

**澄天伟业（宁波）芯片技术有限公司**

|  |
| --- |
| **Security Manual**  **安全手册** |

Document Number文件编号：SM01

Version版本：V1.0

**Distribution Controls发行管制**

The 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**  **更新信息** | **Author**  **主办** | **Censorship**  **审查** | **Approbation**  **核准** |
| 1.0 | 2019/11/04 | First Iusse首发 | 曹海翠 | 毛正峰 | 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

The purpose of the Security Manual is to establish a standard security requirement for Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. It is defined in the Corporate Security Policy, by regulatory bodies and customers. This is to provide detailed guideline for the implementation of security procedures across the company on a common standard. This Manual is written with consideration of the local laws and regulations.

本安全手册的目的是建立澄天伟业（宁波）芯片技术有限公司的安全标准。本手册根据标准为安全流程的改进提供了详细的指导。本手册的制定充分考虑到了地方的法律和法规。

This manual defines the security policy, strategies, operating principles and control mechanism used in the premises of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd., located at No.8, Binjiang Road, Cixi High-tech Industrial Development Zone, Ningbo City, Zhejiang Province, P. R. China.

The above security system is to ensure the integrity, availability and confidentiality of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd., Ltd’s manufacturing technology, product information and customer’s proprietary information are upheld. These principles and mechanism also aimed at avoiding any loss of company’s property.

All the information in this security manual of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. (Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. is aligned with the security principles and standard of Corporate and customers security. In case of any discrepancy, all the information is based on the documents of corporate security for any clarification and definition.It is applicable to all staff in Chengtian Weiye (Ningbo) Chip Technology Co., Ltd..

此手册定义了在宁波，澄天伟业（宁波）芯片技术有限公司中使用的安全方针、策略，运行原则以及控制机制。

上述安全系统确保澄天伟业（宁波）芯片技术有限公司的生产技术，产品信息以及客户信息的完整性，有效性和机密性。这些原则和机制的目标是避免公司及客户财产受到任何损失。

此手册中的所有信息都符合澄天伟业（宁波）芯片技术有限公司安全方针和安全标准。

适用于澄天伟业（宁波）芯片技术有限公司的全体员工。

# 2 PROCEDURE程序

# 

# 2.1INTRODUCTION介绍

## 2.1.1 Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. 澄天伟业（宁波）芯片技术有限公司

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd.Located at No.8, Binjiang Road. CTWY Ningbo is a high-tech enterprise with a combination of research, development, manufacturing and sales of smart card chip. It has tape workshop and module packing workshop. Products are widely used in smart phones, electronic devices, banking and public utilities and so on；The areas also used for the manufacture; embedding and personalization of smart cards。 All these are subject to high security requirements. This high security level is necessary to prevent any incidents, which could result from various malicious activities that could take place within the smart card chip manufacturing system.

宁波中天智能卡位于滨江路8号，是一家集智能卡芯片研发、制造、销售于一体的高新技术企业，设有胶带车间和模块包装车间。产品广泛应用于智能手机、电子设备、银行及公用事业等领域；此区域还用于生产，包括智能卡的植入和个人化，所有这些都要求有高安全的管理水平，以能及时预防在芯片的生产过程中可能会出现的严重损毁事故。

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Security Management System (SMS) is based on an assessment of potential risks and appropriate counter measures for the precisely defined risks. It provides a continuous monitoring of the actual effectiveness of the measures and immediate adaptation to the future technical and structural development of the company and to customer's requirements.This document is classified as "Private" and is available to all Chengtian Weiye (Ningbo) Chip Technology Co., Ltd staff members and employees. The Security Manager will determine the Security Classification of this document.

# 澄天伟业（宁波）芯片技术有限公司的安全管理系统是建立在对潜在风险评估以及对已定义风险采取的适当的预防措施的基础上。我们提供了持续的有效监控措施以及即时措施以适应公司未来技术和结构的发展以及客户的要求。此文件被定义为“内部”文件，适用于公司所有的员工。安全经理有权力定义此文件的安全分类

# 2.2 Management Responsibilities管理者责任

**2.2.1 Chengtian Weiye (Ningbo) Chip Technology Co., Ltd.澄天伟业（宁波）芯片技术有限公司**

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. is bound by both international card organizations, national bodies and its customers to provide outstanding security standards in every respect when producing all card products.

澄天伟业（宁波）芯片技术有限公司作为卡类产品制造商，其产品从任何角度皆表现出非常高的安全标准，同时受到国际卡片组织，国内相关组织和其客户的约束。

Security is a continuous “top down” task through current organizational structures and involves everyone within the organization including management to be dedicated in action and behaviour to achieve the desired security level and to share responsibilities for security.

安全一直是一个“自上而下”的任务，贯穿于目前组织结构中，使组织中的每一名职员，包括管理层，都通过各种行为进行努力，以达到期望的安全水准并分担安全责任。

In accordance with the existing Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. security concept, every employee is responsible for complying with, carrying out or implementing all regulations imposed by the legislation, card organizations, customers, insurance companies, and internal instructions. Employees are also responsible for completeness, including the provision of constant records of processes with respect to security sensitive materials. Managers and supervisors bear responsibilities for security in conducting or ensuring that the security regulations are being observed in their area of responsibilities.

根据现有澄天伟业（宁波）芯片技术有限公司安全理念，每名职员都有责任遵守、执行或贯彻所有法律、卡类组织、客户、保险公司和内部命令所施行的规定。同时，他们还对其完整性负责，包括提供连续的敏感材料安全处理记录。经理和各级主管负责在其辖区内实施安全规定，并保证其安全运作。

The Security Department is commissioned by the senior management of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd to verify and ensure that all regulations issued by Chengtian Weiye (Ningbo) Chip Technology Co., Ltd for the purposes of security are adhered to by all employees, and that compliance with regulations is pursued. The aim of the provisions below is to attain an optimum level of security during the production of security sensitive products.

澄天伟业（宁波）芯片技术有限公司的高级管理层委任安全部门负责查证并保证所有职员都严格遵守澄天伟业（宁波）芯片技术有限公司所颁布的安全相关规定，以及致力于遵守该规定。以下条款力求于生产安全敏感产品时达到最佳的安全水准。

The absolute confidence of all customers is of great importance to Chengtian Weiye (Ningbo) Chip Technology Co., Ltd..and for its acceptance by the responsible organizations. Every employee must therefore be dedicated to ensure that all security issues are in compliance and to continuously uphold the assurance levels of all customers and the good reputation of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd..

客户对澄天伟业（宁波）芯片技术有限公司的绝对信任对我们来说非常重要，有助于我们获得相关责任机构的认可。因此，每一位职员必须全力保证所有安全问题符合规定，一直维持向客户所承诺的水准，这同时保持了澄天伟业（宁波）芯片技术有限公司良好的声誉。

Any violation of the security regulations may be regarded as an infringement of the contract of employment and will entitle the company to act on disciplinary or legal actions against the violator(s).

任何违反安全规定的行为将被视为违反雇用合约，公司有权对违反规定者采取处罚措施或法律行动。

### 2.2.2 Security Strategy安全战略

The security strategy of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd.is to identify the high risks that may result from security breaches and loss of company and customers assets and properties. Chengtian Weiye (Ningbo) Chip Technology Co., Ltd., Ltduses its best efforts to implement effective solutions to reduce the identified risk to an acceptable level

澄天伟业（宁波）芯片技术有限公司的安全战略是对所有可能导致安全漏洞以及公司和客户财产和资产受损的高风险进行识别。澄天伟业（宁波）芯片技术有限公司将竭尽全力实施有效的措施将被识别的风险降低到可接受的水平.

## 2.2.3 Management Statement管理概况

The recognition of a comprehensive Security Management System is fundamental to the success of the business of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. in Ningbo Hence the pragmatic and reliable approach is the appointment of a Security Manager to manage the system efficiently.

