with « Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Restricted» or « Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Confidential” documents has to be in Security Zone.

任何实体处理 «澄天伟业（宁波）芯片技术有限公司受限» 或澄天伟业（宁波）芯片技术有限公司机密"的文件，必须在安全区域中。

All production sites are classified as a Security Zone from their outer perimeter, inwards. This is regardless of the type of production being carried out.

所有生产基地被都列为从其外部外围向内的安全区。这与正在进行的生产类型无关。

The least sensitive R&D activities are also located in Security Zone.

最不敏感的 R&D 活动也都位于安全区。

#### 2.1.3 High Security Zone (HSZ)　　高安全区

Any entity dealing with « Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Confidential» and « Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Secret» classification levels require being located in High Security Zone. This includes the following activities:

«澄天伟业（宁波）芯片技术有限公司机密» 和 «澄天伟业（宁波）芯片技术有限公司秘密» 分类的任何实体处理文件要求在位于高安全区域内。这包括下列活动：

* Within a production site, any area involved in the manufacturing or the personalization of cards.

在生产现场，参与卡的制造或个性化设置的任何区域。

* Vaults used for storing banking cards or security materials used in their production

用于存储GSM卡或用于其生产的安全材料的仓库

* Dispatch areas handling security dispatches; security control rooms

处理安全派单的调度领域；安全控制室

* Research and Development areas, according to their specific activity

研究和发展领域，根据他们的具体活动

* Any other room that the Site Security Manager decides to classify in HSZ.

工厂安全经理决定分配在 HSZ的任何其他房间。

The Security Management Group must be consulted for the implementation of security features in HSZ.

HSZ 中安全功能的实现必须咨询安全管理小组。

### 2.1.4 Outside Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Premises　　澄天伟业（宁波）芯片技术有限公司外部

Some activities, like product demonstration, product customization are frequently performed outside the company premises.

一些活动，如产品演示、产品定制应经常在公司外进行。

Some others like tele-working, access to e-mail or Chengtian Weiye (Ningbo) Chip Technology Co., Ltd intranet can also occasionally take place outside normal working environment.

其他一些活动如远程工作，访问电子邮件或澄天伟业（宁波）芯片技术有限公司内网偶尔也可以在正常工作环境以外的地方实现。

These activities must be restricted depending on the classification level of the information they require to be performed, and the type of environment:

这些活动必须根据它们需要执行的保密级别和环境类型的不同加以限制：

#### 2.1.5 Public Zone (PZ)　　公共区域

A Public Zone is any location where no control is possible, such as airports, planes or trains.

公共区域是不受控制的例如机场、火车站等任何地点。

In such potentially hostile environment, only “Sha Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Public” or “Chengtian Weiye (Ningbo) Chip Technology Co., Ltd private” information may be handled. No sensitive information shall be deciphered or processed.

在这种潜在敌对的环境中，只有"澄天伟业（宁波）芯片技术有限公司公开"或"澄天伟业（宁波）芯片技术有限公司私人"信息可作处理。不能处理或破译任何敏感信息。

#### 2.1.6 External Zone (EZ)　　外部区域

An External Zone is any location outside Chengtian Weiye (Ningbo) Chip Technology Co., Ltd premises where basic controls are possible, like hotel rooms, customer premises, or Chengtian Weiye (Ningbo) Chip Technology Co., Ltdemployee’s home.

外部区域是像酒店客房、客户处所或澄天伟业（宁波）芯片技术有限公司员工之家等澄天伟业（宁波）芯片技术有限公司处所以外的任何位置。

In such context, information up to “Chengtian Weiye (Ningbo) Chip Technology Co., Ltd confidential” may be handled with restriction. For example confidential e-mails received after connection to Chengtian Weiye (Ningbo) Chip Technology Co., Ltd network via to VPN can be deciphered for reading, but they have to be re-enciphered immediately after usage.

在这种背景下，"澄天伟业（宁波）芯片技术有限公司机密"的信息处理方式可能有限制。例如机密邮件到澄天伟业（宁波）芯片技术有限公司网络后通过对 VPN 连接可以解密进行读取，但他们必须在使用后立即加密。

For further details about the way to manage Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. asset and information outside a Chengtian Weiye (Ningbo) Chip Technology Co., Ltd environment refer to the procedure about “Nomadism”.

有关管理澄天伟业（宁波）芯片技术有限公司的方式进一步详细信息和澄天伟业（宁波）芯片技术有限公司环境之外的信息请参阅有关“离散人员”。

## 2.2 Segregation of Areas区域隔离

Another fundamental security principle is, for a given security level, the segregation of areas for:

另一项基本的安全原则是，对于给定的安全级别，隔离的领域：

1. Ensuring that two activities cannot be concurrently held by a single person,

确保两项活动不能由单人同时进行，

1. Protecting the information need-to-know for restricted or confidential information.

保护需知信息的受限和机密。

Based on this principle some activities must be held in separate rooms, with their specific access rights.

基于这一原则，活动必须在单独的房间，和他们的特定访问权限下进行。

Among activities that require such physical segregation, here are some examples：

需要物理隔离的活动为，下面是一些示例：

|  |  |  |
| --- | --- | --- |
| Areas…区域 | **Activity …活动** | **Segregated from …与…隔离** |
| **Production**  **生产** | Personnel flows生产人员 | Goods flows货物流动 |
| GSM card /Module manufacturing GSM卡和模块生产 | GSM card personalization； Module manufacture GSM卡个人化;模块生产 |
| GSM card personalizationGSM卡个人化 | PIN mailer printing PIN邮寄打印 |
| Data preparation数据准备 | Card personalization卡个人化 |
| Product Manufacturing产品制作 | Product development/testing产品开发/测试 |
| **Administration**  **管理** | Human Resources, Payroll, Legal人事部，财务，法律 | Any other team任何其他部门 |
| Purchasing Department采购部 | Subcontracted personnel分包人员 |
| Security teams and systems安全部和安全系统 | Any other team任何其他组 |
| CEO, Top Management, Strategy最高领导人，总经理，政策 | Other teams其他组 |
| IT servers IT服务器 | Teams部门 |
| **R&D**  **研究与开发** | Segregation of areas may be required depending on:  隔离区可依据:   * type of asset: Key, Source, Exe, Doc资产类型 * product type/ family: Native (NPX), Java产品类型 * product layer: OS, Crypto, Platform, Application产品阶层   role in product lifecycle: Development, Validation, Support, Customization, Maintenance  在产品生命周期中的作用：发展、验证、支持、自定义、维护 | |

# 3 PHYSICAL SECURITY MEASURES物理安全措施

## 2.2.1 Site Perimeter Protection现场周边保护

The basis of all physical protection should be to start with a means of protection at the extremity of a site and allow access to the site on a strictly controlled basis. Additional measures should then be put in place to add to the level of security protection which is commensurate with the risk to those products, services or know how in need of protection.

所有的物理保护的基础应是从开始在对一个站点的极端保护并严格控制对站点的访问的基础上，然后对这些产品、服务风险，如何保护等相应添加额外措施。

For this reason, wherever possible, it is recommended that the site should be surrounded by a fence of at least 2 meters in height. It should ideally be of a solid construction, (i.e. metal palisade, not merely chain link.) with access and egress gates being kept to a minimum and controlled from within the premises or by an access control system. Areas where the transfer of “high security” goods takes place should be additionally segregated externally in addition to secure loading bays.

为此，只要有可能，建议厂区应被包围在高度至少 2 米的围墙里。理想情况下应有坚固的结构，(即金属栅栏，) 通道和出口的门被保持在最低限度并和由公司内部或通过门禁控制系统监控。“高安全”货物进行转移的地区应在装卸区的基础上另外划分。

If it is not possible to implement a fence (local law doesn’t allow it, or high building), a formal detection has to be added before the building (i.e. complete CCTV coverage controlled 24 hours/ 24 by a guard, or intrusion system before the building)

如果无法建一个围墙（当地法律不允许，或高层建筑不允许），应在大厦之前添加正规的检测 (即 CCTV 的完全覆盖，由警卫队24 小时控制，或添加大厦的入侵系统)

When the parking area used by employees or visitors is located inside the site perimeter, it is considered as Normal Zone. It must then be physically segregated from loading bay area. So that it is not possible to go from the parking to the loading bay and vice versa.

