**信息等级：重要**

**受控状态：受控**

**文件编号：CM-IM-001-V1.0**

信息安全管理手册

**版本号：V1.0**

**发布日期：2020年06月15日**

**证优客**

**内部资料 版权所有 未经允许 不得抄印**

**变 更 履 历**

| 版本 | 变更内容 | 编制人/  创建日期 | 审核人/  审核日期 | 批准人/  批准日期 | 备注 |
| --- | --- | --- | --- | --- | --- |
| V1.0 | **文档建立，初次发布** | 人力行政中心  2020.06.15 | 刘瑞青  2020.06.15 | 张威  2020.06.15 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目 录

前言 8

1 范围 8

1.1 总则 8

1.2 应用 8

1.2.1 覆盖范围 8

1.2.2 删减说明 8

1.2.3 信息安全手册说明 9

1.2.4 信息安全手册的编制、审核、批准 9

1.2.5 信息安全手册修改 9

1.2.6 信息安全手册发放和保管 10

1.2.7 信息安全手册的评审 10

2 规范性引用文件 10

3 术语和定义 10

3.1 术语 10

3.2 缩写 10

4 组织的背景 11

4.1 了解公司现状及背景 11

4.2 理解相关方的需求和期望 11

4.3 确定信息安全管理体系的范围 11

4.4 信息安全管理体系 11

5 领导力 11

5.1 领导力和承诺 12

5.2 信息安全管理体系的方针 12

5.3 角色，责任和承诺 12

5.3.1 信息安全组织机构 12

5.3.2 信息安全职责和权限 13

5.3.3 承诺 13

6 计划 14

6.1 处理风险和机遇的行动 14

6.1.1 总则 14

6.1.2 信息安全风险评估 14

6.2 可实现的信息安全目标和计划 15

7 支持 16

7.1 资源 16

7.2 能力 16

7.3 意识 17

7.4 沟通 17

7.5 文档化信息 17

7.5.1 总则 17

7.5.2 创建和更新 17

7.5.3 文档化信息的控制 18

7.5.4 外来文件管理 18

8 运行 18

8.1 运行计划及控制 18

8.2 信息安全风险评估 19

8.3 信息安全风险处置 19

9 绩效评价 19

9.1 监控，度量，分析和评价 19

9.2 内部审核 19

9.2.1 总则 19

9.2.2 内审策划 20

9.2.3 内审员 20

9.2.4 内审实施 20

9.3 管理评审 21

10 改进 21

10.1 不符合及纠正措施 22

10.2 持续改进 22

附录1-组织简介 23

附录2-组织机构图 24

附录3-职能分配表 24

**颁布令**

经公司全体员工的共同努力依据ISO/IEC 27001:2013标准证优客建立了信息安全管理体系。

指导管理体系运行的公司《信息安全管理体系手册》经评审后，现予以批准发布。

《信息安全管理体系手册》的发布，标志着我公司从现在起，必须按照信息安全管理体系标准的要求和公司《信息安全管理体系手册》所描述的规定，不断增强持续满足顾客要求、相关方要求和法律法规要求的能力，全心全意为顾客和相关方提供服务，以确立公司在社会上的良好信誉。

《信息安全管理体系手册》是公司规范内部管理的指导性文件，也是全体员工在产品设计和销售及对客户的服务过程中必须遵循的行动准则。《信息安全管理体系手册》一经发布，就是强制性文件，全体员工必须认真学习、切实执行。

本手册2020年06月15日正式实施。

**总经理: 张威**

**2020年06月15日**

**授权书**

为贯彻执行ISO/IEC 27001:2013《信息安全管理体系》，加强对信息管理体系运行的领导，特授权：

1、授权 刘瑞青 为公司管理者代表并为公司风险责任人，其主要职责（角色）权限为：

1）确保公司信息安全管理体系所需过程得到建立、实施、运行和保持。确保信息安全业务风险得到有效控制。

2）向最高管理者报告信息安全管理体系业绩（绩效）和任何改善需求，为最高管理层评审提供依据。

3）确保满足顾客和相关方要求、法律法规要求的信息安全意识和信息安全风险意识在公司内得到形成和提高。

4）在信息安全管理体系事宜方面负责与外部的联络。

2、授权 刘瑞青 为ISMS信息安全管理项目责任人，其职责（角色）和权限为：确保信息安全管理方的控制措施得到形成、实施、运行和控制。

3、授权各部门主管为信息安全管理体系在本部门的责任人，对ISMS要求在本部门的实施负责。

**总经理：张威**

**2020年06月15日**

# 前言

无锡芯软智控系统有限公司《信息安全管理体系手册》（以下简称本手册）依据ISO/IEC 27001:2013《信息技术-安全技术-信息安全管理体系-要求》，参照ISO/IEC 27002:2013《信息技术-安全技术-信息安全管理实用规则》，结合本行业信息安全的特点编写。本手册对本公司信息安全管理体系做出了概括性描述，为建立、实施和保持信息安全管理体系提供框架。