对安全管理系统充分全面的认识是澄天伟业（宁波）芯片技术有限公司商业运行的基础。因此注重实效和可靠的方法是安全经理有效处理和掌控系统的指定方法。

The Site Security Manager is directly responsible for the implementation of the Security Management System. It shall be in line with the Corporate Security Department’s policy. The Security Management system shall endeavor to include all aspect of the security system. It shall include Personnel Security, Physical Security, Audit Security, Products Security, Information Security and the handling of Sensitive Materials. This is the foundation of the Security System where procedures and documentation to reflect its effectiveness will be formulated for purpose of control and implementation.

安全经理直接负责工厂安全管理系统的执行。同时必须符合公司安全部门的各项方针。安全管理系统应该尽量包含安全体系的所有方面。应该包含人员安全，物理安全，审核安全，产品安全，信息安全和敏感物料的安全处理。安全手册是反映安全程序和相关文件有效性的基础，并以阐明如何控制和执行为目的。

All Administrator in Chengtian Weiye (Ningbo) Chip Technology Co., Ltd are responsible for compliance to the Security Management System. They should seek advice and guidance from the Security Manager the CISO and It&Data Manager and Security Supervisor on issues relating to security interpretation, implementation and adherence to the minimum Security Standard of the Accreditation Authority.

所有澄天伟业（宁波）芯片技术有限公司的管理人员都有责任维护安全管理系统。他们应该就如何进行安全改进和执行等问题从CISO、安全经理、IT&数据经理和安全主管处寻求建议和指导。并且必须忠诚的坚持和贯彻执行已被授权的最低限度的安全标准。

The responsibility for security does not stop with management roles. It is the responsibility of every employee of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd.The protection of the assets and know how of the company are vital to the continuing success of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd, its partners and customers.

安全并不仅仅是管理层的责任。同时也是澄天伟业（宁波）芯片技术有限公司每位员工的责任。保护资产及专有知识对公司及其合作方及客户持续成功至关重要。

Everyone must play their part by observing the requirements of this Security Management System.

There should not be any circumvention or compromise in the implementation and enforcement in whatsoever manner of the Security Manual.

每个人都必须严格遵守本手册，不论手册以什么方式执行，都不得以任何理由或欺骗的手段拒绝本安全手册。

This Security Manual is a guideline to the Security Management System within Chengtian Weiye (Ningbo) Chip Technology Co., Ltd .

此安全手册是澄天伟业（宁波）芯片技术有限公司安全管理体系运行的指导

Our Objectives are:我们的目标是

* to ensure the appropriate level of protection of assets and data belonging to Chengtian Weiye (Ningbo) Chip Technology Co., Ltd., Ltdand its Customers at all times by continuous risks assessments.

确保澄天伟业（宁波）芯片技术有限公司及其客户的资产和数据在持续的风险评估措施下始终处在适当的保护水平下

* to ensure Incident Management and Handling Procedure are in place and that all Incidents must be reported in a timely and proper manner

确保事故管理和处理流程的有效性，并且所有的事故都必须及时的并且有效的得以汇报

* to promote security awareness and culture within the organization such that all employee would consider security as an integral part of daily activities and comply to all internal security policies at all times.

提升安全意识和文化，所有员工应视安全为日常工作中不可或缺的一部分并且一直遵守所有的内部安全流程和方针。

* to conduct continuous monitoring and audits to ensure security compliance and to maintain continuous improvements

实施持续的监控和审核确保安全符合性，并且维护持续的改进

**2.2.4 Management Commitment管理者承诺**

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Management Team recognized our responsibilities to our customer in the production of Smart Card technologies. In this context it has developed the Security Management System (SMS), which is based on five relevant factors

澄天伟业（宁波）芯片技术有限公司管理团队基于以下五方面因素发展完善安全管理系统，以体现我们对客户的责任：

**Confidentiality:** Prevention of unauthorized dissemination of information. Clear classification is done to all relevant documents.

**机密性：** 防止信息的未授权分发。对所有相关文档进行清晰的分级。

**Integrity:** Multilevel control to make sure the data is integrated

**完整性：** 进行多层控制以确保数据的完整性

**Availability:** Customer is accessible to the audit trail document as and when require for purpose of audit.

**效用性：** 当有审核需求时，客户可以访问到审计轨迹文件。

**Non-Technical Security Measures:** Monitoring of the organization personnel appointments and administrative checks is under the charge of Administration Dpt..

**非技术安全措施：** 由行政（综合管理部）负责对组织人员指派进行监控并进行管理性检查

**Physical Security Measures**: Building facilities, Access Control, Sensitive Inventories; Rejected items administration, Data Security, Card Audits is under the charge of Security Department

**物理安全措施**： 建筑物设施，门禁控制，敏感目录，淘汰资产管理，数据安全，卡片审计由安全部负责。

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd management staff and employees are committed and involvement in the SMS will certainly assure our customer of high level of security. In furtherance their anticipation in the development of new security requirements for new products is on going.

澄天伟业（宁波）芯片技术有限公司理层员工和所有员工有义务参与并遵守安全管理系统。以确保我们的客户得到高安全级别的服务。并始终参与对新产品新安全需求的开发。

**2.3.1 Security Organisation安全架构**

In company,Security Director/CISO shall be ultimately responsible for the Security function. He shall delegate the Security Manager to head the function. The Security manager reports functionally to the CISO.

在公司内，最高安全管理者/首席信息安全运营官安全总监/首席信息安全官应该对安全部门负责。他应该委派安全经理负责安全部门，安全经理直接向其汇报。

最高安全管理者/总经理Security Director/GM

首席信息安全官CISO

安全经理

Security Manager

IT经理IT Manager

安全主管

Security Supervisor

安全专员

Security Officer

信息安全专员

Information Security Officer

数据安全专员

Data Security

officer

监控/门禁/报警管理员

CCTV/Acess/Alarm

安全助理（安全体系）

Security System

保安

Security Guards

授权人员

Persons in Authority

生产经理

Production Manager

品质经理

Quality Manager

商务经理

Sales Manager

物流经理

OPP Manager

人力资源经理

H.R Manager

工艺技术经理

Technology Manager

财务经理

Finance Manager

**2.3.2Roles and Responsibilities角色和责任**

### 2.3.2.1Security management system (SMS)team安全管理团队

The SMS team is responsible for defining the Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Security Management System and the related security policies according to the external standards and feedback from the field.

安全管理团队负责定义澄天伟业（宁波）芯片技术有限公司的安全管理以及根据外部标准和领域的反馈而涉及的安全方针

**2.3.2.2 Security Director/CISO安全总监/首席信息安全运营官**

The Security Director/CISO is responsible for ensuring the implementation and continuing compliance of the Security Management System within a specified geographic area. Also, he is responsible for the coporate and customers`s assets and Information Security Management.He reports directly to the General Manager. He will supervise the obtaining and renewal of accreditation issued by regulatory bodies, where necessary providing support to the plants within the region.

安全总监/首席信息安全官负责确保安全管理体系在各个指定区域的有效执行和持续遵守。对公司及客户的财产及信息安全负责，他直接向总经理汇报。他负责监督认证机构需求的获取以及更新，并提供区域内所需的支持。

**Back-up Security Director/CISO安全总监/首席信息安全官替补**

The Back-up Security Director/CISOis qualified and empowered to act upon critical security events in the event the CISO is not available.When the CISO backup is functioning on behalf of the CISO, the backup must not perform activities for which they have approval responsibility and must not approve activities which they previously performed.

如果CISO不在时，替补人员有资格及授权处理紧急安全事件。当CISO的替补代替CISO履行职能时，替补人员不能执行他们有批准权限的活动，且不能批准他们之前执行的活动

* **2.3.2.3Security Manager安全经理**

The Security Manager is responsible for ensuring the establishment and application of the local security operating procedures in compliance with the Company Security Policy，external applicable standards and local laws.He reports directly to the Security Director/CISO and functionally to the General Manger in this geographical site.

安全经理负责确保安全操作流程的建立和运用，并与公司安全政策、外部标准和本地法律相一致。他直接向安全总监/首席信息安全官汇报，并且平行汇报总经理。

He is responsible for the development, implementation and documentation of the Company Security Management System. He is also responsible for the management of Security personnel and the monitoring their effectiveness. He shall examines, monitors and documents all corrective and preventive measures which are to be applied following the discovery of any gaps or in the event of any necessary adaptation of procedures following changes within the company. He shall disseminate the General Security Procedure and Regulation to existing and new employee of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. It shall include visitors, registered employees of outside companies and any other persons temporarily present within the building.

