Development Security Policy and Procedures

开发安全政策与流程

|  |  |  |
| --- | --- | --- |
| Author | Reviewer | Approver |
| Julio LI |  |  |

**Version Control**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 0.1 | 29/11/2019 | First document release |
| 0.2 | 15/05/2020 | Combined content from different documents |
| 0.3 | 21/05/2020 | Update contents |
| 0.4 | 18/06/2020 | Update contents of HR and IT |
| 0.5 | 03/09/2020 | Minor changes |
| 0.6 | 10/09/2020 | Minor changes |
| 0.7 | 28/09/2020 | Confirmed comments resolved and version changed |

**Contents**

[1 Introduction 简介 5](#_Toc43386955)

[1.1 Scope 范围 5](#_Toc43386956)

[1.2 Document overview 文档综述 5](#_Toc43386957)

[2 General Statements 通用声明 7](#_Toc43386958)

[2.1 Objectives of the DSS and DSD documentation DSS与DSD文件的目的 7](#_Toc43386959)

[2.2 Production Sites 生产站点 7](#_Toc43386960)

[2.3 Development Security Maintenance 开发安全维护 7](#_Toc43386961)

[3 Asset Management 资产管理 9](#_Toc43386962)

[3.1 Ownership of Assets 资产所有权 9](#_Toc43386963)

[3.2 Inventory of assets 资产清单 9](#_Toc43387006)

[3.3 Acceptable Use of Assets 资产的合理使用 10](#_Toc43387007)

[3.4 Information and Data Classification 信息数据分类 10](#_Toc43387008)

[3.5 Documentation Numbering Management Procedure 文档编号管理程序 11](#_Toc43387061)

[3.6 Destruction of Assets 资产销毁 11](#_Toc43387064)

[4 Information Security Management System 信息安全管理系统 13](#_Toc43387065)

[4.1 Organizational Chart 组织结构图 13](#_Toc43387066)

[4.2 Organizational Responsibilities 组织职责 13](#_Toc43387067)

[4.3 Security Committee Organizational Chart 安全委员会组织结构图 13](#_Toc43387068)

[4.4 Security Committee Responsibilities 安全委员会职责 14](#_Toc43387070)

[5 Human Resources 人力资源 18](#_Toc43387071)

[5.1 Selecting and Hiring 选拔和雇用 18](#_Toc43387072)

[5.2 Security Awareness and Training安全意识和培训 19](#_Toc43387073)

[5.3 Confidentiality and business conduct 保密和业务活动 20](#_Toc43387074)

[5.4 Change of Personnel 人员变动 21](#_Toc43387075)

[5.5 Employment Termination 员工离职 21](#_Toc43387118)

[5.6 Security Discipline 安全纪律 22](#_Toc43387119)

[6 Physical Security Facilities Management 物理安全设备管理 23](#_Toc43387120)

[6.1 Site Perimeter Protection 现场周边保护 23](#_Toc43387122)

[6.2 Exterior Building Security外部建筑安全 23](#_Toc43387123)

[6.3 Physical Access Control 物理访问控制 24](#_Toc43387124)

[6.4 Access Control Management System 28](#_Toc43387125)

[6.5 Visitors Management 访客管理 31](#_Toc43387126)

[6.6 Physical Key Management物理钥匙管理 37](#_Toc43387127)

[6.7 CCTV Monitoring 闭路电视监控 37](#_Toc43387162)

[6.8 Alarm System 报警系统 39](#_Toc43387175)

[6.9 Power Supply 电源供应 40](#_Toc43387206)

[6.10 Inspection for Physical Security Facilities 检查物理安全设施 41](#_Toc43387208)

[6.11 Guarding警卫 41](#_Toc43387209)

[6.12 Goods storage and Vaults货物存储和仓库 42](#_Toc43387215)

[6.13 Secure Cabinets 安全文件柜 43](#_Toc43387216)

[6.14 Receipt and Dispatch Areas收货和发货区 44](#_Toc43387217)

[7 Security Control of Documents 文件的安全控制 46](#_Toc43387218)

[7.1 Controlled Document Management 受控文件管理 46](#_Toc43387219)

[8 Logical Security Management 逻辑安全管理 47](#_Toc43387222)

[8.1 General Principle总则 47](#_Toc43387223)

[8.2 Network Security 网络安全 49](#_Toc43387238)

[8.3 Logical Access Control 逻辑访问控制 57](#_Toc43387239)

[8.4 Data Security 数据安全 62](#_Toc43387246)

[8.5 Removable Media 63](#_Toc43387247)

[9 Production Security Management 生产安全管理 66](#_Toc43387248)

[9.1 Traceability and Accountability可追溯性和问责制 66](#_Toc43387249)

[9.2 Production Audit Processes生产审核流程 66](#_Toc43387250)

[9.3 Sample Management样品管理 67](#_Toc43387251)

[10 Security Incident Management 安全事故管理 69](#_Toc43387252)

[10.1 Incident Preparation事件准备 69](#_Toc43387253)

[10.2 Incident handling 事故处理 70](#_Toc43387254)

[10.3 Incident Report And Closure事故的汇报和关闭 74](#_Toc43387255)

[11 Risk Analysis & Business Continuity 风险分析与业务连续性 75](#_Toc43387256)

[11.1 Risk Analysis 风险分析 75](#_Toc43387257)

[11.2 Business Continuity 业务连续性 75](#_Toc43387265)

[12 Internal Audit Program and Preventive Maintenance内部审计程序及预防性维修 77](#_Toc43387266)

[12.1 Internal Audit Program内部审核系统 77](#_Toc43387267)

[12.2 Reporting to Corporate Security向公司安全部报告 78](#_Toc43387268)

[13 Justification of necessary level of protection 79](#_Toc43387269)

[13.1 General Assessment 80](#_Toc43387270)

[14 Bibliography 81](#_Toc43387271)

1. Introduction 简介

Development security concerns physical measures, procedural measures, personnel measures, and other measures that apply to the development environment to protect confidentiality and integrity of security products such as operating systems, cryptographic libraries, personalization software, cryptographic keys, and so on.

开发安全会综合考虑包括物理措施，程序措施，人员措施以及其他相关的应用于开发环境中的措施，用以保护安全产品（如操作系统，密码库，个性化软件，密钥等）的机密性以及完整性。

This Development Security Document (DSD) deals with the security in the development of security products of CTWY. In particular, the Development Security System (DSS) hereby described apply to the products aiming to the Common Criteria (CC) security certification. Therefore, the security measures described in this document meet the requirements enforced by the CC assurance component ALC\_DVS.2.

本开发安全文档（DSD）用于处理澄天伟业的安全产品开发中的安全性。特别地，这里描述的开发安全系统（DSS）适用于针对通用准则（CC）安全认证的产品。因此，本文档中描述的安全措施满足CC保证组件 ALC\_DVS.2里强制性的要求。

This document takes into account the recommendations given in the document “Minimum Site Security Requirements” (1).

本文档参考了“站点最小安全需求”文件内的相关建议。

Throughout the Development Security Policy documentation, development and related terms (developer, develop) are meant in the more general sense to comprise development and production.

在整个开发安全策略文档中，开发与其相关的术语（开发者，发展）在更一般的意义上是包含开发与生产的。

* 1. Scope 范围

This document applies to CTWY as overall company dedicated to CC certification, as well as to their supporting processes.

本文档适用于那些全部公司都遵循CC认证的澄天伟业，以及他们的支持流程。

* 1. Document overview 文档综述

This document is organized as follows:

* Section 2 provides general information about development security, such as security objectives, sites and on the maintenance of the DSS;
* Section 3 is dedicated to the asset management and deals with classification of confidential information and with identification, preservation and destruction of assets;
* Section 4 is dedicated to the Information Security Management System, focusing on the Organization of the company and the responsibilities assigned to the roles in CTWY;
* Section 5 concerns security aspects of the Human Resource Management;
* Section 6 deals with physical security measures;
* Section 7 describes the configuration and the documentation management;
* Section 8 is focused on security aspects concerning the network;
* Section 9 is dedicated to the Production Security Management;
* Section 10 Security Incident Management;
* Section 11 describes the Risk Analysis & Business Continuity of the company;
* Section 12 is about the Internal Security Audit;
* Section 13 provides a Justification of necessary level of protection;
* Section 14 lists all the documents referred in this document.

1. General Statements 通用声明
   1. Objectives of the DSS and DSD documentation DSS与DSD文件的目的

The DSS has been designed and implemented to keep confidentiality, integrity and availability of the information.

DSS的设计和实施是为了保持信息的机密性、完整性和可用性。

This Development Security Document (DSD) defines security policies, rules and best practices for the implementation of the Development Security System (DSS).

本开发安全文档(DSD)定义了实现开发安全系统(DSS)的安全策略、规则和最佳实践。

* 1. Production Sites 生产站点

The activities of Production considered in this DSD are carried out in the site, that is hosted in the CTWY building located in No.8, Binjiang Road, Cixi High-tech Industrial Development Zone, Ningbo City, Zhejiang Province, P. R. China. This site hosts the technical department, the administrative department, the sales department and a warehouse. This site includes one restricted production areas featuring security measures in compliance with Common Criteria requirements of the assurance component ALC\_DVS.2.

本DSD文档中考虑的活动场地（生产，开发）是在站点中实施的，该站点位于中华人民共和国浙江省宁波市慈溪高新开发区滨江大道8号，澄天伟业的大楼中。这个站点包含有技术部、行政部、销售部和一个仓库。此站点还包括一个受限制的生产区域，其安全措施符合保证组件ALC\_DVS.2的通用准则要求。

* 1. Development Security Maintenance 开发安全维护

This policy is a guideline document, which is drafted and complied by the HR Department according to the relevant requirements and standards. The following must be taken under consideration for the overall document:

本政策是一份指导性文件，由HR部门根据相关要求和标准起草和执行。整个文件必须考虑到下列各点:

* This document is applicable to CTWY and all its employees, to provide policy about all security matters; the actual operation procedures should be based on this policy and be implemented and operated in CTWY.

本文件适用于澄天伟业及其所有员工，提供有关所有安全事宜的政策;实际操作程序应以本政策为依据，以澄天伟业名义实施和操作。

* This document is also applicable to subcontractors and external technical support personnel, to satisfy the wishes of the corporate management in the security policy statement.

本文件也同样适用于分包商和外部技术支持人员，以满足公司管理层在安全政策声明中的意愿。

* All CTWY employees must comply with the laws of the country where they’re working, and the following statement is to be reflected in the procedures related to the employees of. Only in case that observation of these statements will violate laws, or the strict observation of these statements will void the local agreement, could these statements be deviated. These statements are part of the general security procedures and rules, and the general security procedures and rules are part of the mandatory procedures. The general security procedures and rules must be provided to all employees of CTWY.

所有澄天伟业的雇员必须遵守他们的工作地所属国家的法律，下列的一般声明在雇员有关的程序中得到反映。只有在遵守这些声明会违反法律，或者严格遵守这些声明会使局部协议无效的情况下，才可以与这些声明相背离。这些声明是通用安全程序和规则的一部分，而通用安全程序和规则又是强制性程序的一部分。通用安全程序和规则须提供给澄天伟业的所有雇员。

1. Asset Management 资产管理

The intention of this section is regarding the assets (management, identification, etc): It must be ensured that all assets:

本章节关注的是有关资产的（管理或者识别等）。必须保证所有的资产：

* Are clearly identified and classified.

被清楚地识别与分类。

* Need to have an ownership.

需要有一个持有人

* Labelling and handling procedures of information, data and material must be clearly defined and implemented.

信息，数据和材料的标记与处理程序必须被清楚地定义并实施。

* “Need to know” principle is applied to all assets.

所有的资产都要遵循“需知原则”。

* 1. Ownership of Assets 资产所有权

The Assets Inventory must be reviewed annually by the security manager and updated immediately if there is any modification towards the assets of this list. Security manager must sign on the Assets Inventory to confirm the review result.