1. 范围

## 总则

在公司的背景下建立，实施，维护和不断改进信息安全管理体系的要求，确定信息安全方针和目标，对信息安全风险进行有效管理，确保全体员工理解并遵照执行信息安全管理体系文件，持续改进信息安全管理体系的有效性，特制定本手册。

## 应用

### 覆盖范围

本《信息安全管理体系手册》规定了本公司信息安全管理体系涉及的信息安全管理、职责管理、内部审核、管理评审和信息安全管理体系持续改进等方面内容。

### 删减说明

本《信息安全管理体系手册》采用了ISO/IEC27001:2013标准正文的全部内容，对附录A的删减及理由如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 条款号 | 标题 | 删减理由 |
| 1 | A.14.1.3 | 保护应用服务交易 | 本公司在运营过程中无服务交易过程，故此条款不适用 |
| 2 | A.14.2.7 | 外包开发 | 本公司在运营过程中无外包软件开发过程，故此条款不适用 |

### 信息安全手册说明

本手册的编制及颁布可以对公司信息安全管理各项活动进行控制，指导公司开展各项业务活动，并通过不断的持续改进来完善信息安全管理体系。

### 信息安全手册的编制、审核、批准

本手册由信息安全管理小组负责组织编制、经管理者代表审核、总经理批准发布。本手册一经发布，就成为公司信息安全管理的基本要求，公司全体员工必须严格遵守。信息安全管理小组负责本手册的发放与管理，并负责其有效性。本手册的解释权归信息安全管理小组。

### 信息安全手册修改

本手册可根据实际情况的变化进行修改，应由信息安全管理体系相关部门提出申请，经管理者代表审核、总经理批准后方可进行修改。为保证修改后的手册能够及时发放给相关人员，信息安全管理小组对手册实施修改后，应及时发布修改信息，通知相关人员。

本手册的修改分为两种：一、小量的文字性修改，此种修改不改变手册的版本号，只需在本手册的“文档修改记录”如实记录即可，不需保存手册修改前的文档原件；二、大范围的信息安全管理体系版本升级，即改版。在本手册经过多次修改、信息安全管理体系建立依据的标准发生变化、公司的业务范围有较大调整的情况下，需要对本手册进行改版。本手册的改版应该对改版前的本手册文档原件进行保存。

在出现下列情况时，本手册可以进行修改：

信息安全管理体系运行过程中发现问题，或信息安全管理体系需进一步改进

内部信息安全提出新的需求

组织机构和职能发生变化

经营环境和产品结构有调整

发现本手册中的存在差错或不明确之处

引用的法规或体系标准有修改

体系审核或管理评审提出改进要求

本手册的更改控制按《文件管理程序》执行

在出现下列情况时，本手册可以改版：

组织机构、经营环境、信息技术架构、产品结构发生重大变化

相应法规有重大变化

修改涉及了相当多的页次或一个版本的修改达到十次

本手册执行已经满三年

本手册完成修改后，经审批重新发布实施。本手册的原审批岗位对手册的修改负有重新审批的责任。

### 信息安全手册发放和保管

信息安全手册经总经理批准后，由人力行政中心存放到公司的文件服务器指定位置，并通过邮箱将该手册发放给相关人员。

### 信息安全手册的评审

由管理者代表根据实际情况需要，负责组织有关部门（人员）对信息安全手册进行评审，目的在于确定信息安全手册是否需要更新，以保持信息安全手册的有效性。

1. 规范性引用文件

下列文件中的条款通过本《信息安全管理体系手册》的引用而成为本《信息安全管理体系手册》的条款。凡是标注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修改版均不适用于本《信息安全管理体系手册》，然而，信息安全小组应研究是否可使用这些文件的最新版本。凡是不注日期的引用文件、其最新版本适用于本《信息安全管理体系手册》。