安全经理主要负责公司安全管理系统的实施，开发和文档化，以及人员安全的管理和监控他们的效率。他还应该负责根据所发现的缺陷及公司内部流程变化所进行的调整对纠正及预防措施进行跟踪，监控并记录。他应该负责向全体澄天伟业（宁波）芯片技术有限公司员工及新员工宣传通用的安全流程和规章，包括访客，外包员工或者任何在公司内工作的临时员。

* **2.3.3.4 IT Manager IT经理**

The IT Manager is responsible for ensuring the establishment and application of the logical securityoperating procedures in compliance with the Company Security Policy，external applicable standards and local laws.He reports directly to Security Director/CISO

The IT Manager is responsible for the implementation, development and documentation of the Company Security Management System. He is also responsible for the management of IT&Data personnel . He shall examines ,monitors and documents all corrective and preventive measures which are to be applied following the discovery of any gaps or in the event of any necessary adaption of Procedure and Regulation to existing and new employee of company.

IT经理负责确保网络及数据安全流程的建立和运用，并与公司安全政策、外部标准和本地法律相一致。他直接向安全总监/首席信息安全官汇报，并且平行汇报总经理

IT经理主要负责逻辑安全管理系统的实施，开发和文档化，还有网络及数据人员的管理及根据发现的缺陷及公司的内部流程变化所进行的调整及对纠正及预防措施的跟踪，监控并记录并向全体澄天伟业（宁波）芯片技术有限公司员工及新员工宣传通用的信息安全流程和规章。

**2.3.3.5 Security Supervisor & Security Officer安全主管和安全专员**

**2.3.3.5.1 Security Supervisor 安全主管**

The responsibility of Security Supervisor is to secure and monitor Chengtian Weiye (Ningbo) Chip Technology Co., Ltd properties, products, assets, and personnel. In order to effectively fulfilling these responsibilities they are provided by the management the following equipments such as CCTV surveillance, video recording, alarm systems, card access control systems, and communications systems . The Security Supervisor has the administrator access. The other aspect of control is the security instructions, security procedures and security reports and forms that regulate their area of work.

The Security Supervisor report directly to the Security Manager.

安全主管的责任是保护和监控澄天伟业（宁波）芯片技术有限公司的财产、产品、资产以及人员的安全。为了有效的满足这些责任，管理层提供了以下设备，如CCTV监控系统，录像记录系统，报警系统，门禁控制系统以及沟通系统等，安全主管有这些系统的管理权限。其他方面的控制措施是与之工作相关的安全引导，安全流程，安全报告以及安全表格等。安全主管直接向安全经理汇报。

**2.3.3.5.2 Security Officer安全专员**

The Security Officer assist the Security Supervisor with Security work . The Security Officer is responsible for the daily specific Security work such as the management of badge and so on. Meanwhile , the Security Officer has the Operation access and should report the exceptions of system to Security Manager.

安全专员辅助安全主管的工作，主要负责安全具体的日常工作，像门禁卡的管理等。对CCTV监控系统，录像记录系统，报警系统，门禁控制系统以及沟通系统等有操作权限，并负责像安全经理汇报系统的异常情况。

* **2.3.3.6** **Information Security Officer & Data Security Officer信息安全专员和数据安全专员**

**2.3.3.6.1** **Information Security Officer信息安全专员**

Information Security Officer is responsible for Company`s network and information security ,The other aspect of control is the IT security instructions, procedures ,reports and forms that regulate their area of work. The Information Security Officer reports to IT Manager directly.

信息安全专员和数据安全专员负责公司信息和数据安全，还有他们工作范围内的信息和数据的安全说明/程序/记录，他们直接向IT经理汇报。

* **2.3.3.6.2 Data Security Officer数据安全专员**
* Data Security Officer is responsible for Company`s data security ,The other aspect of control is the Data security instructions, procedures ,reports and forms that regulate their area of work.they report to IT Manager directly
* 数据安全专员负责公司的数据安全，还有他们工作范围内的数据的安全说明/程序/记录，他们直接向IT经理汇报。

**2.3.3.7 The Manager of Department部门经理**

The departmental manager is empowered to develop Security Procedures and Security measures that are deem to be relevant to their operational requirement. It shall be implemented with due consultation of the site Security Manager. The department concern shall be responsible for the implementation of such procedure. They shall inform the Security Manager of any deviation in the application or results in the implementation.

部门经理被授权改进完善与操作需求相关的安全流程和安全措施。并在咨询安全经理后进行实施。部门应该充分关心这样的安全程序是否被有效的执行。执行过程中任何违反安全规则的行为都应该通知安全经理。

**2.3.3.8 The Security Guards 保安人员**

The guards’main role is to ensure permanent (at a minimum, during working hours) control of the security systems and maintain a high level of protection of the building, assets, access and staff, Must immediately reporting any discrepancy to the security officer.

保安的主要职责是确保对安全系统的长期稳定性（至少在工作时间内）进行控制，并对建筑物，资产，访客和工作人员保持高度的保护，如有任何差异必须立即向安全员汇报。

**2.3.3.8 The Members of the Management管理成员**

The departmental head plays an active and important role in the enforcement and support of the Security Management System within their respective department. In particular they shall ensure that the subordinates are aware of the security policy and procedure and that it is their obligations to support the security management system.

在他们各自负责的部门中，管理人员应在推行和支持安全管理系统的方面扮演积极的角色。特别是他们应该确保他们的下属了解安全政策和程序，并了解支持安全管理系统是他们责任的一部分。

**2.3.3.9 All Other** **Persons in Authority其他被授权的员工**

They assist the Security Department in the monitoring of the procedure and rules introduced within their working area. They participate in the integration of Security rules in all industrial and administrative processes and monitor their effectiveness and are responsible for the application.

他们负责协助安全部门监控各自工作区域内的流程以及规则。他们参与所有工作和管理流程中安全规则的完整性并监控其有效性，并对其有效性负责。

### 2.3.3.10 Direct and Indirect Employees 直接和间接员工

They have committed themselves with their signature to observe the security rules explained to them upon employment by Chengtian Weiye (Ningbo) Chip Technology Co., Ltd.

They are obligated henceforth to inform the security department or their supervisors of any problem or any observation in relation to the breach to security.

They are directly responsible for the protection of the products, which they are entrusted with in the course of their work regardless of whatever stage of production.

他们必须忠于他们的承诺，严格遵守澄天伟业（宁波）芯片技术有限公司的安全政策。

他们有义务在今后的工作中向安全部门或者他们的主管汇报他们发现或看见的任何违背安全规定的行为。无论处于生产的什么阶段，他们对本工作内被托付的产品进行保护并负有直接的责任。

## 2.4 Risk Analysis风险评估

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd uses Risk Analysis as a tool for Risk Management to protect its clients, their employees and their service providers against principal risks concerning personnel security, product security, material security and information security. The Risk Analysis uses a systematic and measurable approach to identify and priotise critical assets that the company needs to protect.This risk analysis is in place and reviewed periodically (at least once a year) or when a change control is introduced in the environment subject to security impacts on the site.

澄天伟业（宁波）芯片技术有限公司使用风险评估作为风险管理的工具保护客户、员工以及服务提供商，防备涉及人员安全、产品安全、材料安全以及信息安全的主要风险、风险分析采用系统以及可测量的方式识别和确定公司需要保护的主要资源。此风险评估必须定期更新（至少一年一次），若有任何对安全影响的改变控制都应该进行更新。

## Business Continuity Planning可持续性业务发展计划

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd has developed a Business Continuity Plan to maintain appropriate recovery plans for critical business processes and services. This plan is necessary to ensure that critical business activities are restored and maintained as quickly as possible following any major disaster or failure that could affect essential services or facilities. This plan caters for Cards Manufacturing and its related IT Operations.