安全经理必须每年都评审一次资产清单，如果有任何关于清单中的资产需要被修改，资产清单需要立即进行更新。安全经理必须在资产清单上签字以确认评审结果。

* 1. Inventory of assets 资产清单

The security committee will maintain and manage the important **Assets** (such as software , hardware, etc.) of company. These are under the responsibility of the General Manager, reporting the following information:

公司的质量控制小组会管理并维护公司重要的资产（比如软件，硬件等）。这些都是由总经理来负责，统计以下信息：

* 1. Asset No. 资产编号
  2. Type of asset 资产种类
  3. Type of protection 保护类型
  4. Description 资产描述
  5. Asset name 资产识别
  6. Owner 持有人
  7. Location 地点
  8. Protection measures 保护措施
  9. Acceptable Use of Assets 资产的合理使用

The protection level for the assets which is enhanced, the owner of these kinds of assets should be well trained before using the assets.

All the assets must only be used for the official purpose, personal usage for the assets is not allowed in the company.

所有的资产都只能被用于办公目的，对资产的私人使用是不被允许的。

Any changes towards the Assets Inventory should be updated.

资产清单的任何修改都应该立即更新。

* 1. Information and Data Classification 信息数据分类

According to the value for the company and risk severity, the information and data assets will be classified into the following 4 confidentiality levels:

1. 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

1. 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

1. 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

1. 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

The different level of the assets will be restricted to access for different entities.

不同实体对不同安全等级资产的访问需要被严格限制。

The **secret** information and data assets are strictly allowed to be access for the management level of company, or the entity authorized by the management level of company; “Four eyes principle” is applied for assets under this clasification.

严格限制公司管理层或公司管理层授权的实体访问公司的高机密信息和数据资产;“四眼原则（即双人共同管理原则）”适用于该分类下的资产。

The **confidential** information and data assets are allowed to access only by the corresponding department for the internal usage purpose;

机密分类下的信息数据资产只允许相关的部门访问，且只能是内部使用的目的。

The **private** information and data assets are allowed to access in the company;

内部信息数据资产能在公司内部进行访问。

There is no access limit regulation for the **public** information and data assets.

对公共信息数据资产没有访问限制规定。

Assets are restricted under the rule of “need to know” principle in order to avoid the leakage of information.

为了防止信息的泄露，资产必须严格的遵循“需知原则”的规定

* 1. Documentation Numbering Management Procedure 文档编号管理程序

Please refer to *Documentation Numbering Management Procedure.*

请参考《文件编号管理程序》。

* 1. Destruction of Assets 资产销毁

For destruction of production materials, please refer to the “The Control And Destruction Of Rejected Cards Procedure.

生产材料的销毁参照《废卡的控制及销毁程序》。

Deletion of written sensitive information should be done by a shredder. There is a shredder located in the packaging workshop.

纸质敏感信息的销毁必须使用碎纸机。封装车间有碎纸机。

1. Information Security Management System 信息安全管理系统
   1. Organizational Chart 组织结构图

Figure 1 CTWY Organization chart

A green sign with white text

Description automatically generated

* 1. Organizational responsibilities 组织职责
     1. General Manager总经理

Responsible for the company strategy formulation and implementation, market development, corporate culture creation, daily operations management, sales management, as well as the selection of middle and high-level management personnel, and approving the major personnel decisions.

负责对公司的战略制定以及实施，市场开拓、企业文化创建、日常运营管理、销售管理，以及中高层管理人员的选拔，并批准重大人事决策。

Responsible for the implementation of the board of directors' resolutions and regular communication with the board of directors about the company's production operation and major emergencies.

负责执行董事会决议，定期与董事会沟通公司生产经营及重大突发事件。

Make the final approval towards the department structure deployment, staff plan, role and responsibilities adjustment.

对部门结构部署、人员计划、角色职责调整做出最终批复。

* 1. Security Committee Organizational Chart 安全委员会组织结构图



Figure 2 CTWY security committee

The Security Committee is responsible for the operation and maintenance of information security management system. The security committee meeting will be held monthly.

安全委员会负责对信息安全管理系统的运行和维护。安全委员会会议每月召开一次。

* 1. Security Committee Responsibilities 安全委员会职责
     1. Security 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 examine, monitor and document 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。

* + 1. Security Officer安全专员

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 to CCTV surveillance system, video recording system, alarm system and physical access control system and should report the exceptions of system to Security Manager. The other aspect of control is the security instructions, security procedures and security reports and forms that regulate their area of work.

The Security Officer report directly to the 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，门禁控制系统有操作权限，并负责像安全经理汇报系统的异常情况。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。安全员直接向安全经理汇报。

* + 1. IT Engineer IT工程师

IT Engineer is responsible for network maintenance, log management, anti-virus management, information security related management, vulnerability detection and the maintenance of server.

IT工程师主要负责网络维护、日志管理、病毒防护管理、信息安全相关的管理、漏洞侦测和服务器维护。

* + 1. IT Assistant IT助理

IT assistant is responsible for the assistance of performing data security, data backup, vulnerability scanning and data maintenance. Besides, IT assistant in charge of CM system daily operation and management.

IT助理负责数据安全、数据备份、漏洞扫描和数据维护。除此之外，IT助理还负责配置管理系统的日常操作和管理。

* + 1. HR人力资源

HR is responsible for the performing the procedures that prior to employment, during employment and termination of employment and related security measures.

人力资源负责雇佣前、雇佣期间和雇佣终止等流程操作以及相关的安全措施。

* + 1. 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。

1. Human Resources 人力资源

HR department is responsible for formulating the HR plan of the organization, and applying for the recruitment, training, adjustment and dismissal of the personnel for the organization.

HR 部门负责制定组织的人力资源计划，并为组织申请人员的招聘、培训、调整和解聘。

The core responsibility of the HR department is to conduct HR management in a planned way according to the requirements of enterprise development strategy, to select, train, search and motivate talents for the company, reasonably allocate personnel, motivate employees, give play to their potential, create value for the enterprise and guarantee the realization of enterprise strategic goals.

HR部的核心职责是有计划地进行人力资源管理。根据企业发展战略的要求，来为公司选择、培训、寻找和激励人才，合理配置人员、激励员工，发挥他们的潜能，为企业创造价值，确保企业战略目标的实现。

* 1. Selecting and Hiring 选拔和雇用

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

Human Resource department is responsible for screening candidates to be recruited and security investigation of candidates, including education background, employment history, criminal records and credit status, etc. Same procedure applies to contractors and third parties.

人事部负责筛选被录用的候选人，对候选人进行安全调查，包括教育背景、工作经历、犯罪记录、信用状况等。同样的程序也适用于承包商和第三方

In the selection of candidates for employment, the following checks are performed:

在选择雇员时，须进行下列检查:

* Possession of the required skills.

具备必要的技能。

* Completeness and accuracy of the applicant’s curriculum vitae.

申请人简历的完整性和准确性。

* Confirmation of identity.

确认身份。

* Confirmation of claimed qualifications.

确认所声称的资格条件。

* Confirmation that the candidate has no pending prosecutions.

确认候选人没有存在任何指控。

* Confirmation that the candidate is not present in the criminal records.

确认候选人没有任何犯罪记录

All employees should sign NDA before being hired by the company.

所有的员工在入职之前必须和公司签订保密协议。

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 Staff Temporary 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。

* 1. 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。

* + 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。

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。

Awareness Training意识培训

This type of training is 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. This kind of training for all the employees is performed annually.

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。这种针对全体员工的培训每年举办一次。

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。

* 1. Confidentiality and business conduct 保密和业务活动

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。

The GM and related staffs 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，总经理和相关人员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。

* 1. Change of Personnel 人员变动

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。

* 1. Employment Termination 员工离职

Supervising termination procedure is the responsibility of HR department. A checklist is used for performing the procedure by checking whether the employee has cancelled all the logical access right, returned physical badge card and company property before leaving. The checklist is named that *employee termination delivery form*.

监督离职流程是HR部门的职责。一份用于执行这个流程通过检查员工在离职前是否已取消逻辑访问权限、收回物理门禁卡和公司资产。这份清单被命名为*员工离职交接单*。

If termination of employment is a planned event. The Human Resources Department will arrange for appropriate notification to avoid the possibility of security breaches as a result of the employee leaving the company.

当员工辞职离开公司时，人力资源部将安排适当的通知以避免违反安全规定的雇员离开公司的可能性。

All physical and logical accesses should be closed, and sensitive assets inventoried and returned to Human Resources or employee’s management.

应关闭所有的物理和逻辑访问权限，并且清点和交还敏感的资产至人力资源或员工管理。

During exit interviews carried out by the Human Resources department, the employee will be reminded of the confidentiality agreement he/she has signed and that the terms of this agreement will remain in force in relation to confidential information gained during the course of his/her employment after having left the employment of the company. This will be recorded on the exit document, signed by both parties.

在由人力资源部进行离职面谈时，雇员将会被提醒他/她已签署的保密协议和本协议的条款将继续有效，有关机密信息在他/她离开该公司后的就业过程中仍然有效。这将记录在离职文档中，并由双方签署。

If termination of employment is an unscheduled event, The Personnel Department shall confirm the event immediately after receiving the department's notification and complete the above normal contract termination process on behalf of the employee within 24 hours.

如果终止合同是一个非计划内的事件,比如常说的自离，人事部在接到部门通知后，需立即确认此事，并在确认后24小时内代表该自离员工完成以上正常离职流程。

* 1. Security Discipline 安全纪律

In case of violation of the security provisions, we will deal with its nature and gravity of the breach and its impact on confidentiality and integrity of the assets, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors. The corresponding department manager shall teach the employee who breaks the rules and the employee must make the commitment by written to declare that the same mistake will be paid enough attention and not to happen again.

如果出现违反安全规定的情况，需要根据事故的性质，严重性以及其对资产的机密性与完整性的影响来处理，并且还要考虑是是否是第一次违反，违反者是否接受过相应培训，相关立法，商业合同和其他因素。相应的部门经理应教育违规员工，员工必须以书面形式承诺，同样的错误将得到足够的重视，不再发生。

For severe violation of the security stipulations or the laws, the employees will be reported to the police station for treatment. The situation of the fired employee will be posted to inform other employee to avoid the same situation happen, the post notification form will be kept in the employee’s background file.

严重违反安全规定或法律规定的，应当报派出所处理。被解雇员工的情况会被张贴出来通知其他员工，以避免同样的情况发生，张贴通知表格会保存在员工的背景文件中。

For more information, please refer to “Staff Manual v1.0”.

1. Physical Security Facilities Management 物理安全设备管理
   1. Site Perimeter Protection 现场周边保护

There are three sides of perimeter walls and one side of a river surrounded the factory premise. An entry gate of the perimeter wall guarded by security guard. CCTV cameras are deployed in both the perimeter walls and the premise’s wall facing the river and all the CCTV cameras are connected to the security room located within the premise.

工厂厂房三面围墙，另外一面被一条河阻挡。只有一个围墙入口，有安保把守。三面围墙和面向河岸的厂房外墙都部署了CCTV摄像头，并连接到位于厂房内的安全控制室。

Security guard will cruise the roads within the perimeter walls every two hours during daily time. Security guard working in the entry gate will be on duty for 24 hours and 7 days per week.

白天安保会每两个小时在工厂围墙内的路上巡逻。安保7天24小时值班。

Security guards in the security control room are set with two shifts with 12 hours for each shift. At any time, there are at least 2 guards working in the security control room.

安全控制室里的安保每天有两班每班12个小时。在任何一个时间段安全控制室里都有至少2个安保。

Access to the factory premise is controlled by doors equipped with physical access control system where the control panel of the system is deployed in security control server room.

进入厂房的门装备了门禁系统，门禁系统的控制端部署在安全控制室。

Two layers of protection:

两层防护：

Detection layer: registration and identification performed by security guard in the entry gate of the perimeter, CCTV camera deployed around the factory premise, security guards’ periodic cruising.

检测层：围墙入口安保执行的登记和身份识别、部署在厂房四周的CCTV摄像头、安保的定期巡逻。

Stop layer: doors for the entry of the factory premise equipped with physical access control system and security guard coming for any detected issues.