ISO/IEC 27001:2013《信息技术-安全技术-信息安全管理体系-要求》

ISO/IEC 27002:2013《信息技术-安全技术-信息安全管理实用规则》

1. 术语和定义

术语ISO / IEC 27000 的术语和定义适用于本《信息安全管理体系手册》。

本组织、本公司、我公司：证优客。

## 缩写

ISMS：Information Security Management Systems 信息安全管理体系；

SOA：Statement of 证优客适用性声明；

PDCA:：Plan Do Check Action 计划、实施、检查、改进。

1. 组织的背景

## 了解公司现状及背景

本公司根据内外部环境因素，考虑公司的信息安全管理目的，这将作为公司实施信息安全管理体系的核心需求。

## 理解相关方的需求和期望

本公司根据相关方提出的信息安全需求和期望，考虑建立信息安全管理体系，这些需求包括：法律法规、合同义务、地方规定等。

## 确定信息安全管理体系的范围

本公司根据业务特征、组织结构、地理位置、资产和技术确定了范围和边界：

业务特征：已于附录1[组织简介](#_附录1-组织简介)中进行了描述；

组织结构：已在[附录2组织机构图](#_附录2-组织机构图)进行的定义；

地理位置：陕西省西安市高新区细柳街办天谷七路996号数字出版基地B座18-19层

资产分类定义：人员、物理、数据、文档、软件、服务、无形资产；

ISMS的范围是：**与计算机应用软件开发及维护服务相关的信息安全管理活动**

《信息安全管理体系手册》采用了ISO/IEC 27001:2013准正文的全部内容，对附录A的删减及理由详见《信息安全适用性声明SOA》；

ISMS的边界是：陕西省西安市高新区细柳街办天谷七路996号数字出版基地B座18-19层

## 信息安全管理体系

本公司的信息安全管理体系按照ISO/IEC 27001:2013《信息技术-安全技术-信息安全管理体系-要求》规定，参照ISO/IEC 27002:2013《信息技术-安全技术-信息安全管理实用规则》标准建立、实施、运行、监视、评审、保持和改进文件化的信息安全管理体系。

1. 领导力

## 领导力和承诺

我公司管理者通过以下活动，对建立、实施、运作、监视、评审、保持和改进信息安全管理体系的承诺提供证据：

建立信息安全方针(见《信息安全方针》)；

确保信息安全目标和计划得以制定（见《信息安全目标》及相关记录）；

提供充分的资源，以建立、实施、运作、监视、评审、保持并改进信息安全管理体系(见本手册第7.1章)；

建立信息安全的角色和职责(见本手册附录3（规范性附录）《职责权限》和相应的管理程序；

向组织传达满足信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性；

实施信息安全管理体系管理评审，确保信息安全管理体系达到其预期的效果（见本手册第9章）；

指导和支持员工对信息安全管理体系作出有效的贡献;

确保内部信息安全管理体系审核得以实施，促进持续改进（见本手册第9章）；

支持其他相关管理角色来展示自己的领导力，因为它适用于他们的职责范围。

## 信息安全管理体系的方针

为了满足适用法律法规及相关方要求，维持ISMS范围内的业务正常进行，实现业务可持续发展，本公司根据组织的业务特征、组织结构、地理位置、资产和技术确定了信息安全管理体系方针：

**提升信息安全水平，提高风险控制能力，确保核心产品信息安全。**含义为：公司全体员工应严格按ISO/IEC 27001 标准的要求，建立、实施、保持和改进公司信息安全管理体系，不断提升信息安全意识，规范信息生命周期过程的管理，持续识别和控制信息安全的风险，保证公司所有信息的安全。不断加大对信息设备的投入，提升信息技术水平，为公司经营提供高效、便捷、安全的服务，确保总体业务系统持续可靠地运行。

## 角色，责任和承诺

### 信息安全组织机构

本公司成立信息安全领导机构——人力行政中心，职责是实现信息安全管理体系的方针。具体的职责是：研究决定信息安全工作涉及到的重大事项；审定公司信息安全方针、目标、工作计划和重要文件；为信息安全工作的有序推进和信息安全管理体系的有效运行提供必要的资源，负责制订、落实信息安全工作计划，对单位、部门信息安全工作进行检查、指导和协调，建立健全企业的信息安全管理体系，保持其有效、持续运行。