当雇员或访客所使用的停车区域位于内部站点外围时，它被视为正常区域。它必须和装卸区从物理上分隔。即他们是无法到达装卸区的，反之亦然。

## 2.2.2 Exterior Building Security 外部建筑安全

### 3.2.1 Building Construction建筑施工

The structure of the building has to be compliant with the followings:

建筑物的结构必须要符合以下：

* Secured walls (concrete) or shock detectors implemented on the wall

有保护墙 (混凝土) 或休克探测器在墙上

* Secured windows or simple windows with physical protection (unbreakable glass, grids, steel bars…)

安全窗户或简单的窗户用实物(不碎玻璃、网格、钢棒......)保护

* Opening windows in high security areas must be fitted with contact monitors and covered with wire mesh

在高安全区中的窗户必须装有接触显示器并覆盖着金属丝网

* Secured doors (external doors: solid steel or equivalent, contact alarm monitored)

安全门 (外门：固体钢或等效，连接报警监测)

* Secured roof traps (solid steels, contact alarm monitored)

安全屋顶陷阱 (固体钢，连接报警监测)

* External pipes, e.g. drainage/ AC, should be fitted with some form of physical obstruction or other method to prevent climbing.

外部管道，如排水 / AC，应装有某种形式的物理障碍物或其他方法来防止攀爬。

### 3.2.2 External Building Surveillance外部大厦监控

External areas of the site must be illuminated at night and the exterior of the building must be under alarm (see §3.3) and surveyed by CCTV (see §3.9). Special care must be taken to gates, doors and emergency exits.

对站点的外部区域必须在夜间照明，建筑的外墙都必须在警报状态下 (参见第 3.3 节)，并由CCTV监控（见 §3.9）。必须特别注意大门、门和紧急出口。

### 3.2.3 Emergency door of workshop车间应急门

There is CCTV coverage outside and inside of the emergency exit . Once they are opened, the local alarm will sound, and the monitoring room will also receive the alarm signal.车间紧急出口外面和里面都有CCTV覆盖，们一旦被打开，本地报警器响起，同时监控室也会收到报警信号。

## 2.3.3 Alarm System 报警系统

The building should be protected by an alarm system. This should be monitored on site and, when the building is closed during certain periods, through a local alarm monitoring station.

大厦应装有报警系统。它必须由站点监控，在某些时候大厦关闭时，由当地监测台控制。

Power supply should be protected and backed-up by UPS.

电源应保护并由 UPS备份。

### 3.3.1 Basic基本

The alarm system should cover all external doors and windows, internal high security areas such as vaults and places designated for the storage of high security materials. It should provide a means of summoning assistance in the event of emergency i.e. panic attack buttons.

报警系统应涵盖所有外部门窗、高安全存储区和指定存放高安全材料的高安全区。它应提供紧急援助的一种手段如恐怖袭击按钮。

The alarm system may be linked with the access control system or may be a separate installation.

报警系统可能与门禁控制系统链接，或者可能是一个单独的安装。

Records of activation should be maintained together with records of service to the system.

激活记录应在系统中与服务记录一同保存。

A local procedure should document the operation of the system. The procedure should remain confidential to those persons who have a need to be involved in the operation of the system. It should include instructions on how activations are to be dealt with.

本地流程应对系统的运作存档。这个程序应该对那些涉及系统操作的人保持机密。它应包括有关如何处理激活的指令。

### 3.3.2 By Zone根据区域

As a complement to the basic system described above, the alarm system allows to have some specific areas activated closed to some others deactivated.

如上文所述，报警系统允许有一些特定激活的区域与非激活区域相邻。

Activation on one specific area can be:

一个特定领域的激活可以是：

* Manual: e.g. a guard activates one area when nobody is inside

手册：例如警卫队将激活一个地区，当没人在里面时

* Semi-automatic: a time limit is defined to activate the alarm

半自动：对警报设置时间限制

### 3.3.3 Automatic自动化

In some High Security Area, the alarm system is automatically activated when the last person exits.

在一些高安全区域中，当最后一个人退出时将自动激活报警系统。

A software counter must increment the number of cards registered within the card access control system every time that a card has been checked in or out. The area must be protected with an internal movement detector that should activate the alarm system each time the last employee on duty has checked out.

软件计数器必须增加注册卡门禁控制系统内每一张卡已经被签入或签的时间卡的数目。该地区必须由内部运动检测器保护，它应在每次值班的最后一名雇员已签出后激活报警系统。

## 3.4 Access Control 访问控制

Within Chengtian Weiye (Ningbo) Chip Technology Co., Ltd premises, all personnel must be identified by a badge. This badge must be worn visibly at all times by all employees, contractors and visitors and is used by the access control system.

澄天伟业（宁波）芯片技术有限公司处所内的所有人员必须由一个门禁卡。门禁卡必须将佩戴明显地在所有时间所有员工、承建商及访客，由门禁控制系统使用。

The badge management and the operation of access control systems must be documented in a local procedure.

门禁卡管理和门禁控制系统的运作必须记录在本地的过程。

Card access systems that allow entry into restricted areas must have a backup electrical power source capable of maintaining the system for 48 hours.

允许进入限制区的卡访问系统必须有备用电源，能够维持48小时的系统。

### 3.4.1 Basic基本

#### 3.4.1.1 Access control system门禁控制系统

Access to the premises should be controlled with an access control system or suitable locking mechanism in accordance with the zone definitions. The access control system should conform to company standards. A record of authorization of access must be retained in respect of each employee and visitor and updated according to any change from the original requirement.

进出公司应设置门禁控制系统或根据区域定义的锁定机制。门禁控制系统应符合公司的标准。授权访问的记录必须保留每个员工和访客，并对根据原先的要求进行的任何更改作更新。

Access to normal zones is granted to all Chengtian Weiye (Ningbo) Chip Technology Co., Ltd employees.

授予澄天伟业（宁波）芯片技术有限公司的所有员工对普通区域的访问权限。

A principle of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd policy is that access control systems in operation on all sites will utilize Chengtian Weiye (Ningbo) Chip Technology Co., Ltd cards, certified cards readers and access control system software to facilitate entry to sites.

澄天伟业（宁波）芯片技术有限公司政策的一个原则是门禁控制系统中的所有站点上的操作将会利用澄天伟业（宁波）芯片技术有限公司卡、认证读卡器和门禁控制系统软件，设置公司的进出。

### 3.4.1.2 Reinforced加强

The basic access control system has to be reinforced for stronger authentication in high security zones:

基本的门禁控制系统应予以加强，为在高安全区域更强的身份验证：

* In R&D environment, this is achieved in placing successive access controls when moving from a zone security level to another one. An authentication with pin code may be added to reader.

在 R&D 的环境中，通过从一个区域的安全级别移动到另一个时放置连续访问控件实现。身份验证与 pin 代码可能添加到读卡器中。

* In production sites, the access control must guarantee the traceability of all movements from a zone to another for every single person. (for instance placing successive access controls)

在生产车间，访问控制必须保证从一个区域到另一种的每一个人的所有运动的可追溯性。（例如将置于连续访问控制中）

#### 3.4.3.1 Single sluice entry points单闸入口点

Production zones where security products are manufactured or personalized should additionally be subjected to a person-by-person entry system, to make sure that each authorized person is recorded when entering/exiting from high security zone, and separate goods.

用于生产或个性化的生产区在此外应受一个“一人接一人”的进入系统，以确保每个获授权的人和单独的物品从高安全区进入/退出时的记录。

Goods are transferred from secure zone to high secure zone or conversely via good traps and do not allow people: see 3.6.

货物将通过不允许人进入的货闸从安全区转移到高安全区，反之亦然：见 3.6。

#### 3.4.3.2 Anti pass back反潜回门

The anti pass back function consists in managing the gradual passages from one zone to another one. This system enforces people to systematically record their passages at each controlled point.

反潜回门功能包括管理从一个区域到另一个中的逐步通过。这一系统强制记录人员在每个控制点的通过。

### 3.4.4 Specific特殊

Further features are required for specific areas:

特定领域需要进一步的功能：

#### 3.4.4.1 Areas under dual control双控下区域

Such areas require the implementation of two badge readers, distant of at least three meters, both outside and inside.

If it is not possible to implementat least three meters (buildingcan’t allow it,) has to be added “badge + Password” for dual control before into the Areas.