停止层：配备了物理门禁系统的厂房入口门、奔赴检测到事件地点的安保。

* 1. Exterior Building Security外部建筑安全
     1. Building Construction建筑施工

Areas within the scope of this audit only have one window that located in the security control room and it is blurred to prevent external observation. There are security guards on duty within the security control room 24 hours per day and 7 days per week, which is able to prevent entry by breaking the window.

这次审核范围内的区域只有一扇窗户，位于安全控制室而且经过了模糊处理来防止外部的观测。安全控制室内的安保7天24小时在岗，以此能够防止通过打破窗户玻璃进入。

* + 1. 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 monitored by CCTV cameras. 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，建筑的外墙都必须由CCTV监控。必须特别注意大门、门和紧急出口。

* 1. Physical Access Control 物理访问控制

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 have a backup electrical power source capable of maintaining the system for 1 to 2 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1到2小时。

* + 1. Basic基本

**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。

* + 1. High security area 高安区

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：

Doors deployed in high security area are controlled by two persons’ badge for entry and exit.

高安区门的门禁通过双人的门禁卡来控制进出。

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）

**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。

* + 1. Entry to packaging workshop封装车间的进入

Further features are required for specific areas:

特定领域需要进一步的功能：

there are two entry doors to the packaging workshop, which are deployed on the same locality for efficiency consideration. The two doors there not only have physical access control system but also have one-by-one feature. The one-by-one feature can implement anti-pass back function.

进入封装车间的两扇门位于同一地点，两扇门的设置是出于效率方面的考虑。这两扇门不仅有物理门禁系统而且具有单次一人通过的功能。这种功能能够实现防潜回。

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。

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。

* 1. Access Control Management System
     1. Installation of Access Control System 门禁控制系统的安装

The access control panel and device are installed inside the Security Control Room. While the entire card readers are installed at relevant access point throughout the premises.

门禁控制系统设备安装于安全控制室，而全部的读卡器安装在整个工厂的相关访问点。

* + 1. The Method of Control 控制方法

The Point of Access into the facility is controlled by contactless badge. The badges act as an identity card as well as a key to his/her place of work. The access process is divided into 3 barriers of access groups for effective control. They are the following:

进入工厂的通过门禁控制，门禁是由ID卡或密码实现：

a) The Glass Door at the reception and side entrance. 玻璃门在接待处与侧门

b) The one-by-one door into the workshop. 单人通道安装于车间

c ) Dual control for doors in high security area. Two badges for entry and exit. 安全区门的双人控制。两个门禁卡用于进出。

d ) The good traps with interlocking system (three doors’ control) for the transfer of goods. 货物通道具有互锁功能为了货物运输(三门控制)。

* + 1. Security Control on Access Badge System 门禁系统的安全配置

Security officer shall be responsible to check and ensure that the system is functioning effectively to meet the day-to-day workload. He shall review the access rights of staff from time to time. This is achievable by sending a periodical copy of the current access printout to security manager for review monthly and security manager will sign the printout. The returned listing will be updated accordingly into the system. In furtherance, the security officer shall on a weekly basis, update or delete the access right of any staff, acting on written information. Any discrepancy will be reported to security manager for further investigation.

安全员负责检查确保系统功能是有效的并能满足每天的工作量。他应不定时检查员工的门禁权限。通过定期发送当前打印的权限复印件记录至安全经理检查是可适用的，安全经理确认后签字。返回的清单将相应地更新到系统中。安全员应每周更新或删除任何员工的权限并书面记录。为了进一步调查任何不符都需报告至安全经理。

* + 1. The Physical Control on Badges Stock 门禁卡库存的物理控制

The security officer assisted by security guard in the security control room shall be the sole custodian of the Access Badge stock. The movement of the badge shall be recorded in a register. The issue or withdrawer of the badge shall be under the supervision of the security manager.

安全员并在一名保安的协助下，应是唯一的门禁卡存储管理员。门禁卡的转移必须记录。门禁卡的发出或回收都应在安全主管的管控下。

Unused access badges are stored in a secure box located in the security control room and needs two keys to unlock it. One key is kept by the security officer and another key is kept by a security guard within the security control room. Every time when security officer needs to open that secure box and uses the unused badges, that security guard has to help him aside.

未使用的门禁卡被锁在安全控制室的保险柜里，这个保险柜需要同时两把钥匙才能打开。一把钥匙由安全员掌握而另一把在安全控制室的一个安保手里。每次安全员需要打开保险柜使用未使用的门禁卡，有另一把钥匙的安保必须在一旁协助。

* + 1. Predetermine Access Right 预定门禁权限

HR department shall notify security officer in writing upon confirmation of appointment. The staff’s

badge access right is activated in accordance with the individual area of work.

人力资源部应书面通知安全部确认的职位，员工的门禁卡权限依据工作的区域来激活设置。

* + 1. Change of Access Status门禁权限的变更

The involved employee shall raise an ‘Entrance Authorization Application’ for the purpose of any change in the access right of the individual employee. Department manager and security officer will review the application then it shall be approved by security manager.

由涉事员工提交一份员工权限变更申请表来变更权限，部门经理和安全员会审核这份申请再由安全经理评估是否授权。

* + 1. Issue of Badges 门禁卡发行

The Security Officer at the security committee is responsible for the issue of visitor’s badge / temporary badge / contractor badge only on the condition that proper documentation and approval is done prior to the visit, not otherwise. A badge issue log is maintained for all cards issue. This is to ensure that the issued badges are return at the end of the visit. Cards not return should be reported to security officer who shall immediately remove all access rights attached to that badge. The next course of action is to recover the badge with the assistance of the host.

监控室安全人员负责访客卡，临时卡与合约卡的发行，前提是关于访问的适当的文件已经被提前做好并获得批准，否则不行。门禁卡发行日志包含所有的卡片发行。这是为了确保访客卡在最终被返回至安全部。未归还的门禁卡应报告至安全员，安全员将立即取消该卡片的所有权限。下一步是在卡片持有人的协助下找回门禁卡。

* + 1. Monitoring of Anti-Pass Back反潜监控

The security officer shall check the system log showing all internal anti-pass back activation. He hall determine whether follow up action is necessary to be highlighted to the departmental head for discipline action or retraining on the proper use of the access control system by such employee.

安全员将审查所有内部返潜系统记录并决定是否提交至部门领导采取措施或者对此类员工进行培训门禁系统的正确使用方法。

* + 1. Destruction of Badge

Badges returned or surrendered to Security Control Center under the following circumstances:

以下情况门禁卡需归还至安全控制中心：

a) Resignation辞职

b) Termination结束

c) Dismissal 解雇

d) End of Contract 合约终止

e) Damaged / Defective Badge 损毁/卡片失效

The security officer upon receiving the above badge after verification shall immediately cut the

badge into half. This is to render it unusable. He shall deposit it into a box for later transfer to the

Shredder Room for further destruction before final disposal.

安全员在确认后收回以上卡片应立即将卡片剪成两半使其不可再使用。在最终处置之前他应将废卡集中放置在一个盒子里随后运至粉碎间进行进一步粉碎。

* + 1. System Time 系统时间

The System time for this system is to be sync to within 2s manually with the CCTV system and Alarm System and this is to be checked daily and this is in the security control center Checklist. The check is performed by security guard within the security control room per day and security officer will check the record weekly.

门禁系统的时间应手动调整2秒与CCTV监控系统和警报系统同步，此项需每天检查并记录在安全控制中心检查清单上。这种检查由安全控制室里的安保每天来做并且安全员会每星期检查。

* + 1. Password Change 密码变更

Account passwords are to be changed once every 90 days for all user accounts.

所有用户的账号密码需每三个月更新一次。

* + 1. Review 检查

Every month, there will be a review of the Groups Access List and the Personnel assigned to each group. This will be reviewed and verified by the security manager by comparing the prepared list prepared by the security officer against the System entries. The verification can be done by sampling.

Every week, the security officer will check all exception cases such as Anti-pass backs to determine if any unauthorized access or attempts have been done and this will be reviewed by the security manager.

每个月都有一个组权限和人员对应列表。安全经理会审核、验证这些权限通过比对安全员根据门禁系统设施准备的列表。验证可以通过抽样调查。

每周，安全员会检查所有例外的事件比如反潜回等来决定是否有未授权的访问或尝试并且安全经理会做出审核。

* + 1. System Log 系统日志

Access control system log should be retained at least 12 months.

门禁控制系统日志应至少保存12个月。

* + 1. Responsibility 门禁卡管理职责

The security officer shall be responsible for:

安全员负责：

a) The proper handling of the Badge Access System that is installed in the Security Control Center. 安装在安全控制是的门禁系统的适当操作

b) Badge Stock Control. 空白门禁卡控制

c) Maintenance of log register. 维修登记日志

d) Issue badges and return of the badges. 门禁卡的发放与归还

e) The destruction of all return and defective badge. 失效和待销毁门禁卡归还

The Security Manager shall be responsible for the audit of the issue badge system and the audit of the access badge stock.

安全经理负责发卡系统和门禁卡库存的审核。

* 1. Visitors Management 访客管理
     1. Control of Visitors访客控制

The Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. host is responsible for the visitor at all times during his/her stay within the premises and must ensure that he/she is always accompanied by a Chengtian Weiye (Ningbo) Chip Technology Co., Ltd employee.

澄天伟业（宁波）芯片技术有限公司被访者有责任保证访问者在工厂访问的时候有澄天伟业（宁波）芯片技术有限公司员工全程陪伴。

The host department shall be responsible to notify the Security Department of the impending visit. The notification must be served at least 24 hours prior to the visit.

被访部门应负责通知安全部门访问计划，访客入厂核准申请表应在访客到达24小时之前提交给安全部。

The host department upon confirmation of the visit shall adhere the relevant requirements. (i.e. to complete the ‘visitor entry approval application’form)

被访部门一旦与访客确认后，应遵循该相关要求。（如完成“访客入厂核准申请表”）

The host shall be responsible to inform the Visitors prior to their visit that recording material and

smoking is prohibited in the facilities area.

被访问人有义务提前通知访客，在生产区域严禁携带记录设备并且禁止吸烟。

Visitor(s) without an appointment will not allow access to Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. Security Areas. Instead the Security officer shall politely inform the visitor(s) that it is necessary to make an appointment prior to the visit.

未预约的访客不得进入澄天伟业（宁波）芯片技术有限公司的安全区域。安全员应该礼貌的通知访客，在访问之前应该事先预约。

The security officer at the security control room shall contact the host if there is business

urgency. This shall be done on a case to case basis. The host shall meet the visitors outside the

security control room if he decides to entertain this. The host shall complete a ‘visitor entry approval application ’ form on the spot and submit to the Security Manager or Security Supervisor for approval. Visitors to Secure Areas require approval from Security Manager such as R&D, Server Rooms etc.

若有紧急的事务，在安全监控中心的安全主管应该联系被访人，但是应在个案的基础上。若被访问者决定接待该访客，则必须在监控中心外进行接待。被访问人应该完成“访客入厂核准申请表”并且提交给安全经理或者安全主管获得批准。对于需要访问安全区域的访客，必须获得安全经理的批准，如研发中心，服务器室等。

* + 1. Unspecified Visitors 未知访客

The security control room and Reception staff shall take the following action in the course of

meeting with unspecified Visitor(s).

监控中心以及前台在接待未知访客的时候，应按照如下流程进行接待。

* Obtain the name, address and telephone number of the company the person is said to represent. The particular of the host he intends to meet.

应该获得此访客的姓名、地址、电话以及他需要访问的人员。

* Politely inform the person that visitors are required to make an appointment in advance.

礼貌的通知该访客应该事先进行预约。

* The detail shall be submitted to Security Manager.

具体要求应该提交予安全经理。

* Security Manager will contact the company concerned to inform them of our policy.

安全经理应与有关公司联系并通知他们我们的方针。

* Check the identity of the visitor with the company concerned to ascertain the visitor’s bona fides.

核查该访客的身份以确保访客信息的真实。

* If the person is unknown to the company as mentioned, Security shall consider informing the police and notified the accreditation authority.