澄天伟业（宁波）芯片技术有限公司已实行可持续性业务发展计划以维护重要的商务流程以及服务的恢复。此计划对确保主要商务活动在经历重大灾难后的快速恢复是非常重要的。此计划适用于卡片的生产以及相关的IT操作。

The business continuity planning involves identifying and reducing the risks from deliberate or accidental threats to vital Chengtian Weiye (Ningbo) Chip Technology Co., Ltd services. The business continuity planning process covers:

可持续性商业发展计划涉及识别和减少蓄意破坏和事故对澄天伟业（宁波）芯片技术有限公司服务造成的危害。可持续性商业发展计划涉及

1. Initiation of BCP framework and deployment

建立BCP架构和部署

1. Critical assets identification and Control

主要资产的识别和控制

1. Emergency Response and Operations

应急响应和运作

1. Developing and Implementing Business Continuity Plans

发展和实施可持续性发展计划

1. Awareness and Training Plans

意识和培训计划

### 2.5.1 Emergency Evacuation & Recovery紧急撤离和恢复

It is important to note that although personnel safety is our priority in dealing with emergency situations, necessary measures are still necessary in order to minimise the security threats that may arise as a result of such emergency.

我们必须认识到尽管人员安全在紧急撤离的情况下是首要考虑因素,但是必要的措施对于减少安全风险也是非常重要的

* Before the site is evacuated, if possible, the personnel shall lock all products and save information in the habitual storage places, or in temporary storage places.

在撤离公司之前，如果可能的话，相关人员应该将所有产品上锁、信息储存并存放在固定或临时区域。

* At the end of the warning, the personnel will return to the site in order to finish up the protection of the information and products.

在结束报警后，人员应返回工厂并完成对产品和信息的保护

* The site security official will ensure that all the personnel have returned to the site before the access control system is reinitialised.

公司安全管理人员应该确保在门禁系统重置之前，所有员工已经返回厂区

* Checking the quantity in line - When returning to the work location, operators at each station are required to check the quantities of raw materials (such as blank cards, modules), work-in-progress finished cards and leftover rejected cards in their corresponding location.

检查产线上产品的数量：当回到工作区域时，操作工应检查原料的数量（如白卡、模块），在相应区域的在制品，成品卡以及遗留的坏卡也都应该清点数量

* In case of discrepancy, they are required to report to the production supervisor. The production can only be resumed when the quantities at each station are verified and correct.

如果遇到数量差异，他们应该立即汇报给生产主管。在数量被确认正确后，方能重新开始生产

* Checking the machine status - Operators are required to check the status of the machines and ensure all the conditions / parameters setting of the equipment are resumed before the re-start of production. This is to ensure no duplicate cards would be made.

检查设备状态：操作工应该检查设备的状态并且确认设备所有的条件和参数在生产恢复之前都已恢复正常。必须保证不得生产出重卡

* An evacuation checklist will be filled after each evacuation.

每次撤离后，都必须填写撤离检查表。

## 2.6 Incident management事故管理

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd‘s incident handling and reporting procedure is based on Company Standard (See Reference below) to ensure incidents do not cause unnecessary damage to any part, the people, customer and Chengtian Weiye (Ningbo) Chip Technology Co., Ltd property, data and knowledge and the reputation of the company.

澄天伟业（宁波）芯片技术有限公司的事故处理和响应程序建立在公司标准上以确保事故不会对任何部分造成不必要的损失，包括人员、客户、以及公司财产、数据、知识产权以及公司名誉。

Whenever an incident (fire, bomb warning, etc.) requires an evacuation of the site, steps will be taken to ensure:

不论何种需要撤离的事故（火灾、爆炸危险等等），都将采取如下步骤

- the protection of products and information;

产品和信息的保护

- the restarting of the site under satisfactory security conditions.

在安全条件已经达标的情况下恢复生产

Having given such consideration the following assessment must be carried out:

如下评估必须被执行

* Incident identification and evaluation

事故识别以及评估

* Incident notification

事故通知

* Incident response

事故响应

* Incident handling

事故处理

* Activate BCP in case of prolonged disruptions to operations

如遭到持续的破坏，启动业务可持续性发展计划

* Incident reporting and closure

事故报告和关闭

### 2.6.1 Theft / loss of sensitive assets敏感资产的偷盗和丢失

Lost / Theft of sensitive assets/component, data/product classified under restricted/confidential/class 1 require to be reported to the relevant authorities immediately & follow-up by written notification within 4 hours. Relevant Authorities are for example: Customers, security Departmentand Law enforcement

敏感资产的丢失以及偷盗包括1类资产、机密、保密的产品和数据，此种情况应该立即在4小时之内跟踪并书面通知。通知的相关人员包括客户、安全部门以及法律部门。

**2.6.2The unknown incidents未知的安全事故发生**

Once the unknown incidents or undescibed incidents happened, report to the Security Manager and relative stuff immediately and BCP documents should be updated after the issues solved.

一旦发生未知或文件中未描述的安全事故，立即汇报安全经理及相关人员处理，并在该事故处理完毕后，更新BCP并进行安全风险评估。

**2.7 Security Document** Classification**安全文档和分类**

Security Documents supporting the Security Management System were developed following the evaluation of possible external and internal risks. These risk factors could endanger the manufacture, storage, shipment and reception of smart cards or related materials. The risks defined enable the management to the establishment a list of appropriate counter measures, which are intended to assure security survival. These measures are classified according to areas of application in the prevention and/or reduce the risk to negligible level.

The classification of documents and data is of major importance in establishing secure mechanisms for the efficient and secure operation of the company.

支持安全管理系统的安全文档基于可能的内部和外部风险评估的基础上建立。这些风险因素可能导致生产、储存、物流、智能卡的接收及相关物料出现问题。这些风险的详细描述促使管理层建立确保安全运行的适当的对策列表。这些措施按照应用范围是预防还是降低风险级别进行分类。

文档和数据的分类对建立安全机制以确保公司有效安全的运行是非常重要的

**2.8 Arrangement of Security Documentation安全文件的排列**

2.8.1 All necessary documentation on the SMS is arranged in a pyramid structure:

所有安全管理系统中的重要文件都是按照金字塔的方式排列



**1 、Security Manual(SM)**: This is the security manual developed by S Chengtian Weiye (Ningbo) Chip Technology Co., Ltd site.

安全手册：澄天伟业（宁波）芯片技术有限公司编制此安全手册。

**2 、Security Procedures(SP)**: These are the security procedures, which define the operation of

the security equipment and methods of working.

安全程序：这些安全程序详细定义了安全设备和安全工作方法。

**3 、Security Work Instruction** These are the general security instruction, which define the

**(SWI)**: work process.

安全操作指导书：这些是安全指导书的综述，详细定义了工作流程。

**4 、Security Data\ Parameters**: These are specification on the working process

安全参数：这些是对工作流程的规范说明

**5 、Security Records(SR):** These are documentation record reflecting the working process

安全记录：这些是反映工作流程的文件记录

These are documents that form the core of the SMS. These documents are subjected to classification in accordance to company Security Procedure on the topic of Classified Documents.

这些文件是安全管理系统的核心。这些文件根据公司安全程序中保密文件的主题，进行了等级的分类。

### 2.8.2 Classification of Document and Data文档和数据的分类

The classification scheme in Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. adopts the scheme fromCompany Standard.

澄天伟业（宁波）芯片技术有限公司的文档分类标准完全符合公司的标准。

The classification-labeling scheme includes four categories, from highest to lowest:

分类标签共分为4级，从最高级到最低级。

* **Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Secret** (e.g. secret algorithm) – unauthorized disclosure would cause catastrophic damage to the interests of the company

澄天伟业（宁波）芯片技术有限公司绝密-未授权的泄漏会对公司利益造成灾难性的损毁

* **Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Confidential** (e.g. customer data) – unauthorized disclosure would be highly prejudicial to the interest of the company

澄天伟业（宁波）芯片技术有限公司管制（如客户数据）-未授权的泄漏会对公司利益造成高度不利的损毁

* **Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. Private (e.g. internal e-mails)** - disclosure could affect the company business
* 澄天伟业（宁波）芯片技术有限公司内部（如内部邮件）-如果泄漏可能会影响公司业务

**Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Public** (e.g. marketing brochures) – information that can be available to customers, partners or third-parties.