这种领域需要两个门卡读卡器，两边距离至少为三米，内外设置相同。

如果因建筑设置不能满足最少3米的距离，不得不采取门禁卡+密码的双人控制下进入安全区。

It is also recommended that the access control system permanently increments/decrements the number of persons present at a given time and activates an alarm as soon as there only one person present for more than 30 seconds.

建议门禁控制系统永久增量/递减在给定时间的在场人数并在只剩下一人超过30秒时尽快激活警报。

#### 3.4.4.2 Security Control Room安全控制室

Access to the security control room is permitted only to security guards and authorized employees on duty.

仅允许安全警卫和授权雇员访问安全控制室。

The security control room door must be fitted with an “in and out” card reader access control system with anti-pass back function and capable of recording all entry and exit transactions. The door must also be fitted with an automatic closing device. The opening of the door for a time lapse exceeding 30 seconds should automatically activate a sound alarm. The access control system must be programmed whereby access is restricted to authorized personnel only.

安全控制室的门必须装有"进出"卡读卡器的门禁控制系统与反潜回功能，并能记录所有的进入和退出情况。门还必须装有自动关闭装置。门开启超过 30 秒后应自动激活声音报警。门禁控制系统必须进行编程，藉以限制只有授权人员的访问。

When the security control room is located within a high security zone, additional access controls must be enforced to ensure the security guards do not have direct access to the production areas.

The security control room must be equipped with two independent means of communication (one of which being cellular) and a fixed silent duress button, and protected with a passive infrared (PIR) detector.

安全控制室位于高安全区内时，必须执行额外的访问控制，确保安全警卫并没有到生产领域的直接访问。

安全控制室必须配备两个独立的通信手段（其中之一为移动电话）和固定的无声胁迫按钮和受保护的一种被动红外 (PIR) 探测器。

During working hours the security control or receptionist areas must always be staffed by at least one guard or employee. After working hours, all security protection devices (including activation and deactivation) must be monitored electronically by either an in-house security monitoring system or by a private central monitoring company

在工作时间内至少一个警卫或雇员总是必须在安全控制或接待员领域。工作时间后，所有的安全保护装置（包括激活和取消激活）必须监视以电子方式通过任一内部的安全监控系统或私人的中央监测公司

#### 3.4.4.3 EMV Card Production Computer Room EMV卡生产计算机室

The room containing network and computer equipment for the production of EMV banking cards must be located in the high security area. The door must be fitted with an access control system that restricts entry to authorized personnel only. All doors must have an automatic closing device in which the opening of the door for a time lapse exceeding 30 seconds should automatically activate a sound alarm.

包含生产的GSM卡网络和计算机设备的房间必须位于高安全地区。门必须装有限制为只有授权人员才能门禁控制系统。所有的门必须有门开启超过 30 秒的时间间隔应自动激活声音报警自动关闭装置。

The room must be protected with an internal movement detector.

房间必须使用内部运动探测器保护。

An internal CCTV camera must be installed in order to cover the access to this room and provide an overview of the room whenever there is activity inside. The camera must not be provided with zoom or scanning functionality and must not be positioned in such a manner as to allow observation of keystroke entry or the monitoring of the screen during key loading sessions.

内部闭路电视摄像机必须安装以覆盖到这个房间并显示画面无论里面有无活动。相机不能提供缩放或扫描功能，并不允许的击键项观察或在密钥加载会话期间监测屏幕的方式定位。

## 3.5 Guarding 警卫

All Chengtian Weiye (Ningbo) Chip Technology Co., Ltd are guarded by security personnel that are usually subcontracted.

澄天伟业（宁波）芯片技术有限公司都有通常分包的安全人员守卫。

Prior to their recruitment a screening procedure must be performed. When joining an Chengtian Weiye (Ningbo) Chip Technology Co., Ltd, they must sign a Confidentiality Agreement and receive the appropriate training. Their duties should be clearly defined and documented in working instructions.

在其招聘之前必须执行一个筛选过程。当加入澄天伟业（宁波）芯片技术有限公司，他们必须签署保密协定，接受适当的培训。他们的职责应清楚地定义和记录在工作指示中。

### 3.5.1 Standard标准

At the main entrance, a security desk with a guard or a receptionist is responsible for the entrance and departure of visitors during site standard opening hours. He must have unobstructed visual contact with the reception area at all times, and may allow visitors to enter only after identification has been established and the appropriate ID badge issued.

在主要入口处，一名警卫或接待员在公司开放时间内负责访客的进入和离开。他必须总是有广阔的视角，只允许已建立身份认证且持有ID门卡的访客进入。

During working hours the security control or receptionist areas must always be staffed by at least one guard or employee. After working hours, all security protection devices (including activation and deactivation) must be monitored electronically by either an in-house security monitoring system or by a private central monitoring company.

在工作时间内至少一个警卫或雇员总是必须在安全控制或接待员领域。工作时间后，由任一内部的安全监控系统或私人的中央监测公司必须以电子方式监测所有的安全保护装置（包括激活和取消激活）。

## 3.6 Goods Flows and Traps　货物流通通道

Segregation of goods and personnel is a fundamental security principle, implying separate access points and flows.

货物和人员的隔离是一项基本的安全原则，这意味着单独访问点和流动。

Under no circumstances should persons (staff or any other) be afforded access through goods loading bays into any internal area.

在任何情况下，人员 (工作人员或任何其他人) 都无法获得从货物装卸区到任何内部区域的访问。

## 3.7 Goods storage and Vaults　　货物存储和仓库

### 3.7.1 Warehouse　　仓库

All non-sensitive products and materials are stored in a warehouse, accessible only to authorized persons.

所有非敏感产品和材料都存储在仓库中，只有授权人员才能访问。

### 3.7.2 HSA& Vault　　高安全存储区&金库

All sensitive products and materials must be stored in a HSA or Vault: chips, micro-modules, holograms, signature panels, semi-finished cards, finished cards.

所有敏感产品和材料必须存储在高安全存储区或金库中：芯片，微型模块、全息图、签名板、半成品的卡、成品卡。

A vault must be constructed of reinforced concrete (minimum 15 cm), or of materials providing equivalent strength. Outside wall of the building shouldn’t be used as a wall of this vault, and no windows are permitted. Walls and ceiling must be fitted with shock detectors.

金库必须由钢筋混凝土（最低 15 厘米），或提供等效强度的材料建造。外建筑物的墙壁不应该用作此存储库的一堵墙，且不允许有窗户。天花板和墙上必须装有冲击探测器。

It must be fitted with a duress button, be alarmed and locked when nobody is inside (movement detectors) and covered by CCTV system. See also §3.9.

它必须装有胁迫按钮、无人在里面时 (运动探测器)被锁定并被闭路电视系统所覆盖。请参阅 §3.9。

The vault must be equipped with a steel reinforced door bearing a double mechanism that requires dual access control. This main door must be closed whenever no staff is present.

金库必须配备强化门系列，要求双重的访问权限控制的双重机制。每当没有工作人员时，必须关闭此主门。

The inner grid (or “day gate”) must have dual access control as well as an auto closing mechanism. It must remain closed and locked at all times, except when staff requires access to store or remove items.

内部网格（或"天门"）必须具有双重的访问权限控制，以及自动关闭机制。它必须保持在所有时间锁定和关闭，除了工作人员需要访问存储或移除物件时。

HSA&Vault access is restricted to a limited number of persons and must be permanently under dual control.

高安全存储区和金库的访问仅限于有限的人，必须永久双重控制之下。

HSA&Vault security management should be documented in a local procedure that includes details relating to dual control requirement, and opening/ closing routines. The list of authorized accesses should be audited periodically.

高安全存储区和金库安全管理应记录在本地流程中，其中包括有关的双重控制的要求，打开 / 关闭流程的详细信息。应该定期审核授权访问列表。

When the vault is used to store financial and non-financial products, there must be a physical separation between the two categories.

当电子仓库用来存储金融和非金融产品时，必须有两个类别之间的物理隔离。

In banking personalization centers it is recommended to have 2 vault zones:

在银行个性化设置中心建议有 2个电子仓库区：

* Daily zone that contains opened trays

每日区域包含打开托盘

* Stock zone that contains wrapped trays and boxes.