若该访客的公司不认识此访客，安全部应考虑报警并且通知其资格认证。

* + 1. Urgent Visits by Relatives家属紧急访问

There may be urgent need to visit Chengtian Weiye (Ningbo) Chip Technology Co., Ltd by relatives of employees. In this case the following action shall be taken:

如遇公司内家属因紧急事宜访问公司，需按如下规定处理：

* Security will record the particular of the visitor and the urgent nature of the visit in the occurrence register. In the event of uncertainty, the Security Manager shall be notified.

保安记录访客的具体信息和来访的紧急事由。遇到不确定情况应请示安全经理

* The staff concerned will be contacted either by phone or direct approach to the department by the Security Officer.

安全员电话联系员工或直接通知部门找到该员工。

* The meeting place shall be limited to the lobby only and the period of the visit is within a reasonable time.

访客家属只限于在合适的时间在访客大厅进行访问

* Security officer should maintain a DISCREET observation distance from the meeting place. This is to make certain that no illicit transaction occurs.

安全员应在离开访客区一定距离的地方监控现场，以防不法的交接。

* + 1. Visitor entry approval application访客入厂核准申请表

The Host Department shall be responsible to complete the ‘Visitor entry approval application’.

This form must reach the Security Department at least 24 hours prior to the visit. The distribution list of the form is as follow:

被访部门有义务完成访客入厂核准申请表，此通知单必须提前24小时提交给安全部门。表格分发清单如下：

* Security Dept安全部
* Front desk前台

It is the responsibility of the person hosting the visit to prepare the form and seek approval from the

shop floor departmental head, as specified in context below.

陪同访问的被访问有义务完成访客入厂核准申请表的填写并且获得相应的批准，具体描述下文可见。

* + 1. Approval for Visitors访问批准

Short Stay Entrance into workshop ---- Host department manager, production department manager and security department manager approval.

进入车间短期逗留需经接待部门经理、生产部经理和安全部经理批复。

All approved application should submit to security control room.

所有批复的申请都应交至监控室。

* + 1. Visit by Service Provider (Consultants, Contractors, Repairman and Technical support) 供应商来访（顾问，承包商，修理工和技术支持）

The application of visit by the SERVICE PROVIDER should be activated by the Host Department.

The form and procedure in respect of the application is similar to that in clause 6.5.4.

服务商的访问申请应有被访部门完成，申请流程同6.5.4的要求。

The approving authority is either the Production Manager or the Security Manager.

授权由安全经理或者生产经理批准。

The department that engages the service provider shall be responsible to ensure that the said company is licensed, reputable and the workers must be sufficiently covered by insurance for their respective trade.

接待的部门必须确认供应商是注册的，知名的公司，并且其工人必须是入保险工作的。

The service provider upon arrival shall report to the Security Control Center. The security officer will

notify the host. A restricted access pass will be issued to him when he surrendered either his passport or ID card to the Security Officer.

供应商到公司时须通知安全监控中心，安全主管通知受访人接待。访客应自觉在安全监控中心抵押护照或身份证件换公司设定权限的门禁卡。

The departmental staff (host) shall accompany the Service Provider at all time while working in the

sensitive zone. The Security Officer shall pay periodical visit to ensure that the service provider is

working within the site and that they are not left unattended by the host.

若供应商在高安全区域进行作业，应有接待者陪同。安全专员须定期巡查，以确保供应商是否在指定的区域作业和防止其在无接待者陪同的情况下作业。

* + 1. Receiving Protocol for Visitors 访客接待流程

When visitor(s) arrive at front desk, the Receptionist will inform the relevant host(s) of their arrival.

当访客达到前台后，前台应负责通知相关人员（被访人）

The visitor(s) shall surrender their Passport or ID card or equivalent personal document to the

receptionist in exchange for the pre-arranged access badge.

访客应用护照，身份证等有效的个人证件提交给前台，换取进入的证件。

The receptionist shall advise the visitor(s) to sign in the Visitor Register to register their visit with the Company.

前台应该要求访客在访客登记薄上登记。

The visitor(s) will remain in the reception area until the departmental host(s) arrives to escort them to the designated site either for discussions or demonstrations or interview or presentation outside the Sensitive Zone.

访客应该在访客大厅等候被访者接待，并在被访者的陪同下到指定区域。讨论，示范，面试以及描述等应该在敏感区域外进行。

The host shall not allow unauthorized visit to other site other than the approved site or allow the visitor to loiter around the facility unattended.

接待者不应让访客进去其他未批准的区域或任其在厂区在无人陪同的情况下闲逛。

On completion of the visit, the host shall escort the visitor(s) to Reception and return the visitor pass to the security control room. Security guard return identity documents and record leaving time, visitor should sign when get the ID document.

接待结束后，接待者应陪同到安全监控中心交换访客证。保安归还抵押证件并做好访客离开时间的记录，访客离开时签字回证件。

* + 1. White Guidelines访客须知

Customers or Visitors and members of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. who have been given permission to enter the Highly Sensitive Zone **MUST** remain within designated walkways.

获得进入高安全区域权限的客户，访客以及澄天伟业（宁波）芯片技术有限公司的其他成员必须在指定的区域范围内活动。

No recording devices or hand phone are allowed in the Highly Sensitive Zone.

在高安全区域，不得使用记录设备和手机。

Supplier’s Service Engineers carrying out maintenance or repair work are NOT allowed to trespass into other sensitive area of operation.

实施修理工作的供应商维修人员不得进入操作区域以外的保安区域。

Security Officer on routine rounds shall ensure compliance. By default, the Service provider or engineer or Visitor’s entry to the site will be reverted until investigate is completed.

安全主管在日常的检查中应确保符合性。若有违反，供应商，维修人员以及访客的访问行为将被终止直到调查结束。

Specific regulations are to be applied for accessing to production sites. Visitors are not allowed to take any sample or production documents. Mobile phones, camera, video, tape or any king of recording are prohibited inside the manufacturing areas.

特殊规定将被应用于访问生产基地。访客不允许拿走任何样品或生产的文件。禁止在车间内的使用移动电话、拍照、录像、磁带或任何记录方法。

* + 1. Confidentiality Agreement保密协议

Customer or Visitor visiting the Highly Sensitive Zone is required to sign Confidentiality Agreement with the Company.

进入高安全区域访问的客户以及访客应与公司签订保密协议。

The Receptionist or Security Officer shall explain to the Customer or Visitor of such requirement.

They shall advise them to read and understand the agreement prior to their endorsement.

前台或者安全主管应向客户以及访客解释我们的要求。他们应向访客建议，在签署保密协议之前，应充分阅读和了解此保密协议的内容。

Customer(s) or Visitor(s) who refuse to sign the agreement for reason best known to them Will be denied access to the Highly Sensitive Zone.

借故拒绝签署保密协议的客户和访客，不得进入高安全区域进行访问。

* + 1. Responsibility访客管理职责

The host must ensure that the visitors are unable to obtain any details or confidentiality documentation with regards to production and machinery procedure that could be of value to our competitors.

被访人必须确保访客不能获得任何对我们竞争对手有价值的关于生产和设备的机密信息和文件。

The Security Staff is responsible to ensure compliance of this document by all parties’ concern with the visit. The Visitor Access Badge must be returned to Security Control Center at the conclusion of

the visit, failing which is the responsibility of the Host Department to recover the badge from his visitor(s). Meantime, the Security Manager will instruct the SCC to de-activate the card immediately.

安全主管应确保访问期间能够充分遵守此文件规定的要求。访问结束后，访客门禁卡被归还至监控室，若访客在结束访问后未归还访客门禁卡、被访人有责任向访客收回访客门禁卡。同时安全主管应立即将此卡的所有权限删除。

The department manager or his designate shall ensure that this document is being adhered to within their area of responsibilities.

部门经理和指定人员应确保此程序规定要求能够在其区域被充分遵守。

* + 1. Quality Record(S) & Retention Period记录和保存时间

‘Notification Of Visitors’ form to Non-Secure will be retained for 12 months.

进入非安全区域的访客通知单将被保留12个月。

‘Notification Of Visitors’ form with Plant Tour inside the Production Shop floor in the Highly Sensitive Zone will be retained for 2 years.

进入车间等高安全区域的访客通知单将被保留2年的时间。

Confidential Agreement shall enjoy immunity.

保密协议将被无限期保存。

* 1. Physical Key Management物理钥匙管理

There are two kinds of physical keys used within the scope of the audit. One is the key used for locking the IT server room rack, which is managed by IT engineer. Another key is for the secure box located in security control room implemented dual control where security officer and a security guard have it.

Whenever an area is locked with physical key, a register of keys should be maintained and all keys

在这次审核范围内的有两种钥匙。一是用于锁IT机房机柜的钥匙，其由IT工程师掌管。而另一种钥匙用于安全控制室里的保险柜，其实行双人控制，由安全员和一名安保共同掌管。

* 1. 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. The UPS can last for 1 to 2 hours.

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。UPS可供电1到2 小时。

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。

* + 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。

* + 1. 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。

* + 1. 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。

* 1. 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。

According to company policy, high security areas must be protected by infrared detection alarm system and delayed alarm system. There are four areas which are defined as the high security areas and they are also included in this audit scope. There are vault, security control server room, IT server room and card scrap room within the packaging workshop.

根据公司政策，高安全必须由红外摄像探测报警系统和延时报警系统保护。有4个区域被定义为高安区，分别为金库、安全控制机房、IT机房和封装车间的碎卡室。

All the emergency exit doors are equipped with alarm system, once the door is open it will trigger the alarm then security guard will use CCTV camera to check if the alarmed locality and find out if there is unauthorized entry or exit. If there is then security guards will respond immediately.

所有的应急消防门都配备有报警系统，一旦门被打开，即会触发报警之后安保会通过CCTV摄像头查看报警地点，探查是否有未授权出入。如果有，安保会立即响应。

Power supply of the alarm systems are backed-up by UPS and when there is an emergency its capacity can last for 1 to 2 hours.

报警系统的电力供应由 UPS支持，当紧急情况发生时，它的电力供应可持续1到2个小时。

* + 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。

* + 1. 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手动：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
  + 1. 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。

* 1. Power Supply 电源供应

Independent power supply lines must be set up for the physical security facilities, where is equipped with standby power supply. UPS is deployed for supporting CCTV, alarm system and access control system and it can last for 1 to 2 hours. An electricity generator is used for powering access control system, CCTV and alarm system once UPS runs out its power.

独立的电力供应必须提供给物理安全设施。UPS已部署用来支持CCTV、报警系统和门禁系统而且能够持续1到2个小时。发电机用来给门禁系统、CCTV和报警系统提供电力支持以备UPS用完电量。

* 1. Inspection for Physical Security Facilities 检查物理安全设施

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
* Vault locking mechanisms (once people get out and lock the door, the infrared detection alarm system will be activated automatically) 高安全存储区的锁定机制 (一旦人员撤离并锁上门，红外探测报警系统会被自动激活)
* 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 security committee personnel monthly. A copy of the inspection report must be maintained for at least 18 months and presented to auditors on request.

这种每月的检查必须有安全小组人员来完成。一份检查报告必须保存18个月，而且能够呈现给审核员。

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。

* 1. 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 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。

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）。

* 1. Goods storage and Vaults货物存储和仓库
     1. 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.

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。

It must be be alarmed and locked when nobody is inside (movement detectors) and covered by CCTV system. See also.

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。

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。

Vault is equipped with delayed alarm system which means if the door keeps open for a certain time, it will trigger the alarm.

金库配备了延时报警系统，如果门开着保持一段时间则会激活报警。

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

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。这种双重控制同时应用于进出。

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

* + 1. Card scrap room碎卡室

Card scrap room is defined as the high security area.

碎卡室属于高安区。

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。

* 1. Secure Box保险柜

The use of secure box is mandatory to store sensitive information or media as specified in the Information Security Classification Policy. Dual control is used for the secure box.

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。双重控制应用于保险柜的使用。

Only security officer and a security guard in the security control room have the key. The secure box is located in security control room.

只有安全员和一个安全控制室的安保有保险柜的钥匙。保险柜位于安全控制室。

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。

* 1. Receiving 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。

Door 1, 2, 3 must operate on an interlocking basis that allows only one door to be opened at one time.