澄天伟业（宁波）芯片技术有限公司公开信息（如市场手册）-信息可以对客户、搭档以及第三方公开

**2.9 Personnel Security人员安全**

The employment of staff policy in Ningbo aligns with the company policy

宁波雇员方针，符合公司方针

### 2.9.1 General Policy通用方针

All Chengtian Weiye (Ningbo) Chip Technology Co., Ltd employees must comply with the Ningbo laws.

所有澄天伟业（宁波）芯片技术有限公司的员工必须符合宁波的法律法规

A conviction for an offence against the criminal penal code of Ningbo must be divulged before employment

is offered to an individual. Human Resources departments are responsible for maintaining this standard.

在将雇佣合同给到个人之前，必须提供无犯罪证明。人事部门负责维护这项标准。

The Chengtian Weiye (Ningbo) Chip Technology Co., Ltd «General Security Procedures » must be communicated to all Chengtian Weiye (Ningbo) Chip Technology Co., Ltd employees.

澄天伟业（宁波）芯片技术有限公司《安全程序和规章概要》传达到所有澄天伟业（宁波）芯片技术有限公司员工。

Where an employee’s function with the company changes, the security status of the employee must be

reviewed and, where appropriate, amended to take account of the new function. The review will be

undertaken by the Security Manager on advice from the Human Resources Department or the new Line

Manager responsible for the employee.

当员工转换部门时，该员工在新岗位上的安全状态必须被考虑和审核。该审核应由安全经理在人事部门或者其

直线经理的建议下进行。

Any employment of sub-contractors will not be undertaken unless they agree to abide by the rules and

regulations to which regular employees are subject, as outlined above. Sub-contractors must be aware that

any breach of the security regulations through a deliberate act or omission will result in a requirement to

immediately leave the work site. Subcontractors must sign a confidentiality agreement.

承包商只有在完全同意遵守公司规程的情况下，方能开始工作。承包商必须认识到，任何违背安全规程的行

为，都将被立即驱逐出公司。承包商必须签订保密协议。

All Chengtian Weiye (Ningbo) Chip Technology Co., Ltd employees will take all reasonable measures to ensure thesecurity of company premises, procedures, products and knowledge. They will remain alert to and report any suspicious activity that could compromise the company security. This report should be made to their line manager or to a member of the local or central security team.

所有的澄天伟业（宁波）芯片技术有限公司员工应该采取合理的措施以保证公司、流程、产品和知识产权的安全。员工应该时刻保持警惕，遇到任何与公司安全要求相违背的可疑情况应该立即向直线经理或者本地安全团队汇报。

All Chengtian Weiye (Ningbo) Chip Technology Co., Ltd employess will take all reasonable measures to Report any weaknesses in systems, procedures and controls to the Security Department so that improvements can be made. These reports can be done via direct verbal communication or via email.

所有澄天伟业（宁波）芯片技术有限公司员工应采取合理的措施向安全部门汇报系统、流程和控制措施的弱点已取得改进。员工可以通过直接的交流和邮件进行汇报。

### 2.9.2 Recruitment of new employees新员工培训

The Human Resources Department maintains within its recruitment policy and practices the following standards relating to recruitment of new employees. These standards comprise the following pre-employment checks which must be conducted:

人事部门应该根据以下新员工录用标准维护招聘政策和实践。这些标准必须包含以下录用前的检查。

a) A copy of their identification card is provided for newly engaged employees. This

assures that no relevant entries in terms of criminal law are given.

每位新进员工都必须提供其身份证复印件。这能确保此人不涉及相关刑事案件。

b) An employee background check report ( Credit or bankruptcy Checks, Past Employment and Education) must also be conducted by an external appointed entity for sensitive position.

对于敏感职位的员工，必须由制定的第三方进行背景调查（信用或者破产调查，过去雇主以及教育的调查）

c) A document to observe all control and security regulations and maintain confidentiality and

a data protection declaration "Secrecy Agreement" and/or “Code of Ethics” is to be signed by each new employee.

每位员工都必须签订“保密协议”。保密协议的内容包括控制和安全规章以及机密性的维护和

数据的保护。

d) Notify GSMA and Banking or any other relevant authorities (if required) immediately of any personnel changes that directly affect the security of GSM’s products and bank cards or other Security Branded Cards.

若人员的变动对GSM卡和银行及其他有安全标示的产品有直接的影响，应该立即通知GSMA和银行以及相关的组织

### 2.9.3 On departure from company离开公司

An inventory of the information that person holds will be drawn up by the department head. Security Personnel will ensure card access is deactivated within 24 business hours of the departure of the employee. Any anomaly observed will lead to a request for explanation and a momentary stoppage of the departure operations.

部门经理必须回收该员工所持有的所有物品。安全人员应确保该员工的权限在离开公司24小时之内被删除。任何观察到的异常都应该获得解释，并强制其停止离开行为。

### 2.9.4 Temporary personnel临时员工

Recourse to temporary personnel is prohibited on the development premises. It is tolerated for office jobs if the information processed there, or passing through it, is not confidential; the same applies during production.

在发展的前提下，依赖临时员工的行为时被严格禁止的。在信息已经处理并且不是机密的情况下，办公室的工作和后勤部的工作是可以允许让临时工操作的

Any temporary personnel used in Sensitive areas will require the same background checks as Permanent StaffTemporary personnel are monitored and managed by the personnel department.

任何临时工，若涉及到机密区域则必须与正式员工一样，进行背景调查。临时员工的行为受到人事部的监控和管理

### 2.9.5 Visitors访客

* A Visit authorization request is to be made prior to a visit by the Chengtian Weiye (Ningbo) Chip Technology Co., Ltd host and approved by the department manager and Security Manager.

授权访客在到澄天伟业（宁波）芯片技术有限公司访问之前，必须提前获得安全经理的批准

* As a consequence of being allowed to visit the site, before the visit starts, visitors must read and sign a Confidentiality Agreement.

在访问开始前，访客必须阅读和签署保密协议

* Visitor’s identity must be recorded before entering the premises. Their in/out records are maintained.

访客的身份信息在进入之前，必须被记录。并且维护其进出记录

* All visitors are given visitor cards before they enter the premises. Inside the premises, they need to clearly display his/her visitor cards. The visitor cards are to be returned before leaving the premises.

在进入公司之前，所有访客都被发放访客证。在公司里，访客必须时刻将访客卡佩戴在可见位置，离开公司后，归还访客卡。

* No visitors are allowed to enter the production areas without prior approval. Visitors are not allowed to take photographs and video in the premises without pre-authorisation from the Security Manager.

任何访客在未获得批准之前，不得进入生产区域。在未获得安全经理的授权下，任何访客不得在公司拍照和摄影。

### 2.9.6 Security Awareness and Training安全意识和培训

For security to be successful and effective, Department management on down to the rest of the staff need to be fully aware of the importance of enterprise and information security. All employees should understand

the underlying significance of security and the specific security-related requirements expected of them. Chengtian Weiye (Ningbo) Chip Technology Co., Ltd understands these principles and strive to ensure all our employees understood the importance of security and company’s policies on security.

为了确保安全的成功和有效性，部门经理和其部门下的其他员工都必须完全意识到公司和信息安全的重要性。所有员工应该明白安全的意义和对其期望的相关安全要求。澄天伟业（宁波）芯片技术有限公司确保所有员工理解和明白安全的重要性和安全方针的重要性

#### 2.9.6.1 Security Training Plan安全培训计划

In order to be more effective in managing security training, a training plan is established for various types of training such as orientation training, periodic awareness training and specialized training.

为了更加有效的掌控安全培训，必须为各式各样的培训如入职培训、定期意识培训以及特殊培训建立培训计划。

#### 2.9.6.2 Orientation Training入职培训

This type of training is for new staff and provide basic security policies and requirements to new staff.