存储区域包含包装托盘和箱子

Such organization facilitates inventories and audits

这种组织方便了库存和审计

### 3.7.3 Shredding Room　粉碎间

Sensitive product reject destruction has to be performed in a shredding room, accessed under dual control, covered by CCTV system and locked when nobody is inside.

敏感产品的销毁必须在粉碎间进行，双控访问，有CCTV摄像头且在无人时锁定。

Destruction sessions must be fully documented, including exact number of cards, exhaustive description, date, time and signature of the two custodians.

必须充分记录销毁过程，包括卡片数目、详尽的描述、日期、时间和保管者的两个签名。

## 3.8 Secure Cabinets 安全文件柜

The use of secure cabinet is mandatory to store sensitive information or media as specified in the Information Security Classification Policy. They have to be fitted with a digital code or classic key locking mechanism.

安全文件柜是强制用来存储敏感信息或作为信息安全分类策略中指定的媒体。他们必须装有一个数字代码或传统的密码锁定机制。

Those systems can also be used to protect from fire.

这些系统也可以用于保护免受火灾。

## 3.9 CCTV Monitoring 闭路电视监控

To assist in maintaining a secure environment - both inside and outside the building – a Closed Circuit Television monitoring system should be utilized. The power supply of this system should be protected and backed-up by UPS, as well as the lighting of covered areas.

为了协助维持一个安全的环境--大厦内部和外部 —应加以利用闭路电视监控系统。这一系统的电源应保护和备份的 UPS，以及照明的覆盖区。

Monitors and recorders must be located in an area that is restricted from unauthorized personnel.

监视器和录像机必须位于一个领域，限制未经授权的人员。

A local procedure should document the operation of the system.

本地流程应存档系统的运作。

### 3.9.1 Camera Location摄影机位置

This system will cover at least all exterior boundaries of the building and all areas inside defined as security manufacturing or personalization areas, including vaults and loading bays.

这一系统将涵盖至少大厦的所有外部边界，里面的所有领域都界定为安全制造或个性化领域，包括电子仓库和货物装卸区。

In order to cover all high security and restricted areas, CCTV cameras must be strategically located:

为了涵盖所有的高安全和受限制的区域，闭路电视摄影机必须从战略上位于：

* At all accesses to these areas,

所有访问到这些地区的地方，

* Within production areas to cover all activities for manufacturing sites.

生产领域内覆盖制造车间的所有活动。

All work in progress (WIP) stored in sensitive or high security areas must be within range of a CCTV camera. Also, staff should be aware that when working in high security areas they are subject to constant camera surveillance without knowledge of the camera’s visual range.

在敏感或高安全领域中的所有进展中的工作 (WIP) 都必须在闭路电视摄像机范围内。此外，工作人员应认识到在高安全性领域中工作时他们受到恒定摄像机监视，但不知道可视范围。

Each camera view must include all activities necessary to provide adequate security coverage with recommended scanning frequency of 24 seconds. Critical areas must be under constant video surveillance.

每个相机视图必须包括所有活动，建议每秒24帧扫描以提供充分的安全保障。关键领域必须在不断视频监视之下。

Each internal CCTV camera and recording system must be equipped with an automatic recording capability in case of an alarm event.

每个内部闭路电视摄像机和录音系统必须在发生报警事件配备自动录制能力。

CCTV cameras must be connected at all times to:

闭路电视摄影机必须在所有时间连接到：

* Monitors located in the control room.

坐落在控制室的监视器。

* The Alarm System.

报警系统。

* A 7\*24 image-recording device.

一台7\*24的图像记录设备。

### 3.9.2 Video Recording视频记录

Images received from cameras should recorded using an appropriate recording system and must be retained for a minimum period of three months. Tapes or discs used to store images must be checked daily to ensure images are being recorded correctly.

收到来自摄像机的图像应使用适当的记录系统记录，必须保留为期至少三个月。用来存储图像的磁带或磁盘必须每日检查，以确保正确地记录图像。

At least annually all images received from cameras must be reviewed to ensure the image being captured is the image for which the camera was originally installed to provide for, and the image is still relevant to the security of the building or process. The technical operating standards required of a CCTV system may be obtained from corporate security.

至少每年对从摄像机接收的所有图像必须都审查，以确保正在捕获的图像是为其相机最初安装的提供的图像和图像仍然与该建筑物或进程的安全相关的。闭路电视系统所需的技术操作标准可索取公司安全。

Finally, it is important to ensure that only Chengtian Weiye (Ningbo) Chip Technology Co., Ltd security management people have access to recording system.

最后，它重要的是要确保只有澄天伟业（宁波）芯片技术有限公司安全管理人有对录音系统的访问。

### 3.9.3 Monitors监视器

Images received from cameras should be displayed on monitors, with appropriate size and definition.

收到来自摄像机的图像应带适当的大小和定义监视器上显示。

CCTV monitors should be located in a security room, with a person in charge of checking regularly the images, especially for very sensitive areas.

闭路电视监视器应位于监控室，且有一人负责定期检查图像，尤其是非常敏感的地区。

They can be placed in the security control room, in a position that allows guards to check images but not visible to visitors and personnel.

可以将它们放在安全控制室，在允许警卫检查图像但参观者和工作人员不可见的位置。

## 3.10 Receipt and Dispatch Areas 收货和发货区

To facilitate the shipment and delivery of secure products, the loading/unloading area must be composed of at least two consecutive rooms that minimize physical contact between the individuals collecting or delivering materials and the Chengtian Weiye (Ningbo) Chip Technology Co., Ltd shipping/delivery employees.

为了安全产品便于装运和交货，货物装卸区必须由至少两个连续的房间组成，尽量减少个人收集或提供材料和澄天伟业（宁波）芯片技术有限公司发货/交付员工之间的身体接触。

|  |  |
| --- | --- |
| Doors ➀➁ and ➂must operate on an interlocking basis that allows only one door to be opened at one time.  门1、2和3必须允许只有一扇门一次打开互锁基础上运作。  The intermediate zone allows the driver to load/unload the truck, without any Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. personnel being present.  中间区域允许装货/卸载卡车，没有任何澄天伟业（宁波）芯片技术有限公司人员在场。  Chengtian Weiye (Ningbo) Chip Technology Co., Ltd employees transfer the shipped/delivered goods when no truck is present.  澄天伟业（宁波）芯片技术有限公司员工转让已发运交付货物时没有卡车在场。  Door ➂must also be protected by an In and Outaccess control system.  门3也必须按出入口控制系统得到保护。 |  |

An intercom communication system allows identification of driver and goods to be delivered/shipped.

对讲通信系统允许鉴定司机和要发出/接收的货物。

In addition, CCTV cameras must be installed and oriented to cover the external and internal access doors, and capture all activity during shipment/delivery.

此外，必须安装并面向包括内部和外部的访问门，并在装运/交货期间捕获所有活动的闭路电视摄影机。

One of the walls separating this area from the facility contains a security window ➃for the exchange of documents.

隔离这一区域的一面墙壁须包含安全窗4用于交换文件。

Receipt and dispatch of secure products and materials together with instructions on identity checks to be carried outon couriers should be the subject of local procedures.

收货和发货安全可靠的产品和材料，包括有关身份检查以关于携带者进行的说明应该是本地程序的主题。

## 3.11 Mail 邮件

Receipt of mail, which includes instructions on how to deal with suspect packages, must be documented in a local procedure. Specific staff training for those employees who are most likely to come into contact with suspect packages should be provided.

接收的邮件，其中包括有关如何处理可疑包裹的说明，必须记录在本地流程中。应提供具体的工作人员培训那些最有可能接触到可疑包裹的雇员。

## 3.12 Physical Key Management 物理钥匙管理

Whenever an area is locked with physical key, a register of keys should be maintained and all keys should be stored in a secure cabinet under control of Site Security Manager when not in use, and when they are used to access to high security zones. It is recommended that key tags be color coded to clearly define the different types of keys in use in a building and thus the different conditions applying to their use. A local procedure should document the storage, issue and general control of keys.

每当一个区域用物理钥匙锁住后，应维持一份钥匙登记册，所有钥匙应在不使用时储存在安全经理控制下的文件柜里。建议对钥匙标记颜色编码来清楚地定义不同类型的钥匙，从而将应用于其使用的不同条件。本地过程应存档存储、问题和一般控制钥匙。

# 4 PRODUCT AUDITABILITY MEASURES产品的可审计性措施

## 4.1 Traceability and Accountability 可追溯性和问责制

Each high security and restricted area (such as card storage area, card manufacturing and waste disposal area, personalization area, mailing area, shipping and delivering area, and vault or other area containing any other sensitive card product material or carrier) must maintain audit logs for recording the movement of all security component or partly processed products that are transferred between areas.