门必须允许只有一扇门一次打开互锁基础上运作。

The first door is managed by security control room and the other two doors are managed by delivery related staffs.

第一扇门由安全控制室管理而另外两扇门由收发货区员工管理。

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 3 must also be protected by an In and Out access 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 4 for 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 out on 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。

1. Security Control of Documents 文件的安全控制
   1. Controlled Document Management 受控文件管理

The contents and provisions of all documents, and their distribution and keeping must satisfy the security requirements and regulations, without any conflicts with the security regulations.

所有文件的内容、规定及其分发、保管必须符合安全要求和规定，不得与安全规定冲突。

The storage mechanism for the private or above level of documents must be in place.

必须具备内部或以上级别文档的存储机制。

The document formulation, management, modification, storage, invalidation and destruction should follow the relevant procedure.

文件的编制、管理、修改、保管、失效和销毁应遵循相应的程序。

Useless paper or documents should be put into the shredder. There is a shredder in the packaging workshop.

无用的纸张或者文件应该放入碎纸机。封装车间有一个碎纸机。

Documents related to the DSS are subject to Documentation Control and Configuration Control.

与DSS相关的文档遵从文档控制和配置控制的要求。

1. Logical Security Management 逻辑安全管理
   1. General Principle总则
      1. IT Physical Security 信息技术物理安全

Servers systems are 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。

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 VLAN logically. Network for Security Control System are physically isolated.

办公网络与生产网络通过虚拟局域网隔离，安全控制系统网络在物理上是独立的。

* + 1. 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 performed by IT engineer and approved by security manager.

所有防火墙规定的修改通过IT工程师操作由安全经理批准。

* + 1. IT System Security 信息系统安全

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 computer 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。

There are three types of computers used within the packaging workshop:

封装车间里使用三种电脑：

* ERP computer is the computer installed ERP system which is aimed for production assistance. This computer is located in the workshop and connected to the internet. But it has strict control on the usage of network.

ERP电脑是安装了用于生产辅助的ERP系统的车间电脑，此电脑接入互联网但是有严格的网络使用控制

* Git computer is the computer installed Git for the purpose of the configuration management. The computer is connected to the production network VLAN which is not allowed for accessing internet.

GIT电脑是安装了用于配置管理的GIT系统的车间电脑，此电脑连入生产网络的虚拟局域网即不可访问互联网

* Production machine equipped computer is the computer participating the production process and storing production data, this kind of computer has no physical connection

生产机器电脑参与生产流程并存储生产数据，此电脑没有物理连接

* 1. Network Security 网络安全

Network is to be defined and separated according to the function / usage.

网络是通过功能及用途来进行定义与分隔的。

Keep an updated network topology that includes all system components of the network, to ensure correct evaluation and update to the network topology.

保留一份最近的包括网络中所有系统组件的网络拓扑图，确保适当时对网络拓扑图进行评估和更新。

Applications and systems with sensitive, critical, or very critical content shall not run in shared environments.

携带敏感、机密或者高机密内容的应用和系统禁止在共享环境内运行。

There shall have a set of agreement for network services provided in-house or outsourced. The agreement needs to detail and identify the security features, service levels and management requirements.

需要有一组内部或外包的网络服务协议。协议需要详细说明和确定安全特性、服务级别和管理需求

* + 1. Network Structure 网络结构

**Office Network办公室网络**

The office network allows using Internet, however, to limited business uses. Office network cannot access to production network for any data.

办公室网络是允许可以使用网际网络，但限于营业的使用。办公室网络不得于生产区网络存取资料。

**Production Network 生产区网络**

Production area network cannot connect with the Internet or any other networks, including business and admin networks.

生产区网络不得与互联网或其他网络相连接，包括公司的办公网络。

**Public Server Network公用服务器网络**

AD Server and File Server are all devices in public server network. They are protected by the internal firewall system. All servers of public server network are not for internet use, only for internal company use.

AD服务器、档案服务器都放在共用服务器网络，并受保护于防火墙系统，共用服务器网络不对外开放，仅公司内部使用。

**Customer Network顾客网络**

We propose customers to use encryption methods to protect the transmission of files. Customer can use the encryption methods of Shanghai Chengtian Smart Card Co., Ltd to protect data security. Customers can still choose unsafe manner, transmitting level 3 or level 2 files, but Shanghai Chengtian Smart Card Co., Ltd has the obligation to inform customer of the relevant risk and keep relevant logs and records for viewing by auditors during audit.

客户传输的档案资料，建议要加密处理，可透过安全的加密传输程序。客户仍可以选择不安全的方式传输档案，但宁波澄天伟业芯片技术有限公司有告知客户相关风险之责任，并将有关日志存档，在审计时让审计师过目。



Figure 3 Company Production and Office network [topological](javascript:;) [graph](javascript:;)

The wireless network is not deployed for the plants.

车间内没有部署无线网络。

* + 1. Firewall 防火墙

#### Firewall Management and Configuration Strategy 防火墙管理和配置策略

Firewall configuration default rule forbid all service. The rule must be set up according to the principle of restricting all access and allowing only those services, protocols and ports necessary.

防火墙设置缺省规则为禁止，必须依据关闭所有访问权限，只让必要的服务或端口通过的原则。

All the pc in the production network must set their IP in the firewall and under the control by the firewall. Forbid any connection from external to any internal zone. Firewall must prohibit servers that only need inbound connections to make outbound connections.

生产网络中的所有电脑的IP 必须设定到防火墙中，受到防火墙的控制。禁止任何从外部网络至内部网络的访问。

不需要向外传输资料的服务器必须有防火墙禁止它们作从内向外的连接。

The firewall policy and configuration must be accurately documented.

防火墙的设定记录必须详细文件化。

#### Firewall Audit 防火墙审核

Any change in firewall settings must be handled according to procedures. The procedure is operated by IT engineer and approved by security manager. The procedure needs to follow the 4-eyes principle.

任何防火墙设定变更都必须依据程序处理，流程由IT工程师操作由安全经理批准。防火墙规则变更过程中需遵循四眼原则。

The firewall machines must be subject to regular monitoring and yearly audits. The IT engineer check the firewall rule monthly and sends it to security manager for approval.

防火墙设备必须遵从定期监测和年度检验。IT工程师每个月进行一次防火墙的规则审查并将之发送给安全经理审批。

Users and firewall administrators should be aware of their responsibilities and be educated so that they can assume these responsibilities. Only firewall administrators are allowed to perform administration activities.

使用者及防火墙管理员应注意到他们的职责，并且受到培训，这样才能正确运用他们的职责。只有防火墙管理员能够进行管理活动。

Logs should be archived for at least one year.

日志至少必须保存一年。

#### Use Area of Firewall 防火墙使用区域

Configure a firewall between the Internet and the official network.

在因特网和办公网之间配置防火墙。

#### Main functions of firewall防火墙主要功能

1. 入侵防御与Web防护 IPS and Web protect

Get the latest threat information at the first time, accurately detect and defend attacks against vulnerabilities. It can protect against a variety of attacks against the web, including SQL injection attacks and cross site scripting attacks

第一时间获取最新威胁信息，准确检测并防御针对漏洞的攻击。可防护各种针对web的攻击，包括SQL注入攻击和跨站脚本攻击等.

1. 数据防泄漏 Data leakage prevention

By identifying and filtering the transferred files and contents, you can accurately identify the real types of common files, such as word Excel, PPT, PDF, etc., and filter the content.

对传输的文件和内容进行识别过滤，可准确识别常见文件的真实类型，如Word、Excel、 PPT、 PDF等，并对内容进行过滤。

1. 应用识别与管控 Application identification and control

Identify common applications, access control accuracy to application functions. Application recognition and intrusion detection, anti-virus, content filtering

Combined with this method, the detection performance and accuracy are improved.

可识别常见应用，访问控制精度到应用功能。应用识别与入侵检测、防病毒、内容过滤相结合，提高检测性能和准确率。

1. URL过滤 URL filtering

More than 120 million URL classification libraries can speed up access to specific categories of websites and guarantee the access experience to high priority websites.

Support DNS filtering, directly filter the visited web pages according to the domain name.

Support for SafeSearch, filter the resources of Google and other search engines, and ensure access to healthy network resources

URL分类库超过1.2亿，可对特定类别网站的访问进行加速，保障对高优先级网站的访问体验。支持DNS过滤，直接根据域名对访问的网页进行过滤。支持safesearch，对google等搜索引擎的资源进行过滤，保障访问健康网络的资源。

* + 1. Virus Control 病毒控制

ANTI-VIRUS Software反病毒软件

Against intrusion and infection by virus, antivirus software (McAfee Endpoint Security) must be deployed on all Chengtian Weiye (Ningbo) Chip Technology Co., Ltd networks. 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。

Except production machine computer that maintained by equipment supplier, other computer such as production computer, office computer and ERP computer are maintained by IT engineer. IT engineer will push the update of the anti-virus software to the domain account user through the anti-virus software server deployed in IT server room. This operation is done by IT engineer and approved by security manager. The update frequency is per month.

除了生产机器电脑是由设备供应商维护外，其它的电脑如生产电脑、办公电脑和ERP电脑都由IT工程师来维护。IT工程师会通过IT机房内部署的反病毒软件服务器来给域用户推送反病毒软件的更新。这个过程由IT工程师来操作由安全经理批准。更新的频率为一个月。

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。

* + 1. Terminal Access 终端访问

#### Desktop Clear桌面清理

Files containing confidential information or important information, records, disks, discs, or other forms of storage media should be locked into a filing cabinet or a safe when a person leaves. Prevent from being obtained by unauthorized person

含有涉密信息或重要信息的文件，记录，磁盘，光盘或其他形式存储的媒体在人员离开时，应锁入文件柜或保险柜等。防止被未授权人获取。

#### Computer Screen Lock 电脑屏幕锁定

Computers which are left unattended or the user leave shall be protected by user logging off or activating a screen lock with password enabled. User is not allowed to deactivate the any screen lock/saver settings. Screen protection time is not more than 5 minutes.

The internal auditor checks whether the computer is locked according to the requirements during the monthly internal audit.

电脑一段时间无人使用时或使用者离开，使用者必退出或设定进入有密码保护的屏幕保护状态，使用者不得关闭屏幕保护设定。屏幕保护的时间不大于5分钟内审检查人员在每月的内审检查中，检查电脑是否按照要求进行锁定。

* + 1. System Maintenance 系统维护

The WSUS（Windows Server Update Services） module is configured on the domain control server to control the group policy of the domain to issue update source, plan cycle and restart time. Group policy is named update and configured to accept update notifications for non-administrator users.

通过在域控服务器上配置WSUS（Windows Server Update  Services）模块，调控域的组策略下发更新源，计划周期和重启时间等。组策略命名为update并且配置为非管理员用户接受更新通知。

Except for production machine computer that maintained by equipment supplier, office computer, production computer and ERP computer are all maintained by IT engineer. IT engineer will push the system update to the domain user monthly through WSUS deployed in server located in IT server room. This operation is done by IT engineer and approved by security manager.

除了生产机器电脑由设备供应商维护外，办公电脑、生产电脑和ERP电脑由IT工程师来维护。IT工程师会通过部署在IT机房的WSUS每个月来给域用户推送更新。操作由IT工程师完成经由安全经理批准。

IT engineer will monthly check the use of hardware resources in production computer, production machine computer, ERP computer and server located in IT server room. make sure the resources are not depleted and there is no abnormal incident or unauthorized installation of software. IT engineer will leave a record for the maintenance.

IT工程师每个月会检查生产电脑、生产机器电脑、ERP电脑和位于IT机房的服务器的硬件资源利用情况。确保资源的使用没有耗尽而且没有非正常事件出现或未授权软件的安装。IT工程师会留下维护记录。

#### Update test 更新测试

The IT department keeps a special testing machine and issues the update configuration to the testing machine before issuing the update in batches. After the testing machine updates the patch and confirms that there is no system problem, it issues the update patch in batches to other terminals.