此培训适用于新员工，内容涉及基本安全方针以及新员工需要知道的要求

#### 2.9.6.3 Awareness Training意识培训

This type of training are usually done periodically to remind existing staff on security rules, policies, recent incidents or new threats. The format of the training can be in a format of presentations, videos or email articles

此培训用于定期提醒在职员工安全规章制度，事故分享。此培训的形式可以是演讲、录像以及邮件的任何

方式

#### 2.9.6.4 Specialised Training特殊培训

This type of training is targeted towards technical oriented staff who needs to have more in-depth or specific security knowledge in their jobs such as software/product development and IT administration.

此种形式的培训适用于技术员工，在他们的工作中，需要对安全知识有更深层次的要求，如软件/生产开发

人员和IT管理人员。

## 2.10 Insurance Policy保险方针

Chengtian Weiye (Ningbo) Chip Technology Co., Ltd seeks to protect and preserve both its tangible and intangible assets from any loss or damage that could materially affect its ability to discharge its responsibilities to its customers, employees, shareholders, and the communities in which it operates. Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Insurance is managed on a company level and engages in risk management and has retained insurance coverage to:

澄天伟业（宁波）芯片技术有限公司力求保护丢失和损毁的无形和有形资产，这些丢失和损毁的资产影响了公司对客户、员工、股东以及社团责任的行使。澄天伟业（宁波）芯片技术有限公司的保险是在公司水平和对风险控制的基础上掌控的。并且保险覆盖

* Identify and assess the risks to which Chengtian Weiye (Ningbo) Chip Technology Co., Ltd is exposed

识别和评估澄天伟业（宁波）芯片技术有限公司现有的风险

* Select and implement cost-effective risk control measures to avoid or reduce the exposures to loss

选择和实施符合成本效益的风险控制措施以避免或者减少丢失的风险

* Arrange appropriate risk financing (including, but not limited to insurance) to offset the effects of any losses that may occur, so that the lowest sustainable cost of risk is obtained over the long term

Monitor and continuously improve the execution of the risk management process for all Chengtian Weiye (Ningbo) Chip Technology Co., Ltd assets, including buildings, equipment, data and products.

安排适当的风险融资（包括但是不仅仅包括保险）以抵消丢失所带来的影响，用最低限度的可以承受的风险成本获得长期的对澄天伟业（宁波）芯片技术有限公司的资产包括建筑、设备、数据以及产品的风险管理流程的执行进行监控和持续改进

**2.11 Contract Examination合同审查**

The contract department shall examine matter in connection with security requirement, before a new contract is signed with a customer.

在与客户签订新的合同之前，合同部门必须根据安全要求对合同进行审查。

Each New Contract is examined for:

每一个新的合同都必须经过如下审查

1) Conformity between the customer's security requirements and those of the Chengtian Weiye (Ningbo) Chip Technology Co., Ltd SMS (Including documentation).

同时符合客户的安全要求和澄天伟业（宁波）芯片技术有限公司的安全要求（包括文件）

2) Additional requirements (in the case of amendment to or extension of a contract).

附加要求（在合同修订或者扩展的情况下）

3) Fulfill ability of the contract requirements.

完全遵守合同约定的要求

## 2.12 Management Review管理评审

The Management Review Meetings are conducted periodically (at least once a year) to monitor security management process andto ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement

管理评审会议应该定期召开（至少每年一次），监控安全管理流程并确保其连续的是适配性，适当和有效性。此评审应该包括改进评估

The management reviews meetings include:管理评审会议应该包括

* Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Performance Review from top management down to specific department and down to Team Rewarding System of the operators.

澄天伟业（宁波）芯片技术有限公司从最高经理到部门经理以及关于系统操作员的业绩评审

* Any security breach is a killing factor for the Team Rewarding System programmed.

任何的安全违规行为

* Monthly operation reviews with action follow up defined.

月度整改行动的评审

* Risks review

风险评审

* Risk Treatment Plan

风险处理计划

* Corrective actions from internal and external audits,

内部、外部审核的整改行动

* Follow up of incidents and claims,

跟踪事故和投诉

* Changes that could affect the security management system,

可能对安全管理系统造成影响的改变

* Check relevance of the Updates

审核更新

Preventive and corrective actions with the associated resources are established and new security objectives validated. Conclusions and decisions from these reviews are documented and records shall be maintained. Actions plan with description, owners and time-line should also be included.

建立与资源相关的预防纠正措施和新的安全目标。任何通过该评审得到的结论和决定都必须形成记录。并且应该包括行动计划、行动负责人以及计划完成时间。

**2.13 Physical Security物理安全**

Physical Security is managed in accordance with the definitions set out in the Company Security

Policy and is managed in accordance with the company Directive.

物理安全必须符合公司的安全政策和公司相关指导。

**2.13.1 Security Zones 安全区域**

The zones are divided into five levels for purpose of security implemented. They are the High security Zone, Security Zone,Security control center,Security Control Center server room and Control Zone. The five zones are separated by partition such as fences, walls and doors. They are in turn protected by an integrated access control and alarm system. These systems are supported by a video surveillance and recording devices. The following security area range from highest to lowest according to their security level.

为了贯彻安全，整个区域被划分成了5个水平的区域。分别是高安全区、安全区、监控室、监控室服务器机房、控制区。这五个区域被栏杆，墙以及门等划分开，他们依次处于门禁控制和报警系统的保护下；这些系统都在录象监督和记录的监控下。以下区域安全级别由高到低排列。

**High security Zone: Data generation server room(IT Room) and SCC server room/Vault/shredder room.** **高安全区：数据处理及服务器机房，监控室机房，碎卡室，金库**

Dual control access is implemented in High Security Zones which means only two different personnel can have access to open the door at by swiping the sensor. If visitors and unauthorized personnel have to go into the High Security Zones, approval/escort/registration are necessary Besides,anti-back, motion detector, Open Door Time-lapse Alarm and full coverage of CCTV are also implemented in High Security Zone

在高安全区域实行门禁双控，进入这些区域必须要求不同的两人分别刷卡进入，门禁反潜控制；访客和非授权人员进入要批准和陪同，进入要登记；移动侦测报警、延迟关门报警、CCTV全覆盖。

**Security Control Center  监控室：**

It is managed and controlled by a Duty Security Officers on a 24-hour coverage basis and seven days a week shift system inside the Security Control Center. (SCC).Also ,anti-back function is working.if visitors and unauthorizide personnel have to go into SCC, Approval /escort/registration is nessarary.if Nobody in SCC or the personnel on duty fell in sleep , than it will trigger CCTV alarm .Besides ,Open Door Time-lapse Alarm and emergency duress button are implemented in SCC.

在监控室内实行安全专员（保安员）24小时 X 7天的系统监控，门禁反潜控制；访客和非授权人员进入要批准和陪同，进入要登记；无人（睡觉）15分钟自动报警、延迟关门报警、紧急胁迫按钮。

**Security Zone : security IC encapsulation production area /material warehouse/shipping area/IC office/IC changing room/IC meeting room安全区：模块封装车间、、物料仓库、货物通道、IC办公室，IC更衣室，IC会议室。**

One personnel can swipe into Security Zone,but man-trap is necessary. And all doors are set anti-back function, including man-trap door. Also ,if visitors and unauthorizde personnel have to go into the Security Zones ,approval/escort is necessary.Besides, motion detector/Open Door Time-lapse Alarm and full coverage of CCTV are also implemented in Security Zone. Shipping area implement inter-lock/ emergency duress button and visual intercom.