每个高安全性和限制的区域（如卡存储区域、卡制造和废物处理区、个性化设置区、邮寄区、装货和交付区域，和高安全存储区或包含任何其他敏感卡产品材料或承运人的其他区域），必须保持审计日志中的记录所有安全组件移或部分区域间转移的产品的活动。

All cards must be accounted for throughout the production process. All card products must be counted and reconciled prior to any transfer of responsibility.

在整个生产过程中，所有卡产品必须计数。责任移交时也必须计数和调解。

A local procedure must document the overall traceability and accountability system.

本地过程必须存档整体的可追溯性和问责制度。

## 4.2 Production Audit Processes 生产审核流程

An effective audit control trail must be established for each of the functions associated with production activities of card products or components. Audit control documents must be completed at the end of each production cycle and attached to, or included with, the work-in-process.

为每个卡产品或组件的生产活动与相关的职能必须建立有效审核控制记录。必须在每个生产周期结束时完成和附加到或附带-工作审计控制文件。

In addition, two persons at the end of each production step must sign the control documents. Audit control documents always must be reconciled and attached to unfinished batches when changing shifts:

此外，两人在结束了每个生产步骤后必须签署控制文件。审计控制文档总是必须核对且换班时附加到未完成的批处理：

**Initial stock = good + sample + quality/test + rejected + not used**

最初的库存 = 好品 + 样品 + 质量/测试卡 + 坏卡 + 未使用数

Audit control logs that can account for the quantity and location of all card products and components within their facility (such as partly processed and finished card products, lithographic films and printing plates, signature panels, magnetic tapes and diskettes, or any other carrier containing sensitive information).

审核可以说明所有卡产品和组件（如部分加工、成品卡产品、平版印刷薄膜和印刷板、签名板、磁带和磁盘、或任何其他包含敏感信息的载体）的数量和位置的控制日志。

Vendors must be able to confirm that the materials used in the manufacture of card products, including waste, matches the amount indicated in the inventory control

供应商必须能够确认所使用的卡产品，包括废物、制造的材料与高安全存储区中的数量相匹配

## 4.3 Sample Management 样品管理

When orders are being manufactured, the factory may retain:

当订单开始生产，工厂必须保持：

* A partially processed sample of card product or a component

部分处理过的卡产品或组件的示例

* A portion of a previously printed sheet

部分预先打印的工作表

* A sample product received from an outside source provided that documentation indicating the source, quantities and the distribution of each sample also is included

外部源提供的样品，以文件说明来源、数量，也包括每个样品的分布

While in the production workshop, samples are to be stored in a job jacket or the work packet. They can be used for quality inspections, or sent to certification bodies or to the customer.

而在生产车间，样品是存储在工作夹克或工作包中。他们可以用于质量检验、或发送到证书颁发机构或客户。

When not stored in the vault or sent outside the production site, GSM card samples must be appropriately voided.

当不存储在存储库中或发送外部生产站点时，GSM卡样本必须适当地失效。

A local procedure must document the sample management.

本地过程必须以文档示例管理。

The same measures apply when semi-finished products are to be sent to development/qualification centers or marketing teams for producing pilot or tests cards.

同样的措施在半成品要发送到开发/质量中心或市场营销团队生产试验或测试卡时也应用。

In such cases the receiving site must also comply with the procedure “Card Management in Non production Environment”.

在这种情况下接收站点也必须遵守"卡在非生产环境中的管理"程序。

# 5 ABNORMAL EVENT MANAGEMENT异常事件管理

Abnormal situations include all suspect packages, bomb threats, terrorist incidents or hostage situations.

异常情况包括所有可疑包裹、炸弹威胁、恐怖事件或人质的情况。

The term “terrorist incident” is often used to categorize a number of types of incident and these are not always ideologically based, as the true source of terrorist attacks in fact are more likely to be criminally based.

"恐怖事件"一的词往往用于分类那些不是基于思想的事件，而恐怖袭击的真正来源更倾向于是以犯罪为前提。

This standard requires that consideration is given to the possibility of such incidents occurring at respective sites around the world and regular assessment of the possibility of such attacks is made and recorded. It is also required that procedures are in place locally to cater for such incidents, the primary objectives of which are the protection of staff and others and the protection of company property.

这一标准需要考虑到各自站点在世界各地发生的此类事故的可能性和所作和录得的这种攻击的可能性的定期评估。它也需要本地流程以应付此类事件的发生，其中的首要目标是保护工作人员和其他人和公司财产的保护。

Threat assessments should be made which examine the long-term threats and short-term threats.

应作威胁评估审查长期和短期威胁。

Long-term threats should examine the site, its occupants and the nature of the business. Each of these threats should be examined in relation to its attractiveness as a target for terrorists. Such analysis should bear in mind any previous threats and the outcome of them. Knowledge of any threats made to other companies within our industry is also helpful in making an accurate assessment. Liaison with local police is another means of improving the accuracy of any assessment. Long-term assessments should generally be carried out annually by Site Security Managers in conjunction with members of the Security Management Group.

长期威胁应审查站点、其居住者和业务性质。每个这些威胁应予其作为目标的吸引力研究为恐怖分子。这种分析应铭记任何先前的威胁和它们的结果。对我们的行业内的其他公司所做的任何威胁的知识也是有助于作出准确的评估。与当地警方联络是另一种改进评估准确性的方法。长期应一般每年由站点安全管理人员配合安全管理组的成员进行评估。

Short-term assessments are based on sets of facts or circumstances that are known to exist. These will be carried out in the same manner as described above. However they will be carried out as soon as positive information comes to hand.

短期评估基于一系列事实或已知存在的情况。这些将以同样的方式进行如上文所述。不过他们将在积极信息到达之前出现。

### 5.1.1 Terrorist Threats恐怖威胁

#### 5.1.1.1 Parcels and letters包裹和信件

Terrorists or other organizations or individuals are capable of making a number of different types of bomb which purpose is to cause death, injury or damage. The assessment at this point in time is that parcel or letter bombs are the most likely type of device to affect this company.

恐怖分子或其他组织或个人能制作一定数量不同类型的炸弹来造成死亡、伤害或损害的目的。在这个时间点的评估是那包裹或信件炸弹最有可能影响本公司的设备的类型。

A local procedure should therefore be in place to counter such threats.

本地过程因此应到位，以对付这种威胁。

#### 5.1.1.2 Telephone calls电话

In addition to the threat of actual devices being received or placed within company premises, telephone calls may be received to the effect that such devices have been placed within the company premises. Such threats should never be ignored.

除了实际设备接收或放在公司处所内的威胁，可能会在公司内安置了这种装置的接收到电话的情况。这种威胁永远不应该被忽略。

Careful recording of the call should take place, using the form Terrorist Attack Call Checklist [R3]. Staff whose primary role is the answering of telephones as initial point of contact with the company should be schooled in the taking of such calls and the completion of the form.

应仔细记录电话内容，使用恐怖威胁电话清单的形式。负责接听电话的公司工作人员应受过此类训练并能完成表格。

### 5.1.2 Incident Handling事件处理

The nature of a threat or the receipt of a suspect package turns a threat into an incident. Control of such incidents is the means by which the safety of employees and others is achieved during the course of the incident.

威胁本身或接收可疑包裹将威胁转变成事件。这类事件的控制是其中员工和其他人的安全已经确保后进行的。

This standard requires that there should be a person at each site who is capable of taking charge of such incidents together with a nominated deputy. Generally this person should be thesecurity manager.

这一标准要求应该有一个人在每个站点能够负责处理这类事件以及提名的副手。一般此人应为安全经理。

A bomb incident procedure should be developed for each site. This should include plans, including details of personnel, of how searches will be carried out once a threat has been received and assessed to the extent that action is required. It should also include plans for summoning police assistance and the evacuation of the building. In developing this procedure it should be noted that summoning the police will not necessarily mean they will conduct searches. Also the evacuation plan for a site in relation to bomb incidents must not automatically be regarded as being the same as for escape from fire.