IT部门留用一台专用的测试机，在批量下发更新之前先下发更新配置给测试机，测试机更新补丁之后确认没有系统问题以后再将更新补丁批量下发给其他终端。

* + 1. Backup and Disaster Recovery 备份以及灾难恢复







Backup 备份

**Server system backup服务器系统备份**

Server in the IT server room deployed domain management service, anti-virus software service and system update service is using two system HDD, which means if one of the system HDD is broken then another system HDD can be used immediately.

IT机房的服务器部署了域控管理服务、反病毒软件服务和系统更新服务。这个服务用用两块系统硬盘，意味着一旦其中一块出了问题另外一块能够立即提供服务。

**CM repository backup配置管理系统备份**

Configuration management system is deployed in production computer. The backup of CM repository is done by IT engineer and approved by security manager. Backup frequency is per month. Use PGP encryption to encrypt data before storing it in the removable HDD. The removable HDD will be transferred to secure box in security control room following 4-eye principle.

配置管理系统部署在生产电脑。配置管理系统库的备份由IT工程师操作经由安全经理批准。备份频率为一个月。在储存备份到移动硬盘前使用PGP加密数据。移动硬盘在转移到安全控制室保险柜的过程中遵循四眼原则。

**Production data backup生产数据备份**

The backup of production data stored in production machine computer is performed by the operating system backup. The backup is done by IT engineer and approved by security manager. Backup frequency is per month. The removable HDD storing the backup will be transferred to secure box in security control room following 4-eye principle.

生产数据的备份是通过生产机器操作系统的备份实现的。备份由IT工程师操作经由安全经理批准。存储备份的移动硬盘在转移到安全控制室保险柜的过程中遵循四眼原则。

**Firewall configuration backup 防火墙配置备份**

Firewall configuration backup is performed by IT engineer and approved by security manager. The backup is encrypted and transferred to a USB driver that transferred to secure box in security control room following 4-eye principle.

防火墙配置的备份由IT工程师执行由安全经理批准。备份加密后传输到USB存储器，然后遵循四眼原则转移到安全控制室的保险柜中。

#### Restore Procedure还原程序

A notification must be issued to all department and employee about the detailed restore information, regarding status, content, schedule and so on. IT engineer should get the related media to perform the restore.

进行还原程序前须发给所有部门及员工详细的资料还原信息，内容关于状态、还原内容、日程等等。IT工程师应该取得相关的媒体执行还原工作。

Restoring for production data on production computers or production machine computers must be performed by IT engineer and IT assistant . CCTV must be active during the whole process of restoring to enable traceability.

在生产区档案服务器还原生产的资料，必须由生产区IT工程师和IT助理。 CCTV必须全程录影所有还原的动作以供日后追踪用途。还原的数据要做好相关记录。

#### Handling of Backup Media备份媒体的处理

All offline backup media of production data must be stored in secure box in security control room and must be kept all the time.

生产区资料的所有离线备份媒体必须完整保存于主要的安全控制室的保险柜中。

During transferring backup media, a 4-eyes-princple must cover the whole procedure. Security guard should be with ITengineer. After the procedure is performed, a form Media Handover log must be filled out. The identification of media must be traceable by filling Removal Storage Registration

在备份媒体转移过程中，整个程序必须包含四眼原则。安全人员应陪同IT工程师。在完成这些程序之后，必须填写媒体移交日志。媒体确认时必须填写“可移动存媒登记表”并可以用于追踪。

* + 1. Software Management 软件管理

#### Software installation process 软件更新流程

Only production needed software can be allowed to be installed on production computer.

只有授权的与生产需求相关的软件才被允许安装到生产电脑上。

Only business needed software can be allowed to be installed on office computer.

只有与商业需求相关的软件才能被允许安装在办公电脑上。

The installation is performed by IT engineer and approved by security manager. 4-eye principle needs to be followed during the installation.

安装由IT工程师操作经由安全经理授权。安装过程遵循四眼原则。

#### Special software installation approval process 特殊软件安装审批流程

For the production machine computers supporting individual workshop equipment, special unconventional software provided by some suppliers shall be installed. The department head of workshop equipment shall apply for it, and then the IT department shall log in to the local administrator for installation after being approved by security manager .

针对个别车间设备配套的电脑需要安装一些供应商提供的特殊非常规软件，需要由车间设备所属的部门主管提出申请，经过安全经理审批之后再由it部门进行登录本地管理员进行安装。

#### General rules通用规则

All computers are under AD domain control. The assigned domain account does not have the right to install the software. The software can only be installed through the local administrator account. The administrator account password is controlled by the IT department and cannot be disclosed to other company employees.

所有电脑都加入ad域管控，分配的域账户没有安装软件的权限，只能通过本地管理员账户安装软件，管理员账户密码由it部门管控不能透露给其他公司员工。

#### Production area computer生产区电脑

It is forbidden to install Wechat, QQ and other communication software on computers in the production area, and to install AutoCAD, office365, Foxmail and other office software in a unified way. According to the needs of individual equipment connecting computers, IT department implements the installation of personalized production software.

生产区电脑禁止安装微信，QQ等通讯软件，统一安装autocad，office365，foxmail等办公软件。根据个别设备连接电脑需求由it部门实施安装个性化生产软件。

#### Patrol inspection 巡检核查

The IT engineer needs to check the system and software installation and uninstallation of anti-virus software of all the computers of the company every month. When it finds that the computers installed with software inconsistent with the regulations are confirmed with the relevant departments, it will talk about software deletion to standardize the system.

IT工程师每个月需要对公司所有的电脑的系统和软件安装进行一次核查，发现安装了与规定不符的软件的电脑后与相关部门确认后，再讲软件删除，使系统标准化。

* 1. Logical Access Control 逻辑访问控制
     1. Logical Access 逻辑访问

A set of procedures must be created for the request to access to an operating system.

必须建立一套程序，用于对访问计算机系统的请求。

Requests for logical access are approved by the applicant's manager and the system and/or data owner, authorization is implemented by the IT engineer following four-eye principle.

逻辑访问请求由申请人的经理和系统和/或数据所有者批准，授权由IT工程师在四眼原则下实现。

Access permissions can not to be provided before the appropriate authorization procedures have been completed.

在未完成适当的授权程序之前不得提供访问许可。

The details of the authorized users and user accounts must be kept in a unified list as a reference that is independent of the system itself and the list should be reviewed regularly.

经授权的用户以及用户帐户的详细情况必须保留在一张统一的清单内，作为一种参考独立于系统本身并定期进行检查。

For the systems or sensitive computer applications, which can be accessed by password authentication, the login behaviour of users must be controlled. The system or the application will be locked after several failure attempts and will be log out after a while if no one uses it.

通过用户名和密码进行身份验证后方能访问的系统或敏感电脑应用，对用户登录行为必须进行控制。在多次失败尝试之后，系统或应用程序将被锁定，而如果没人使用，系统或应用程序将在一段时间后注销。

Access control must be in place to prevent unauthorized connection to the secure network, including the implementation of port level security. Systems with sensitive, critical, or very critical content have a dedicated (isolated) computing environment.

访问控制必须到位以防止产生未授权连接安全网络，包括执行端口级别安全。包含敏感、机密或高机密内容的系统应具有专用的（隔离的）计算环境。

The supplier's activities shall be monitored.

供应商的访问活动应受到监视。

* + 1. User Account Management使用者帐号管理

#### Identifying Users识别账号

Each individual user is responsible for all activities performed under his or her User ID.

All the user accounts need to application, approval before creating. Assign the role permissions by “because of the need to know” and User Account Access Matrix, deny all the access by default except have any special permit. Every Level User have their access privilege, if the apply form permission out the User Account Access Matrix, which should be approval by the security manager.

每一位个别的帐号权限及执行活动都依据他/她的指定帐号。所有用户获得权限必须通过申请，审批，分配权限时根据权限矩阵表按照”因需知晓”原则，除非获得特别许可，缺省情况下拒绝所有访问，各级别用户具有相应的访问权限和责任。如果申请表的权限超出权限矩阵表，那需要安全经理确认后才能授权。

All User IDs are logged and traceable for every log on/off.

所有的帐号登入拜访的记录都能够被追踪。

User IDs are never re-used for different/new employees.

账号不能共享

The company divided user into two kind of type according the network user’s privilege and access control. the user needs to choose the type when application the user.

1) Administrator User: Manage and deploy all the system resource

2) General User: Use some system resource and do some special function

访问网络的用户根据权限大小和对网络资源访问控制，将用户分为如下两种类型，申请用户时需选择相应的用户类型：

1）管理员用户：负责管理和分配所有的系统资源的用户。

2）普通用户：使用某些系统资源和实现特定业务功能的操作用户。

Accounts (User ID) that has been inactive for 90 days must be suspended from the system. Accounts need to be deleted if still have no any activity after suspended 30 days.

一个帐号若超过90天没使用，必须从系统中停权。停权30天后仍未使用的账号应予以注销。

Forbid remote logon (remote dial or VPN) operate.

严格禁止远程登录（远程拨号或VPN）操作。

#### User Account Application账号申请

User account must ONLY be created and activated after the User Account Request Form is filled and submitted by HR department.

使用者申请表格填写好后，经由人事部门的传递，帐号才能被启用。

The User Account Request Form is a basic information form that records user’s information, whenever user’s information is to be changed, or, he/she is going to be transferred between departments, HR department must release a new form to indicate the modification.

使用者帐号申请表是一个基本的信息表，记录使用者的信息，每当使用者的信息异动或部门职务转换时，人事部门必须更新相关信息及修正。

#### User Account De-active账号停用

When an employee has quit from the company, HR department must inform IT department as soon as possible, the IT department must de-active the user’s account on every network within one working day.

当员工辞职离开公司，人事部必须尽快通知IT部门。IT部门则必须在一天之内完成停权的执行动作。

#### User Account Checking账号检查

The IT engineer checks monthly if there are abnormal user account in the domain pc and check if the account privilege has been changed without authorized. User access right list will be sent to security manager for review.

IT工程师每月检查一次域控电脑中是否存在非法用户，用户账号的权限是否被非法更改。用户权限列表会发给安全经理审核。

#### User Account lock and unlock账号锁定与解锁

The system will lock the user account if the user input the wrong password continue 3 times When the user logon the system. lockout duration must be at least 30 minutes for all systems, or until the IT engineer unlocks it. The account holder needs to fill the account unlock applicate form. IT engineer unlocks the account after approval and inform the account holder.

用户登录系统，连续3次密码输入失败后，锁定该用户的账号，账户锁定期限至少必须在30分钟以上或账号持有人需填写账号解锁申请表，经过审批后，由IT工程师对该账号进行解锁，并由IT工程师通知该账号的持有人。

#### User Account delete账号删除

Auto freeze the account which don’t have any activity in continue 90 days. Written off the account have not any activity after freezing 30 days.

自动冻结连续90天未使用的账号，冻结后30天仍未使用的，对该账号予以注销。

* + 1. Password Management 密码管理

The password is used with user ID to uniquely identify all users prior to allowing access to system resources.

密码是用来与用户识别的独特识别所有用户之前允许进入系统资源。

The following lists Ningbo Chengtian Chip Technology Co., Ltd. standards for passwords.

下列为宁波澄天伟业芯片技术有限公司密码标准规范。

1. All passwords used within Ningbo Chengtian Chip Technology Co., Ltd network(s) are static passwords whereby users are required to remember. The following lists the standard policies with regard to passwords and accounts.

所有密码使用宁波澄天伟业芯片技术有限公司网络的静态密码,用户使用者必须记住个人的帐号密码。下面列出的标准方面的政策，密码及帐户。

1. System assigns initial password and user must change on first use. Initial passwords are random and not common through all users. If it is updated/upgraded from old password, the current old password must be authenticated before allowing any new password to become effective. Newly set passwords must meet complexity requirements and must pass the dictionary check function. The dictionary check function may be implemented via software.