在安全区实行单人刷卡进入，进入该区域必须单人刷卡通过单人通道依次进入，门禁反潜控制；访客和非授权人员进入要批准和陪同，移动侦测报警、延迟关门报警、CCTV全覆盖。

货物通道实行门禁互锁、紧急按钮、可视对讲。

**Control Zone : production office / changing room/toilet/hallway 控制区：SIM卡生产办公室、更衣室、卫生间、走道等**

Enter into Control zones need to swipe access card. And the doors are implemented anti-back function. if visitors and unauthorized personnel have to go into the Security Zones ,approval/escort is necessary.Besides, Open Door Time-lapse Alarm and full coverage of CCTV are working all the time.进入控制区需要刷卡进入，门禁反潜控制；访客和非授权人员进入要批准和陪同，延迟关门报警、CCTV全覆盖。

**2.13.2 Access to the Building进入办公楼的权限**

Access inside the building is further controlled by the access control system. There are a number of zones within the building. The security manager maintains a matrix which defines these zones andwho has access to them. Everyone can access the area only after getting approval from both local department and security department

进入办公楼后，将会有进一步的门禁控制系统。在办公楼里有很多区域，安全经理必须根据这些区域以及相应拥有这些区域权限的人编制矩阵表，并定期更新。只有获得本部门和安全部门的批准后方能访问办公区域

**2.13.4 EXCEPTIONS免责条款**

In exceptional circumstance, there may be a need to bypass certain physical access constraints in order to facilitate movement of people or material example in a case of a sudden emergency or to facilitate movement of large equipment or materials.

In such a circumstance, the requestor will require to make a written application stating the reason and duration of the exception. Approval required by management or the Security Manager for such request. In cases of emergency, this request can be verbal and also taken independently by the Site Security Manager in attempt to preserve life.

For equipment and material move, depending on the duration, additional Guards Service may be used to provide checks at the point of entry/exit. At other times, specific time-based access may be given and certain bypassed made to the system. However, this would only be to facilitate the actual movement and to be disabled once it is completed.

在特殊情况下，为了方便人员或者大型物料的进出，会取消特定的物理门禁约束，如在紧急逃生的情况下。在这种情况下，申请者必须提出书面申请，并注明使用原因和使用的期限，并获得管理层和安全经理的批准。在紧急情况下，可以提起口头申请，并且由安全经理独立掌控以确保生命安全。

对于设备和材料的移动，取决于使用期限，保安必须全程陪同。其他时间，可以在系统中设置特定的进出时间。然后，这仅限于方便实际的移动并且在使用结束后，应该立即关闭。

**2.13.5 Staff Access员工权限**

Departmental managers or the HR department authorizes the access into the building for employee according to the specific area of work. The Security Manager verifies this before access into the area is granted. An Access Status Application forms record the request for employee’s extension of his / her access right according to the job enlargement status. Access may be granted for particular areas, by time periods and for particular days of the week. Security officer is responsible for granting the access rights to employees, and department manager is responsible for quarterly review to their employees’ access rights

根据区域和工作的不同，部门经理或者人事经理授权员工可以进入的区域。安全经理负责查验他们在进入这些区域之前，是否得到批准。由于扩大工作范围而需要进行权限变更的，必须根据其工作范围填写权限变更申请表并记录。权限的授权可以根据特殊区域，时间限制以及一个星期内的某些天数来进行设置。安全人员负责根据权限申请对员工权限进行授权，并由部门经理对所属部门员工的权限进行季度审核

**2.13.6 Visitor Access访客进入**

The Host Dept must submit the Notification of Visitor to security manager prior to the visitor. The visit is subjected to approval by the relevant authority. The visitors should be escorted by host department at all time during visit.NDA is needed for all visitors before any access to security area and high security area.

在访客到达之前，接待部门必须向安全经理提交访客信息，访问必须得到相关授权并且由接待部门全程陪同。所有进入安全及高安全区域参观的人员必须签署保密协议。

**2.13.7 Sub contractor Access承包商的权限**

Sub contractor can access the office area only after they got proper approval, the access rights can maximal granted by months. Sub-contractors seeking access to work in the facility is subjected approval by the relevant authority.

承包商只有获得相应的批准后方可访问办公区域，访问权限不超过一年。承包商在工作时的权限是必须有相关授权的。访问前必须签署保密协议。

## 2.13.8 Vehicular Access车辆权限

Security Dept. must make available a vehicle authorization list to Security Control Center (SCC). VIP may enter by the Main Gate upon approval with prior notification. The Security Officer controls the vehicles access to the facility. All commercial vehicles shall report to SCC to process their access into the facility.

安全部门负责向监控中心提供车辆进入授权名单。VIP车辆在获得提前授权的情况下，可以直接进入。安全专员负责控制车辆进入的设备。其他任何商务车辆在进入之前，都必须报告安全监控中心，并完成车辆进入流程。

**2.13.9 Alarm and CCTV Operation报警和CCTV的操作**

The site is further protected from unauthorized entry by an alarm system and a CCTV monitoring system. Actions to take in the event of an alarm being activated are covered in the security officers’ instruction manual and are logged both within the system and in the occurrence log maintained in the Security Control Center.

报警系统和CCTV系统能够在有未授权人员进入公司的时候，起到保护作用。报警系统报警后，所有报警记录必须记录。

**2.13.10 System Maintenance系统维护**

Maintenance of the Access Control System, the Alarm System and the CCTV system is by contract on a call out basis and through monthly maintenance contract. Contractor will provide a comprehensive report regarding any intervention requirement.

门禁系统的维护，报警和CCTV系统的维护由供应商在接到电话后进行即时维护并按照合同进行月度维护。供应商应根据要求向我们提供详细的报告。

**2.13.11 Physical Keys 物理钥匙**

The Security Department managed the physical keys in accordance to the procedure under Physical Key Management.This procedure defines the level of security access to the key in security custody. The withdrawal of the key is by authorization and the movement of the key shall be register in the KEY ISSUE REGISTER. This is for the purpose of accountability.

安全部门负责根据程序文件的要求管理物理钥匙，文件规定了钥匙的安全权限。钥匙的借用必须经过授权，并在钥匙借用登记表中登记，以确保可以稽查性。

**2.13.12 Security Audit安全审核**

Security audit relates to the management and operation of audit trails within the various productions processes at the Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Ltdplant. It covers receipt of raw materials, storage of raw materials, issuance of materials for the manufacturing processes, manufacture of products, personalization of products, storage of products, dispatch of products to customers and destruction of materials and products

安全审核涉及到澄天伟业（宁波）芯片技术有限公司管理和各种生产流程。包括原料接收，原料储存，生产过程中的发料，产品制造，产品个人化，产品储存，产品向客户的派送，产品和物料的损坏等。

**2.13.13 Classification of Material and Product物料和产品的分类**

Materials and products are classified according to company procedure in relation to sensitiveness of the item. This procedure determines their security classification and from the classification the manner in which they are handled and stored

物料和产品是根据公司中敏感物料条目的相关程序文件进行分类。这个程序文件决定了他们的安全分类以及相对应的处理和储存方式。

**2.13.14 Receipt of Raw Material原材料的接收**

Security Officers will never permit a vehicle to enter the site to deliver materials unless its arrival has been pre-notified by the relevant authority. They will always ensure that before a vehicle is allowed to enter a loading/unloading dock. The logistics personnel are available to handle the delivery in accordance with existing procedures. The receiving of sensitive component or material shall be under dual control and immediate transfer to highly secure area for storage. An incoming count for such material will be conducted at the earlier possible time together with the property owner.

在没有得到相关部门事先通知的情况下，安全专员不得允许车辆进入公司递送材料。他们必须确保在车辆进入货物装卸区之前，物流部员工已经根据现在的流程做好收货的准备。敏感物料的接收必须在双重控制下并且应该立即储存在高保安区域。类似于这种材料的接收请点应尽可能早的与财产所有者共同进行。

**2.13.15 Storage of Raw Material原料的储存**

Storage of raw materials will be in accordance with their security classification. Highly sensitive material will be immediately stored inside the relevant Security High Area upon receipt. Non-sensitive material can be stored in the logistic storage bay.

原料的储存必须符合安全分类要求，高敏感性的材料在接收后必须立即储存到高安全存储区中。非敏感性的材料可以储存在物流储存区域内。

**2.13.16 Issuance of Raw Material to Production Dept.原料到生产部门的运送**

Raw materials will only be issued for manufacturing by logistics operatives on receipt of appropriate paperwork. Where necessary items will be counted upon issuance by both the issuer and receiver and these facts will be documented. The stock records will also be adjusted to reflect the issue of the raw materials to manufacturing.