应为每个站点开发一个处理炸弹事件流程。这应包括计划，包括人员，包括一旦收到了威胁，搜索行动如何进行。它还应包括召唤警方援助和大楼疏散计划。在发展中国家应该指出的是召唤，警方将不一定意味着他们会在此过程中进行搜索。此外一个站点就炸弹事件的疏散计划不能自动视为相同的火灾逃生。

Assistance in preparing such plans is available from the Security Management Group.

安全管理组可编制这种计划援助。

Refer to the Security Incident Handling & Reporting Procedure

请参阅安全事件处理&报告程序

# 6 INTERNAL AUDIT PROGRAM AND PREVENTIVE MAINTENANCE内部审计程序及预防性维修

Many of the requirements of this policy and the corresponding procedures require regular checking processes. In addition to a preventive maintenance plan including regular technical inspections and servicing of equipment, an internal audit program must ensure the continued, correct and effective operation of all security devices.

这一政策和相应程序的要求的许多需要定期检查过程。包括定期技术检验和维修设备的预防性维修计划，内部审计程序必须确保所有安全设备的持续、正确和有效运作。

## 6.1 Internal audit program 内部审核系统

The frequency of checks must be defined based on the importance and reliability of each physical security system. Guidelines should be in place defining precisely how checks are to be carried out.

检查频率的定义必须基于每个物理安全系统的可靠性和重要性。在适当的位置有准则精确定义应如何进行检查。

Audit plan and results need to be documented and auditable such that the date and time of each individual element being checked can be determined.

审计计划和结果需要记录和可审核，每个个例的时间和日期都能被检查到。

### 6.1.1 CCTV system闭路电视系统

Checks must be performed on the images provided by CCTV equipment to ensure:

必须由CCTV提供的图像执行检查：

* The images are relevant to the security of the premises

有关公司经营场所的安全的图像

* Each monitor, camera, and video or digital recorder must function properly, without being out-of-focus, blurred, washed out, or excessively darkened.

每个显示器、照相机和视频或数字录音机必须正常运行，没有被焦外模糊，被冲垮了，或过分变暗。

### 6.1.2 Alarm system警报系统

Regular tests on alarms must verify that:

定期测试警报必须验证：

* All alarms are activated and work properly

所有报警被激活和正常工作

* All access doors are under control, without security system disconnection or obstruction.

所有访问门都正在控制，安全系统连接没有断开或梗阻。

* The response time to any alarm activation is compliant with agreed process between Chengtian Weiye (Ningbo) Chip Technology Co., Ltd and the security guards company.

对任何报警激活的响应时间是符合澄天伟业（宁波）芯片技术有限公司和保安公司之间商定的。

### 6.1.3 Access control system门禁控制系统

The audit program carried out on access control system must cover:

门禁控制系统进行的审计程序必须包括：

* The correct and effective of operation of access controls devices

正确和有效地操作访问权限的控制设备

* The justification and record of all given access rights.

已给访问权限的记录和原因。

* The response time and escalation process in case of authorized access attempt.

尝试授权访问的响应时间和升级过程。

## 6.2 Reporting to Corporate Security 向公司安全部报告

The results from above security audits must be monthly collected and reported to the Corporate Security thought SCART (Security control and reporting tool)

安全审核结果必须每月收集和通过SCART（安全控制和报告工具）向公司安全部报告

In addition to these physical tests all production sites must also report using SCART:

这些物理测试所有生产站点还必须都使用 SCART报告：

* Logical tests on anti-virus management, server and network access, logs, etc.

逻辑测试防病毒管理、服务器和网络的访问权限、日志等。

* Production tests on audits trail data.

生产测试审计跟踪数据。

## 6.3 Specific Banking Requirements 具体银行业务要求

Each site manufacturing or personalizing banking cards also has to comply with Banking regulatory bodies specific requirements.

每个制造或个性化银行卡的站点也须遵守银行业监管机构的具体要求。

A semi-annual inspection must be conducted on all security devices and hardware including:

每半年必须对所有的安全设备和硬件进行检验包括：

* Access control system

门禁控制系统

* Alarm system

报警系统

* Silent duress buttons

无声胁迫按钮

* Vault locking mechanisms

高安全存储区的锁定机制

* CCTV cameras, monitors, and video or digital recorders

闭路电视摄像机、监视器和视频或数字录音机

* Uninterrupted Power Supplies.

不间断的电源。

Such inspections should be carried out by an external organization licensed to perform such functions. A copy of the inspection report must be maintained for at least 18 months and presented to auditors on request.

这种检查应由领有牌照来执行这种功能的外部组织进行。必须保持一份检验报告至少18个月并提交给审核官。

Records of service must be maintained which show what parts of the system have been serviced and any parts that have been modified or replaced.

必须保存维护记录以便显示在系统的哪些部分有服务和被修改或更换任何部件。7 LOGBOOK USE日志使用

Logbooks are used whenever there is a need for keeping records of specific events.

日志是用于保留特定事件的记录。

Logbooks in card production are mainly used for:

卡生产中日志主要用于：

* Visitor control

访客管制

* Vault access

高安全存储区访问

* Safe content and in-out movement logs

安全内容和进出日志

* Key management server access

密钥管理服务器的访问

* Physical key usage for sensitive areas

敏感领域物理密钥的使用

* Logical key management

逻辑密钥管理

* Film/plate destruction

菲林/印版销毁

* Reject destruction.

不合格品销毁。

Logbooks must be identified (Title, Number, Location, Start date), bound with pre-numbered pages and prepared with all the fields to be completed.

日志必须确定（标题、数量、位置、开始日期）、绑定预编号页和所有准备。

At each new occurrence of an event all necessary information must be filled with indelible writing in the next available record (line, column or page), dated and signed.

在每个新事件发生的所有必要的信息必须在接下来的可用记录（行、列或页）中填满不可磨灭的笔记，标日期和签署。

Unless otherwise specified, all logbooks should be archived for at least two years.

除非另外指定，否则所有日志应存档，至少两年。

They should be audited periodically to make sure that all events can be properly traced back.

他们应定期进行审计，以确保可以正确跟踪所有事件。

# 8 ANNEX 1 : Security Features Required by Domain附件1：域所需安全功能

## 8.1 Production Sites 生产站点

The following tables define for each zone level (normal zone, security zone, and high security zone) the corresponding security measures applied in a production site.

下表为每个区域级别（正常区域、安全区和高安全区）定义了相应的安全措施在生产现场中的应用。

These security controls are further detailed above, in the paragraphs 3 and 4.

这些安全控制进一步详见上文，3和4。

### 8.1.1 Minimal security features for Normal Zone (NZ) in a Production site

生产现场正常区域的最小安全特征

|  |  |  |
| --- | --- | --- |
| **Site Perimeter Protection**  **站点周围保护** | External fence with control access  外部围栏配置访问控制 | [3.1](#_Site_Perimeter_Protection) |
| **Alarm system**  **警报系统** | Basic: External doors and windows coverage  基本：覆盖外部门窗 | [3.3.1](#_Basic) |
| **Access control**  **访问控制** | Basic: Cards access control system  基本：卡权限控制系统 | [3.4.1](#_Basic_1) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.2](#_Permanent) |
| **Secure Cabinets**  **安全文件柜** | Safe or locked cabinet mandatory to store sensitive information  保险箱或带锁柜子强制性存储敏感信息 | [3.8](#_Secure_Cabinets) |
| **CCTV**  **闭路电视** | Entire activities coverage  覆盖整个活动 | [3.9](#_CCTV_Monitoring) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |

### 8.1.2 Minimal security features for Secure Zone (SZ) in a Production site

生产现场安全区域的最小安全特征

|  |  |  |
| --- | --- | --- |
| **Site Perimeter Protection**  **站点周围保护** | External fence with control access  外部围栏配置访问控制 | [3.1](#_Site_Perimeter_Protection) |
| **ExternalBuilding Security**  **外部大厦安全** | Reinforced building construction and external surveillance  加强大厦建筑和外部监视 | [3.2](#_Exterior_Building_Security) |
| **Alarm system**  **警报系统** | By Zone: Alarm system activated when nobody is inside the area  按区域：无人时激活区域警报系统 | [3.3.2](#_By_Zone) |
| **Access control**  **访问控制** | Second access control from Normal Zone to Secure Zone  从正常区到安全区的第二次访问控制 | [3.4.2](#_Access_to_Secure) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.2](#_Permanent) |
| **Goods Flows and Traps**  **货物流通和货闸** | Separated access points and flows for goods and personnel  货物和人员流通访问点隔离 | [3.6](#_Goods_Flows_and) |
| **Storage and destruction**  **存储和销毁** | Vault or Warehouse storage and shredding room mandatory  高安全存储区或仓库和粉碎间强制性 | [3.7](#_Goods_storage_and) |
| **Secure Cabinets**  **安全文件柜** | Safe or locked cabinet mandatory to store sensitive information  保险箱或带锁柜子强制性存储敏感信息 | [3.8](#_Secure_Cabinets) |
| **CCTV**  **闭路电视** | Entire activities coverage  覆盖整个活动 | [3.9](#_CCTV_Monitoring) |
| **Receipt & Dispatch area**  **收/发货区域** | Loading bay with interlocked system  装卸区配置联锁系统 | [3.10](#_Receipt_and_Dispatch) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |
| **Sample management**  **样品管理** | Secure storage and accountability of sample  样品安全储存和问责制 | [4.3](#_Sample_Management) |

### 8.1.3 Minimal security features for High Secure Zone (HSZ) in a Production site

生产现场高安全区域的最小安全特征

|  |  |  |
| --- | --- | --- |
| **Site Perimeter Protection**  **站点周围保护** | External fence with control access  外部围栏配置访问控制 | [3.1](#_Site_Perimeter_Protection) |
| **ExternalBuilding Security**  **外部大厦安全** | Reinforced building construction and external surveillance  加强大厦建筑和外部监视 | [3.2](#_Exterior_Building_Security) |
| **Alarm system**  **警报系统** | Automatic: Alarm system is automatically activated when the last person exits  自动化：当最后一人离开时自动激活警报系统 | [3.3.3](#_Automatic) |
| **Access control**  **访问控制** | Reinforced access control (anti pass back or Single sluice)  强制访问控制（反潜回门或单闸） | [3.4.3](#_Specific) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.2](#_Permanent) |
| **Goods Flows and Traps**  **货物流通和货闸** | Separated access points and flows for goods and personnel  货物和人员流通访问点隔离 | [3.6](#_Goods_Flows_and) |
| **Storage and destruction**  **存储和销毁** | HSA &Vault or Warehouse storage and shredding room mandatory  高安全存储区&金库或仓库和粉碎间强制性 | [3.7.2](#_Vault) |
| **Secure Cabinets**  **安全文件柜** | Safe or locked cabinet mandatory to store sensitive information  保险箱或带锁柜子强制性存储敏感信息 | [3.8](#_Secure_Cabinets) |
| **CCTV**  **闭路电视** | Entire activities coverage  覆盖整个活动 | [3.9](#_CCTV_Monitoring) |
| **Receipt & Dispatch area**  **收/发货区域** | Loading bay with interlocked system  装卸区配置联锁系统 | [3.10](#_Receipt_and_Dispatch) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |
| **Sample management**  **样品管理** | Secure storage and accountability of sample  样品安全储存和问责制 | [4.3](#_Sample_Management) |

### 8.1.4 Production site security zones生产现场安全区

The table below identifies for each domain of activity, the required security zone and specificities.

下表为每个域的活动、所需的安全区和特殊性。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Domain of activity** | | | | **Zone Level** | **Specificities vs. zone definition** | **§** |
| **Administrative area管理区** | Order management,  订单管理  Finance财务 Security, Facilities,  安全设施 Human Resources,  人力资源 IT & MIS | | | **NZ** | 1 - CCTV coverage not mandatory  1.CCTV 非强制性覆盖  2 - Locked office mandatory for human resources & financial.  人力资源部与财务部强制上锁 | [3.9](#_CCTV_Monitoring) |
| **Computer room (office network)** |  | | | **SZ** | **Not mandatory** within this **SZ** area:  1- Mail procedure  2 - Sample management process | [3.11](#_Mail)  [4.3](#_Sample_Management) |
| **Studio (Check & print)** |  | | BNK | **SZ** | **Not mandatory** within this **SZ** area:  1- Separate access points and flows for goods and personnel  2- Shredding room and vault storage  3- CCTV coverage  4- Loading bay | [3.6](#_Goods_Flows_and)  [3.7](#_Goods_storage_and)  [3.9](#_CCTV_Monitoring)  [3.10](#_Receipt_and_Dispatch) |
|  | | GSM | **NZ** | Locked office mandatory |  |
| **Data processing** | Office/Desk | | | **HSZ** | Alarm by zone sufficient (like for **SZ**) | [3.3.2](#_By_Zone) |
| Computer Room | | | **HSZ** | With an access control specific to the computer room see § 3.4.4.1 | [3.4.4.1](#_Areas_under_dual) |
| **Production** | Micro-electronics | | | **HSZ** | Alarm by zone sufficient (like for **SZ**) | [3.3.2](#_By_Zone) |
| Card Body Production | | BNK | **HSZ** | Alarm by zone sufficient (like for **SZ**) | [3.3.2](#_By_Zone) |
| GSM | **SZ** | - |  |
| Chip Embedding | | BNK | **HSZ** | Alarm by zone sufficient (like for **SZ**) | [3.3.2](#_By_Zone) |
| GSM | **SZ** | - |  |
| Card Personalization | | BNK | **HSZ** | - |  |
| GSM | **SZ** | - |  |
| PIN code/ Mailer | | | **HSZ** | - |  |
| Shipment & Delivery | | BNK | **HSZ** | Alarm by zone sufficient (like for **SZ**) | [3.3.2](#_By_Zone) |
| GSM | **SZ** | - |  |
| Maintenance | | | **SZ** | - |  |
| **Storage** | Vault | | | **HSZ** | With access control under dual control | [3.4.4.1](#_Areas_under_dual) |
| Warehouse | | | **SZ** | - |  |
| **Facilities** | Technical room | | | **NZ** | In a reinforced building construction with external surveillance | [3.2](#_Exterior_Building_Security) |
| **Security** | Security control room | | | **HSZ** | With an access control specific to the security control room see § 3.4.4.2 | [3.4.4.2](#_Security_Control_Room) |
| **Quality** | Office | | | **NZ** | 1 - In a reinforced building construction with external surveillance  2 – With a process of sample management | [3.2](#_Exterior_Building_Security)  [4.3](#_Sample_Management) |
| Card Testing | BNK | | **SZ** | Sample storage in vault mandatory | [3.7.1](#_Warehouse) |
| GSM | | **SZ** | Basic Alarm system sufficient | [3.3.1](#_Basic) |

## 8.2 Research and Development Sites 开发和发展站点

The following tables define for each zone level (normal zone, security zone, and high security zone) the corresponding security measures applied in R&D departments.

下表为每个区域级别（正常的区域、安全区和高安全区）定义了相应的安全措施在 R&D 部门中的应用。

These security controls are further detailed above, in the paragraphs 3 and 4.

这些安全控制进一步详见上文，第 3 和第 4 段。

### 8.2.1 Minimal security features for Normal Zone (NZ) in a R&D site

|  |  |  |
| --- | --- | --- |
| **Alarm system**  **警报系统** | Basic: External doors and windows coverage  基本：覆盖外部门窗 | [3.3.1](#_Basic) |
| **Access control**  **访问控制** | 1 - Basic: Cards access control system基本：卡权限控制系统  2 - Locked offices锁办公室 | [3.4.1](#_Basic_1) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.1](#_Standard) |
| **Secure Cabinets**  **安全文件柜** | Safe or locked cabinet mandatory to store sensitive information  保险箱或带锁柜子强制性存储敏感信息 | [3.8](#_Secure_Cabinets) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |
| **Sample management**  **样品管理** | Secure storage and accountability of sample  样品安全储存和问责制 | [4.3](#_Sample_Management) |

### 8.2.2 Minimal security features for Secure Zone (SZ) in a R&D site

|  |  |  |
| --- | --- | --- |
| **Alarm system**  **警报系统** | By Zone: Alarm system activated when nobody is inside the area  按区域：无人时激活区域警报系统 | [3.3.2](#_By_Zone) |
| **Access control**  **访问控制** | Second access control from Normal Zone to Secure Zone  从正常区到安全区的第二次访问控制 | [3.4.2](#_Access_to_Secure) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.1](#_Standard) |
| **Secure Cabinets**  **安全文件柜** | Safe or locked cabinet mandatory to store sensitive information  保险箱或带锁柜子强制性存储敏感信息 | [3.8](#_Secure_Cabinets) |
| **CCTV**  **闭路电视** | Entire activities coverage  覆盖整个活动 | [3.9](#_CCTV_Monitoring) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |
| **Sample management**  **样品管理** | Secure storage and accountability of sample  样品安全储存和问责制 | [4.3](#_Sample_Management) |