分配制度的初始密码和用户必须改变对首次使用。初始密码是随机而不是通过共同所有用户。如果是更新/升级，从旧密码，目前旧密码必须认证才允许任何新密码生效。新设的密码必须符合复杂性要求并通过字典调查。字典调查功能可由额外软件提供。

1. Passwords are to be changed at least once in 30 days for production network and office network.

密码的修改，生产区网络与办公室网络需于30天内修改。

1. Password shall not be reusable for 5 expiry cycles.

密码于最近5次内的循环使用不得再用。

1. Minimum password length is 8 alphanumeric characters.

最小密码长度是8个英文字母。

1. Users are briefed to use passwords that are not easy to guess and derive. No writing down of passwords is allowed. Passwords are encrypted when transmitted over networks. Passwords cannot be the same as the user ID, and must have at least 3-character complexity out of 4 character types, namely lower-case, upper-case, numerals and symbols.

帐号用户使用简单的密码，但不易猜出及连想，只要没有另外记录书写是允许的。当密码传输时，必须经由加密处理。密码不可以和用户识别一样，并要有四种字符的至少三种：大写，小写，数字，符号。

1. Every personnel shall be fully responsible for their user password and keeping it confidential.

每一个帐号拥有者必须全面负责他们的用户密码并保持机密。

1. Passwords stored must be protected with strong encryption methods and never shared, available or known to others, including administrators. No password is to be displayed in clear when it is being entered. Password shall not be shared or kept on paper. Password shall not be stored in any medium in clear, macro, function key or any auto logon script. Password may only be kept in tamper-evident sealed envelope if necessary.

密码的保存必须是受到保护的加密方式、没有共享或其他可能性提供给其他人知道，包含系统管理员。正在登入系统时，密码是不可以显示出来的。密码不允许被公开或记录在纸上。密码也不得记录于未加密的储存媒体或任何自动登入的程序。如果有需要的话，密码只能保存于密封的信封袋。

1. If any password is compromised or suspected to be compromised, the account is immediately locked until the User ID and password are changed.

如果怀疑密码可能失窃或受到损害时，帐号需立即锁定，直到帐号和密码改变。

1. Access rights shall only be granted on authorized need basis. User access into unauthorized folders or files is strictly prohibited.

系统存取权必须只能允许在基本的授权上。未经授权的存取资料夹或档案是被禁止的。

1. User accounts are locked after 3 failed log-on attempts with password.

密码经过三次尝试登入错误时，用户帐户必须被上锁。

1. User accounts are locked when the respective employee leaves the company and deleted upon completion of leaving clearance.

当个别的职员离开公司或暂时停职离开其职位时，帐户必须被锁。

1. In case of reset password or unlock account, the user must the department manager and the IT manager must approve it before the password is to be reset.

上述为例，如需要重置密码，解除帐户锁定时，用户必须经由相关部门经理及IT部门经理的同意，密码才能重新设定并重置。

1. Password lockout duration must be at least 30 minutes for all systems, or until the administrator unlocks it.

所有系统密码锁定期限至少必须在30分钟或以上，或直到IT部门的管理者解锁。

1. If the password of the account is hold by two personnel, each part password should match the complexity.

如果一个账号的密码由两个人共同持有，每个人设定的密码部分也需满足密码的复杂度。

* 1. Data Security 数据安全
     1. Software introduction软件介绍

PGP is the abbreviation of English pretty good privacy. It is an encryption software series based on RSA public key & private key and AES encryption algorithm. The commonly used version is PGP desktop professional, it includes mail encryption and identity confirmation, data public key & private key encryption, hard disk and mobile disk password protection, network sharing data encryption, PGP self-extracting document creation, data security erasure and many other functions.

PGP是英文Pretty Good Privacy (更好的保护隐私)的简称，是一个基于RSA公钥&私钥及AES等加密算法的加密软件系列[1]。常用的版本是PGP Desktop Professional(PGP专业桌面版)，

它包含邮件加密与身份确认，资料公钥&私钥加密，硬盘及移动盘全盘密码保护，网络共享资料加密， PGP自解压文档创建，资料安全擦除等众多功能。

* + 1. Internal transmission of confidential documents公司内部传输机密文件

When transferring highly confidential files within the company, you can use PGP to create PGP keys to create key rules. You can create private, one-to-one key rules, as well as public key rules. And share the created key to others and expand their own KeyStore. After receiving another PGP encrypted file, the file will be decrypted according to the corresponding key.

在公司内部传输高机密文件时，可以使用PGP创建PGPkeys来创建密钥规则，可以创建私有的，一对一的密钥规则，还可以创建对公的密钥规则。并且把创建的密钥分享给别人，并且扩充自己的密钥库。在接收到别人的PGP加密文件以后会根据对应的密钥对文件进行解密。

* 1. Removable Media
     1. Removable Media Control Policy移动媒体的管制政策

This Policy is applied to all removable storage media and refers to all media that can be used to store data and information that can be moved. These includes but not limited to the following:

这项政策适用于所有的抽取式储存媒体，并可以参照所有的可移动媒体使用于储存资料及资讯。

- portable hard disk, floppy disk, CD-R/RW, DVD-RW, ZIPdisk.

- memory cards (e.g. CompactFlash, SmartMedia, Memory Stick, Micro Drives, etc.)

- PCMCIA slot-based storage.

- USB-based storage devices, digital tapes and etc.

Removable storage media devices also refer to all device drives that controls and can write data and information into removable storage media. These includes but not limited to the following:

可移动储存媒体设备也可参考所有装置、控制、写资料及资讯传输至可移动存储媒体。这范围不限于包含下列：

- portable CD-R/RW drive, floppy drive, PDA, ZIPdrive, MO drive, tape drive, etc.

可携式CD-RW设备、软盘、个人数位助理、ZIP装置、MO装置、磁带机，Ｕ盘，硬盘等其他

The following standard policy is to be followed下列标准政策是应遵循的：

- All removable items shall be controlled items and need to store in a secure box at the security control room.

所有可移动物品应为受管制物品。应当存放在安全控制室的保险柜中。

- All removable items within the premises shall be registered before they are allowed to be used within the premises.

所有现场可移动的媒体应该是事前经过核准登记才能使用

- It is prohibited to bring any of these removable items into or out of the production area or premises, without prior proper authorization.

未经适当授权时，可移动存储媒体携入或带离开生产区或厂房是被禁止的。

- All the removal media must delete all the data information before return to the customer and the removal media which don’t need to use must be destructed following 4-eye principle and leave a record. The records need to be kept at least 1 year.

- 退回给客户的可重复使用存储介质，必须安全规定删除所有数据信息。保存有数据信息的存储介质不再使用时，必须在四眼原则下焚毁或者粉碎，并做好相应的记录，该类记录至少保存一年。

- All non-registered removable items found shall be impounded by the Security Manager or nominated person.

若发现所有非经登记的可移动存储物品，应暂时由安全经理及指定的人保管。

- Non-conformance to the procedure shall be reported. Disciplinary action may be taken at the discretion of the management.

有不符合程序时应立即回报。纪律处分可以斟酌管理。

* + 1. Procedures程序

Normally all the pc in the production network forbid to use removeable media. We forbid the removeable media by the system policy.

正常情况下生产网络中的电脑不允许使用可移动设备。我们通过系统策略禁用可移动设备。

- All removable media items must be registered before they can be used. A registration data sheet must be fulfilled, see form Removal Storage Registration.

所有可移动式媒体物品必须登记，然后才能使用。登记资料表必须确实执行。

- All authorization for transfer of removable items into and out of the production area premises shall be recorded.The responsible person shall obtain the prior authorization before transferring the removable items into or out of the premises. The approving authority shall be either the Security Manager or the head of department(s). The responsible person shall notify and pass the authorization form to the Security Manager or nominated person during the transfer.

所有授权可传输资料的可移动媒体的携入及带出生产区或厂房应有记录。有责任的人应取得事前的授权才能将这些物品携入或带出厂房。有关核准权应由安全经理或是部门主管。有责任的人应通知及递交 授权表格给安全经理或指定的人。

- Network administrator must check weekly the status of removable device against the registration form and virus.

网络管理员必须每周检查这些可移动媒体的状态，预防登记表及病毒。

- On a periodic basis, the Security Manager or nominated person shall check for non-registered removable items within the premises.

在周期的基础上，安全经理及指定的人应检查在厂内未登记的可移动存储物品。

1. Production Security Management 生产安全管理

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

* 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。

Traceability is achieved by barcode in wafer, mapping file indicating each chip by physical axis and lot number in tape.

可追踪性由晶圆上的条形码、定位每个芯片物理坐标位置的对比图文件和条带上的批次号码实现。

* 1. 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。

* 1. 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。

1. Security Incident Management 安全事故管理
   1. Incident Preparation事件准备
      1. Incident Response Team事故响应团队

Effective incident handling may require different areas of responsibility, a variety of skill sets and ultimately the authority to take decisive actions.

有效的事故处理需要不同部门共同承担负责，多种技能的组合能得到最终权威的决定。

The incident response team should be available for contact by anyone who discovers or suspects that an incident involving the organization has occurred.

事故响应团队应该与事故的发现人员进行有效的联系，该事故的发生已经牵涉到组织。

One or more team members, depending on the magnitude of the incident and availability of personnel, will then handle the incident. The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage to the organization and restore normal services.

根据该事故的严重性以及人员的可用性，决定一名或者多名团队成员参与事故处理。事故处理主管负责分析事故数据，决定事故的影响并且进行合适的行动将损害减少的最小并且恢复正常的服务。

Specific responsibilities for handling certain incidents or aspects thereof will request assistance to other departments such as:

处理某些安全事故的时候需要其他部门的协助，如

- IT administrators IT管理员

- Human Resources 人力资源部

* + 1. Incident response process 事故响应程序

The method of response to the incident or weakness should then be decided upon having regard to the goals and objectives that have been decided up.

对事故和薄弱环节的响应应该考虑决定后达成的目的和目标。

Consideration should also be given to the legal implications of the manner in which investigation and resolution of the incident is to be carried out.

在进行事故调查和处理的过程中，应考虑法律方面的影响。

The incident handling and reporting process is presented below. It defines the general approach for security incident management and need to be adapted according to local organization and regulation.

安全事故的管理途径必须适应当地的组织和规定。

* 1. Incident handling 事故处理
     1. Incident identification and reporting 事故的分类和报告

Any incident that occurs on a site or any suspected security weakness that may have security consequences must be reported within the same day to the Security Manager or to IRT using a security Incident Form.

任何可能有安全影响的事故或者疑似事故发生后，必须在当天使用安全事故汇报表格向安全经理汇报。

* + 1. Impact assessment 影响评估

An impact assessment has to be performed by the IRT in collaboration with whoever reported the incident. The object of the impact assessment is to categorize the incident, determine its likely impact and allocate the most appropriate resources to handle it. The impact level is assigned indicating the seriousness of the incident as follow:

事故负责小组将与事故汇报人一起评估事故的影响。影响评估的目的是对事故进行分类，以在事故处理中分配最合适的资源。影响水平就事故的重要性被分为:

- Critical = Very High Impact Level: The incident will seriously affect elements of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd. resources or reputation and will require immediate action. It could lead to the loss of a customer or of a certification.

Any incident involving law enforcement agencies will automatically have a Very High Impact level.

- 严重=非常高的影响水平：此事故将对澄天伟业（宁波）芯片技术有限公司的部分资源和声誉造成严重的影响，并需要立即的行动响应。该事故可能会造成客户和认证的丢失。任何涉及执法机构的事故都被自动定义为非常高影响水平。

- Major = High Impact Level: The incident affects elements of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd resources and should be dealt with as soon as possible. It could lead to a customer loss of confidence or certification suspended.

- 重要=高影响水平：该事故对澄天伟业（宁波）芯片技术有限公司的部分资源造成影响，并应尽快处理。此事故可能会使客户丧失对我们的信心，以及认证机构的怀疑。

- Minor = Low Impact Level: The incident will not immediately affect any element of Chengtian Weiye (Ningbo) Chip Technology Co., Ltd resources but requires corrective action and should be monitored in case the impact level changes.

微小=低影响水平：此事故不会对澄天伟业（宁波）芯片技术有限公司任何资源造成立即影响，但是需要采取整改措施并且应随时监控防止影响水平的改变。

After this evaluation, the IRT can decide of immediate local action plan. It may include the immediate production stop for investigation.