物流部门收到相应的文件后，方能将原料运送至生产部。运输的时候必须由发送方和接收方确认并形成书面记录。储存记录也必须调整以反映出原料已运送到生产部。

## 2.13.17 Personalisation个人化

Personalization of cards is a part of the manufacturing process outlined above (i.e. in line) or a separate process. In either case cards and personalization data will be handled according to a local procedure, which ensures full accountability for both cards and data.

卡片的个人化是生产流程中的一部分或者是完全独立的流程。不论是卡片还是数据的个人化都必须完全遵循本地流程，并确保数据和卡片数量的一致性。

**2.13.18 Storage of Finished Product成品的储存**

Storage of finished products is either securely locked inside the steel trolleys (where the product is to be dispatched upon completion and final reconciliation of the order) or transfer to the logistic warehouse for storage pending shipment. Generally, it is a good security practice to secure the finished products under lock and key at all time and it should not be left unattended longer than necessary.

成品需要储存在安全的并且上锁的小推车里（储存在里面的成品是将要被运送以及根据订单协调完成的产品）或者储存在物流的仓库中作为暂时中转。总而言之，时刻将成品储存在有钥匙和锁的地方是一个良好的安全习惯，并且不要将卡长时间的遗留在无人照看的状态。

**2.13.19 Destruction of Rejected Material and Overrun不合格品的处理**

The destruction of rejected materials and products will be in accordance with a local developed procedure. It deals with the method of destruction for all material generated during manufacturing process.

对于需要销毁和拒收的材料和产品必须符合本地程序。这是处理所有在生产过程中产生的材料的方法。

**2.14 Information Technology Security信息技术安全**

**2.14.1 IT Physical security 信息技术物理安全**

* Servers systemsare located in a High security zone with dedicated access control.
* 服务器系统位于独立访问控制的高安全区内。
* Racks containing firewalls, DMZ VPN gateways are kept closed and access restricted to authorize people only.
* 包含防火墙，非军事区（DMZ），虚拟专有网关的机柜保持关闭状态并仅限于已授权人员访问。
* Network cabling is consistent with the zoning: a network cable related to security level N cannot go through a lower security zone without appropriate encryption.
* 网络布线与安全区域相一致：没有经过适当加密处理的网络线缆不能经过较低级别的安全区域。
* Office network and production network are separated by firewall. Network for Security Control System are physically isolated.
* 办公网络与生产网络通过防火墙隔离，安全控制系统网络在物理上是独立的。

**2.14.2 IT network Security 信息技术网络安全**

* Chengtian Weiye (Ningbo) Chip Technology Co., Ltd physical network is operated by IT network team
* 澄天伟业（宁波）芯片技术有限公司物理网络由IT网络团队进行操作
* All firewall rule modifications are approved by security Department
* 所有防火墙规定的修改需要得到安全部的批准后方可进行
* Rules and architecture modification are proposed by local IT team and approved by securityDepartment
* 规则和架构修改由本地信息技术团队建议，由安全部批准后实施。

**2.14.3 IT system security 信息系统安全**

* Desktop
* 台式电脑
* All desktops connected to the Chengtian Weiye (Ningbo) Chip Technology Co., Ltd I.S. must comply with the following requirements:
* 所有连接到澄天伟业（宁波）芯片技术有限公司网络的台式电脑都应当遵守以下规定：
* The desktop must run the anti-virus system selected by Chengtian Weiye (Ningbo) Chip Technology Co., Ltd IT department. Its configuration must also comply with the Chengtian Weiye (Ningbo) Chip Technology Co., Ltd IT standards (i.e. policies).
* 台式机必须运行由澄天伟业（宁波）芯片技术有限公司IT部门选择的杀毒软件。其配置必须遵守澄天伟业（宁波）芯片技术有限公司的标准（比如策略）
* Administrative and support generic accounts should be disabled or protected by a random or station by station diversified password. Otherwise, very strong passwords must be used; a brut force attack on the password hash must require consequent resources and time to prevent such attack.
* 管理员以及通用支持账户应当被禁用或由随机密码保护。否则，必须使用安全级别高的密码；密码的哈希值在遭到暴力破解的时候必须要求能够承受一定的时间。
* That applies also to the computers used by external people needing to access to the Chengtian Weiye (Ningbo) Chip Technology Co., Ltd network for their duties.
* 这也同样适用于外部工作人员借用连接澄天伟业（宁波）芯片技术有限公司网络的电脑。
* That has to be noticed that a disk encryption tool will be available upon request and if this need is justified by the requester duties.
* 同样需要注意的是硬盘加密工具只有在申请人确实因工作需要的时候才可以使用。
* Laptops
* 笔记本
* In addition to security requirements applying to desktops, laptops must comply with the following requirements:
* 除了台式机的安全规定以外，笔记本还需要遵守以下规定：
* The laptop must run a personal firewall that prevents intrusion to the system when connected to a network which is less secure than its usual assigned network, including external networks.
* 笔记本在连接低安全网络，包括外部网络的时候，必须运行个人防火墙以防止发生系统入侵。
* The use of BIOS and hard disk level passwords is highly recommended.
* 强烈建议启用BIOS和硬盘级密码。
* • Laptops must be secured with anti-theft cables at any time they are not under their owners’ supervision, including outside Chengtian Weiye (Ningbo) Chip Technology Co., Ltd premises.
* 笔记本在无人监管的时候尤其是在澄天伟业（宁波）芯片技术有限公司外面的场所，必须使用防盗线缆锁住。
* Secure laptops
* 安全笔记本
* Enhanced security has been enforced on laptops assigned to personnel working in Security level 2 or 3 areas. Those additional measures are agreed between the IT and Security department and should consider:
* 当笔记本在安全等级2或3的区域被使用时，应该使用增强的安全措施。这些额外的措施应当经过IT和安全部门的同意。

• The furniture of secured media for data backups and exchanges.

* 用于数据备份和交换的加密媒体。
* The systematic installation of a disk encryption tool.
* 硬盘加密工具的安装。
* •The obligation to use a token (two-factor) for strong authentication and any data encryption (VPN, disk encryption, email…).
* 使用令牌（双因素）以加强认证以及任何数据加密（VPN，硬盘加密，邮件等）
* ANTI-VIRUS
* 反病毒软件
* Against intrusion and infection by virus, antivirus software must be deployed on all Chengtian Weiye (Ningbo) Chip Technology Co., Ltd networks when such software exists. The software must be installed, enabled and regularly updated (antivirus signatures) on all computing devices to prevent, detect, and remove viruses.
* 为了防止病毒的入侵，所有澄天伟业（宁波）芯片技术有限公司司网络必须部署反病毒软件。软件必须在所有电脑上安装，启用及定期更新（反病毒特征），以防止、检测和删除病毒。
* Those preventive and corrective actions must also be applied on all incoming and outgoing flows (i.e. emails).
* 那些预防性和纠正性措施必须同时应用在所有输入和输出流上。（比如电子邮件）
* Such software must be continuously enabled on all networked IT devices, even if the IT equipment is connected intermittently.
* 即使IT设备间断地连接网络，反病毒软件也必须持续地在所有网络IT设备上启用。

# 3 RESPONSIBILITY责任

Employee’s of the company is responsible to maintain the minimum Security Standard as written in this procedure. Security is everybody business. Hence it is the sole responsibility for all staff to report any discrepancy or violation to the Security Manager or the Production Manager for follow-up action.

所有员工都有责任维护本手册规定的最基本的安全标准，安全是每个人的职责。因此，每个员工都有责任向安全经理或生产经理汇报违反安全的行为以便更好的跟踪此行为。

# 4 ABBREVIATION AND TERMS缩写和指代

Company：It is defined as Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Ningbo.

**公司**指澄天伟业（宁波）芯片技术有限公司

# 5 QUALITY RECORDs质量记录

The normal minimum retention period for all quality record is 2 years unless specify.

除非有特别要求，否则所有记录将保持两年时间

# 6 REFERENCE DOCUMENT(S)参考资料

Security Guideline 安全指导方针

# 7 appendix附件

# 1】.安全等级区域划分图Security zones division layout

# 2】CISO任命书CISO appointment letter.