### 8.2.3 Minimal security features for High Secure Zone (HSZ) in a R&D site

|  |  |  |
| --- | --- | --- |
| **Alarm system**  **警报系统** | Automatic: Alarm system is automatically activated when the last person exits  自动化：当最后一人离开时自动激活警报系统 | [3.3.2](#_By_Zone) |
| **Access control**  **访问控制** | Reinforced access control (anti pass back or Single sluice)  强制访问控制（反潜回门或单闸） | [3.4.3](#_Specific) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.1](#_Standard) |
| **Secure Cabinets**  **安全文件柜** | Safe or locked cabinet mandatory to store sensitive information  保险箱或带锁柜子强制性存储敏感信息 | [3.8](#_Secure_Cabinets) |
| **CCTV**  **闭路电视** | Entire activities coverage  覆盖整个活动 | [3.9](#_CCTV_Monitoring) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |
| **Sample management**  **样品管理** | Secure storage and accountability of sample  样品安全储存和问责制 | [4.3](#_Sample_Management) |

### 8.2.4 R&D site security zones

The table below identifies for each domain of activity, the required zone level and specificities.

|  |  |
| --- | --- |
| **Domain of activity** | **Zone Level** |
| IT System “Secure Network” | **SZ** |
| IT Application “Secure Network” | **SZ** |
| Secure Network server room | **HSZ** |
| Personalization Software Engineering (PSE) standard development | **NZ** |
| PSE security software | **SZ** |
| Tools Development | **NZ** |
| OTA platform | **NZ** |
| GGS non sensitive software | **NZ** |
| Order Engineering | **NZ** |
| Readers and POS | **NZ** |
| Card OS and GGS sensitive activities | **SZ** |
| POS sensitive activities | **SZ** |
| Hardware development | **SZ** |
| Corporate Test/Qualification labs | **SZ** |
| Security labs & cryptography | **HSZ** |
| Product Quality & others labs | **SZ** |

## 8.3 HeadQuarter, Administrative & Sales sites 总部、行政和销售站点

The following tables define for each zone level (normal zone, security zone, and high security zone) the corresponding security measures applied in an administrative site (headquarter, sales, etc.).

下表为每个区域级别（正常的区域、安全区和高安全区）定义了相应的安全措施在管理网站中的应用（总部、销售等）。

These security controls are further detailed above, in the paragraphs 3 and 4.

这些安全控制进一步详见上文，第 3 和第 4 段。

### 8.3.1 Minimal security feature for Normal Zone (NZ) in an administrative site

|  |  |  |
| --- | --- | --- |
| **Alarm system**  **警报系统** | Basic: External doors and windows coverage  基本：覆盖外部门窗 | [3.3.1](#_Basic) |
| **Access control**  **访问控制** | Basic: Cards access control system  基本：卡权限控制系统 | [3.4.1](#_Basic_1) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.1](#_Standard) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |

### 8.3.2 Minimal security features for Secure Zone (SZ) in an administrative site

|  |  |  |
| --- | --- | --- |
| **Alarm system**  **警报系统** | By Zone: Alarm system activated when nobody is inside the area  按区域：无人时激活区域警报系统 | [3.3.2](#_By_Zone) |
| **Access control**  **访问控制** | Second access control from Normal Zone to Secure Zone  从正常区到安全区的第二次访问控制 | [3.4.2](#_Access_to_Secure) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.1](#_Standard) |
| **Secure Cabinets**  **安全文件柜** | Safe or locked cabinet mandatory to store sensitive information  保险箱或带锁柜子强制性存储敏感信息 | [3.8](#_Secure_Cabinets) |
| **CCTV**  **闭路电视** | Entire activities coverage  覆盖整个活动 | [3.9](#_CCTV_Monitoring) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |

### 8.3.3 Minimal security features for High Secure Zone (HSZ) in an administrative site

|  |  |  |
| --- | --- | --- |
| **Alarm system**  **警报系统** | Automatic: Alarm system is automatically activated when the last person exits  自动化：当最后一人离开时自动激活警报系统 | [3.3.2](#_By_Zone) |
| **Access control**  **访问控制** | Reinforced access control (anti pass back or Single sluice)  强制访问控制（反潜回门或单闸） | [3.4.4](#_Security_Control_Room) |
| **Guarding**  **警卫** | Permanent presence of guards  保安永久在现场 | [3.5.1](#_Standard) |
| **Secure Cabinets**  **安全文件柜** | Safe or locked cabinet mandatory to store sensitive information  保险箱或带锁柜子强制性存储敏感信息 | [3.8](#_Secure_Cabinets) |
| **CCTV**  **闭路电视** | Entire activities coverage  覆盖整个活动 | [3.9](#_CCTV_Monitoring) |
| **Mail**  **邮件** | Reception of mails (suspected mail) to be documented  邮件（可疑邮件）接收存档 | [3.11](#_Mail) |
| **Physical keys**  **物理钥匙** | Physical key management process documented  物理钥匙管理过程存档 | [3.12](#_Physical_Key_Management) |

### .3.4 Administrative site security zones 管理工厂的安全区域

The table below summarizes for each domain of activity the required zone security level and the specificities.

下表总结了每个活动定义所需的区域安全等级与具体情况。

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain of activity**  **活动定义** | **Zone Level**  **区域等级** | **Specificities vs. zone definition**  **具体情况vs区域描述** | **§** |
| Top level Management最高级管理 | **SZ** | - |  |
| Sales 销售 | NZ | - |  |
| Customer Services客服 | NZ | - |  |
| Marketing市场 | NZ | 1 - With a process of sample management  2 - Safe or locked cabinet or locked office  1-样品管理过程  2-保险柜或上锁的柜子或上锁的办公室 | [4.3](#_Sample_Management)  [3.8](#_Secure_Cabinets) |
| Human Resources人力资源 | NZ | 1 - Locked office mandatory  2 - Safe or locked cabinet  1-办公室强制上锁  2-保险柜或上锁的柜子 | [4.3](#_Sample_Management)  [3.8](#_Secure_Cabinets) |
| Legal法律 | NZ | Locked office mandatory  办公室强制上锁 |  |
| Licenses & Intellectual Property  许可证&知识产权 | **SZ** | - |  |
| Finance财务 | NZ | Locked office mandatory  办公室强制上锁 |  |
| Communication沟通 | NZ | - |  |
| Consulting / subcontractor  顾问/转包商 | NZ | - |  |
| Supply chain/ Purchasing  供应链/采购 | NZ | - |  |
| Corporate Manufacturing teams  企业生产小组 | **NZ** |  |  |
| Studio (Check & Print) | **SZ** | - |  |
| Security office  安全部 | NZ | Locked office mandatory  办公室强制上锁 |  |
| Corporate IT Security/ key management  企业IT安全/密钥管理 | **HSZ** | - |  |
| Security Control Room/ systems  安全控制室/系统 | **HSZ** | - |  |
| Security Control Room/ Guards  安全控制室/保安 | **HSZ** | - |  |
| Quality Office  质量部 | NZ | With a process of sample management  样品管理程序 | [4.3](#_Sample_Management) |
| Test Laboratory  测试实验室 | **SZ** | With a process of sample management  样品管理程序 | [4.3](#_Sample_Management) |
| IT offices IT部 | NZ | - |  |
| IT system admin “office network”  IT系统管理“网络部” | NZ | Locked office mandatory  办公室强制上锁 |  |
| IT application admin “office network”  IT申请管理“网络部” | NZ | Locked office mandatory  办公室强制上锁 |  |
| Servers Room 服务器房 | **SZ** | - |  |
| Technical supportOffice技术支持部 | NZ | With a process of sample management  样品管理程序 | [4.3](#_Sample_Management) |
| Technical support Lab.技术支持实验室 | **SZ** | With a process of sample management  样品管理程序 | [4.3](#_Sample_Management) |