评估完成后，事故负责小组应该决定进行本地行动计划。包括立即停产以便调查。

Any communication about the event – internal and external – is managed by the Sales and Security teams.

任何关于事故的交流-内部和外部-由市场部和安全团队负责。

* + 1. Incident containment 事故控制

Containing the incident is the top priority. It should ensure no propagation, change or disappearance before it can be dealt with. The steps that need to be performed will obviously depend on the nature and impact of the incident and will include some or all of the following:

有限考虑事故的控制。确保在处理之前，无传播、改变以及消失。其他需要进行的步骤取决于事故的本质和影响，包括如下：

- Remain calm - Work methodically, do not rush;

保持镇静-有条不紊的工作，不急促

- Preserve as much evidence as possible;

保护尽可能多的证据

- Minimize disruption of resources and prevent further damage;

将对资源的破坏减小到最少，并且预防进一步的破坏

- Maintain and restore services, protect sensitive items that may have been exposed as a result of the incident, avoid escalation and further incidents;

维护和恢复服务，保护由于事故而可能导致暴露的敏感项目，避免事故的逐步扩大

- Protect data, including proprietary, managerial and other data;

保护数据，包括专利,管理以及其他数据

- Restrict information, Information should be disseminated on a need to know basis

信息保密，信息应基于在应该知道的人员范围内传播

* + 1. Evidence Gathering 证据收集

Evidence gathering relates to the identification, capture and recording of tangible proofs (photos, printed copy, electronic file, etc relevant to the incident investigation.

证据收集涉及到鉴定，捕获以及记录确实的证据（照片，打印的副本，电子文件等涉及到事故调查的文件）。

It is important to note that the security manager and other authorized personnel have the authority to inspect and to quarantine under special conditions any system that is deemed to be part of an incident investigation.

需要注意的是，若认为是事故调查的一部分，安全经理和其他授权人员有权在特定的条件下检查和检疫任何系统。

Evidence must be gathered in a manner that ensures the integrity of the data and establishes an evidence chain of custody.

证据的收集必须确保数据的完整性以及建立证据的保管链。

Since the process of gathering evidence may lead to the disclosure of sensitive, restricted or personal information only authorized trained personnel may undertake this task.

由于在证据的收集过程中可能导致敏感、机密以及个人信息的泄漏，因此仅允许授权的受训人员完成这项任务。

Certain incidents may require a more rigorous forensic analysis approach to be undertaken. Forensic analysis techniques would be used to discover and record evidence that established the following:

某些事故可能需要更加严密的法律分析以接近受控。法律分析技巧将被用来发现和记录如下建立的证据。

- What happened 发生了什么

- Where it happened 在那里发生

- When it happened 什么时候发生

- Who was responsible 谁是负责人

- How it was done 如何做

Forensic evidence gathering requires that everything be documented in a form that is capable of recreating the exact steps that were followed to gather the evidence. The evidence classified as “Restricted” or “Confidential” must not be altered or contaminated and a chain of custody must be maintained.

法证的收集要求所有事都形成文件的形式，并可以根据这些证据再现事故。证据被分类机密或保密信息，因此不得更改和污染证据，并应该建立证据保护链。

A chain of custody consists in the logs containing dates, times and signatures of the persons who had custody of the evidence.

保护链由日志组成，日志包括日期、时间以及保护证据人员的签名。

* + 1. Eradication and Recovery 根除以及恢复

It will be necessary to fix any issue and consequence associated to the incident and recover any systems and services affected; this might involve:

修复任何与事故相关的问题和结果以及恢复受影响的系统和服务是非常重要的，或许涉及到：

- A forensic analysis if incident and assessment warrants.

如果事故和评估许可，进行法律分析。

- Find a temporary or a definitive solution.

寻找一个临时或者决定性的解决方法。

- Establish post-incident procedures and upgrade standards and procedures if necessary.

如果需要，建立事故张贴程序并且升级标准和程序。

- Re installing operating systems, file systems and user data.

重装运营系统，文件系统以及用户数据。

- Applying all operating system, applications and manufactures recommended security patches.

启用所有的营运系统，应用软件以及生产推荐的安全补丁。

Once all affect have been removed, all issues fixed and all affected systems or services recovered then under the direction of the IRT any containment measures may be removed.

一旦所有的影响被消除，所有的问题被修复，所有受影响的系统和服务被恢复，在事故恢复小组的指导下。所有的控制措施都可消除。

Prior to removing any containment measures the IRT may perform independent tests to ensure that vulnerabilities have in fact been removed or addressed.

在消除所有控制措施之前，事故恢复小组成员应该进行独立的测试确保弱点已经被消除并且被处理。

* + 1. Follow up Analysis跟踪分析

The follow up analysis is intended to provide a detailed incident report, archive evidence, review the incident handling process, gauge its effectiveness and learn from the experience; in particular;

跟踪分析的目的是提供详细的事故报告，归档证据，回顾事故处理流程，评估有效性以及学习经验，尤其是：

- Collate and secure all documentation and evidence.

整理和确保所有的文件和证据

- Produce reports to include: 报告包括

 Actual impact assessment, 实际影响评估

 Actions taken, 采取的措施

 Follow up actions to eliminate or mitigate weaknesses.跟踪措施以消除或者减轻弱点

- Identify lessons learned and any changes required to Chengtian Weiye (Ningbo) Chip Technology Co., Ltd Policies or procedures.

确定经验学习，以及按需要改变的澄天伟业（宁波）芯片技术有限公司方针和程序。

It is the responsibility of the IRT to ensure that a proper 'follow up analysis' is conducted and that all evidence is securely stored. In most cases it will be necessary to archive all incident reports and original and backup copies of evidence collected.

事故应急小组有责任确保跟踪分析的实施以及所有证据被安全的保存。在大多数情况下，有必要对所有的事故报告，收集的原始和复制证据归档。

Under exceptional circumstances it may be necessary to destroy some of the material collected and this must be done using secure disposal methods

在特定条件下，销毁部分材料是必要的，同时销毁方式必须是安全的。

* 1. Incident Report And Closure事故的汇报和关闭

A monthly reporting of security incidents or weaknesses with action plan and current status is sent by each site to the Sites Security Coordination Team. This tracking report process aims:

每月所有站点都应向地区安全协调团队汇报有整改措施的安全事故和弱点以及目前的状态，此跟踪报告的目的是

• To strengthen all incidents.

加强事故教育。

• To highlight recurrent traceability incident.

强调经常发生的事故。

• To emphasize common issues between two or several sites.

强调在2个或者更多地区中的普遍问题。

1. Risk Analysis & Business Continuity 风险分析与业务连续性
   1. Risk Analysis 风险分析

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 protect 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。

* 1. Business Continuity 业务连续性

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:

1. Initiation of BCP framework and deployment 建立BCP架构和部署
2. Critical assets identification and Control主要资产的识别和控制
3. Emergency Response and Operations应急响应和运作
4. Developing and Implementing Business Continuity Plans发展和实施可持续性发展计划
5. Awareness and Training Plans

For more information, please refer to “BCP Control Procedure”.

请参考《BCP Control Procedure企业持续营运-应急计划管制程序书》。

1. 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。

* 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。

The inspection must be carried out by auditor or auditing team of the relevant operators or supervising personnel in other separate area.

检查必须由相关操作人员或其他独立领域的监督人员的审核员或审核组进行。

The report about the non-compliance items found in the audit should be submitted to the audited department and should be required to be improved before the specified deadline; the security committee are responsible for tracking, inspection / confirmation; if the non-compliance items are not closed in time, the security committee should repeatedly report to the management, and continue to track, until the non-compliance items are closed.

审核中发现的不合格项，应当向被审核部门提交报告，并令其在规定的期限内予以改进；安全委员会负责跟踪、检查/确认；如果发现不符合规定的项目没有及时关闭，安全委员会应反复向管理层报告，并继续跟踪，直至不符合规定的项目关闭为止。

The significant non-compliance items must be reported to the general manager in time, so they can be systematically and thoroughly rectified.

重大的不合格项必须及时向总经理报告，以便系统地彻底地纠正该项错误。

The security committee is responsible for conducting the internal audit for the security related department, corresponding discussion will also be conducted to analysis the reason of issues.

安全委员会负责对安全相关部门进行内部审计，并进行相应的讨论，分析问题产生的原因。

Internal audit will cover:

内部审计包括

* The logs, forms and tables review;检查日志、表格和表单
* Onsite review for all the departments;实地检查所有的部门
* Interview for the employee randomly chosen from each department;随机抽查各部门的员工
* Issues found during the last audit.上次审核中发现的问题
* CCTV systems, alarm systems and access control system

The audit issues and corresponding solving measures will be recorded on the Internal Audit Record.

审核问题及相应的解决措施需要记录在《内部审核记录》中。

The issue solving evidence should be provided to CISO and general manager. CISO and GM will sign to confirm on the Audit Record.

解决问题的证据应提供给CISO和总经理。CISO和总经理将在审核记录上签字确认。

* 1. 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.

安全审核结果必须每月收集并向公司安全部报告。

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。

1. Justification of necessary level of protection

In this chapter the justification is given that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Security measure** | 1. **Chapter** 2. **(this document)** | 1. **Confidentiality of TOE preserved** | 1. **Integrity of TOE preserved** |
| 1. Data recovery | 1. 8.2.6 | 1. The server used for backup shall be controlled following 4-eyes principle. | IT group must ensure that all internal, confidential and strictly confidential information assets must be fully backup monthly. |
| 1. Data back up | 1. 8.2.6 | 1. The server used for backup shall be controlled following 4-eyes principle. | For each time, the full backup restoring process should be conducted to ensure the backup’s availability. |
| 1. Destruction | 1. 3.6 | Before destruction, the data of the media should be formatted, and then the disk of the hard drive should be taking out and smash into pieces to ensure that the hard drive cannot be read and restored any more. | Before destruction, the data of the media should be formatted, and then the disk of the hard drive should be taking out and smash into pieces to ensure that the hard drive cannot be read and restored any more. |
| 1. Virus protection | 1. 8.2.3 | 1. Antivirus tools are updated automatically/manually and regularly. | 1. Antivirus tools are updated automatically/manually and regularly. |
| 1. Data transfer | 1. 8.4.2 | computers deployed in the production network have the function to encrypt all the data which transfer from the computers deployed in the production network by the specific PGP encryption tool | 1. computers deployed in the production network have the function to encrypt all the data which transfer from the computers deployed in the production network by the specific PGP encryption tool |
| 1. Object access control during production | 1. 8.3 | 1. Access to the production area is restricted to authorised persons only. | Obsolete or unqualified sensitive assets must always be collected and sent back to customer by following secure procedures, and the related log must be kept. |
| Organisational security | 4.2 | CTWY guidelines are implemented and employees are trained regularly. | Emergency plans and procedures exits for TOE production site. |
| 1. Physical security | 1. 6 | The authorized employees enter the related area with their badge cards and keys and the unauthorized employees are restricted to enter the unauthorized areas that are not within the range of their work. | The site is located in an industrial park surrounded by fences with CCTV and sensors. And security measures are divided in Stop layers and Detection layers. |
| 1. Personnel security | 1. 5 | All the employees, interns, third parties and subcontractors shall sign the NDA. | 1. Personnel will use their ID card to enter or exit from the security places. |
| 1. IT Security | 1. 8 | 1. Network is protected by firewalls. | Connections coming from the Internet and directed to the Internal Network are not allowed; |

* 1. General Assessment

Due to the implementation of the above listed security measures through the entire TOE development and production process the necessary level of protection for the confidentiality and integrity of the TOE is implemented.

1. Bibliography

1. **Library, Join International.** *Minimum Site Security Requirements.* 2019 April. version 2.2.

2. **EUROSMART.** *Security IC Platform Protection Profile with Augmentation packages.* Version 1.0, 2014.

3. **Common Methodology for Information Technology Secuirty Evaluation.** *Supporting Document, Site Certification.* Version 1.0, Rev.1, October 2007.

4. **Common Criteria for Information Technology Security Evaluation.** *Part 3: Security Assurance Components.* Version 3.1, Rev. 5, April 2017.