本公司采取相关部门代表组成的协调会的方式，进行信息安全协调和协作，以：

确保安全活动的执行符合信息安全方针；

确定怎样处理不符合；

批准信息安全的方法和过程，如风险评估、信息分类；

识别重大的威胁变化，以及信息和相关的信息处理设施对威胁的暴露；

评估信息安全控制措施实施的充分性和协调性；

有效的推动组织内信息安全教育、培训和意识；

评价根据信息安全事件监控和评审得出的信息，并根据识别的信息安全事件推荐适当的措施。

### 信息安全职责和权限

本公司总经理为信息安全最高责任者。总经理指定信息安全管理者代表,无论信息安全管理者代表其他方面的职责如何，对信息安全负有以下职责：

建立并实施信息安全管理体系必要的程序并维持其证优客信息安全管理体系的运行情况和必要的改善措施向信息安全小组或最高责任者报告。

各部门负责人为本部门信息安全管理责任者，全体员工都应按保密承诺的要求自觉履行信息安全保密义务。

各部门、人员有关信息安全职责分配见附录3（规范性附录）《职责权限》和相应的程序文件（管理标准）、规定及岗位说明书。

### 承诺

为实现信息安全管理体系方针，本公司承诺：

在公司内各层次建立完整的信息安全管理组织机构，确定信息安全方针、安全目标和控制措施，明确信息安全的管理职责；

识别并满足适用法律、法规和相关方信息安全要求；

定期进行信息安全风险评估，信息安全管理体系评审，采取纠正预防措施，保证体系的持续有效性；

采用先进有效的设施和技术，处理、传递、储存和保护各类信息，实现信息共享；

对全体员工进行持续的信息安全教育和培训，不断增强员工的信息安全意识和能力；

制定并保持完善的业务连续性计划，实现可持续发展。

1. 计划

## 处理风险和机遇的行动

### 总则

公司信息安全风险管理在规划时需考虑4.1和4.2条款中提出的需求，以确保风险评估可以实现可预期的结果，实现体系的持续改进。

### 信息安全风险评估

* 风险评估的方法

信息安全小组制定《信息安全风险管理程序》，建立识别适用于信息安全管理体系和已经识别的业务信息安全、法律和法规要求的风险评估方法，建立接受风险的准则并识别风险的可接受等级。按信息安全风险评估执行《信息安全风险管理程序》进行，以保证所选择的风险评估方法应确保风险评估能产生可比较的和可重复的结果。

* 识别风险

在已确定的信息安全管理体系范围内，本公司按《信息安全风险管理程序》对所有的资产和资产所有者进行了识别；对每一项资产保密性、完整性、可用性和法律法规及重要性级别进行了量化赋值，根据重要资产判断准则确定是否为重要资产，形成《重要资产清单》。同时根据《信息安全风险管理程序》识别对这些资产的威胁、可能被威胁利用的脆弱性、现有的控制措施及现有控制措施的有效性，并通过对这些项目的赋值计算出在丧失保密性、完整性和可用性可能对重要资产造成的影响。

需对风险的所有者进行指定。

* 分析和评价风险

本公司按《信息安全风险管理程序》分析和评价风险：

针对重要资产的价值和脆弱性严重程度，计算出风险发生的影响值；

针对每一项威胁发生频率、脆弱性被威胁利用的容易程度进行赋值，然后计算得出风险发生的可能性；

根据《信息安全风险管理程序》计算风险等级，从而得出风险等级；

根据《信息安全风险管理程序》及风险接受准则，判断风险为可接受或需要处理。

* 信息安全风险处置

信息安全小组及相关部门根据风险评估的结果，形成《信息安全风险处理计划》，该计划明确了风险处理责任部门、负责人、处理方法及起始、完成时间。

对于信息安全风险，应考虑控制措施与费用的平衡原则，选用以下适当的措施：

控制风险，采用适当的内部控制措施；

接受风险；

避免风险；

转移风险。

* 选择控制目标与控制措施

信息安全小组根据相关法律法规要求、信息安全方针、业务发展要求及风险评估的结果，组织有关部门选择和制定了信息安全目标，并将目标分解到有关部门（见《信息安全适用性声明》）：

信息安全控制目标获得总经理的批准。

控制目标及控制措施的选择原则来源于ISO/IEC 27001:2013录A，具体控制措施参考ISO/IEC 27002:2013信息技术-安全技术-信息安全管理实用规则》。

本公司根据信息安全管理的需要，可以选择标准之外的其他控制措施。

* 剩余风险

对风险处理后的剩余风险应形成《信息安全剩余风险评估报告》并得到公司管理者的批准。

* 适用性声明

信息安全小组编制《信息安全适用性声明（SoA）》。该声明包括以下方面的内容：

所选择控制目标与控制措施的概要描述，以及选择的原因；

对ISO/IEC 27001:2013录A中未选用的控制目标及控制措施理由的说明。

## 可实现的信息安全目标和计划

根据信息安全目标规划的框架指定公司信息安全可测量目标：

* 重要信息泄露/损坏的事态不得发生。
* 内部审核和管理审核实施及时率100%
* 年度信息安全培训人员覆盖率100%
* 大面积内网(达到60%)中断时间每年累计不超过240分钟

信息安全目标需根据公司组织架构进行拆解，指定目标的负责人以及考核方式，详见《信息安全目标》

1. 支持

## 资源

本公司确定并提供实施、保持信息安证优客适当措施，使影响信息安全管理体系工作的员工是有能力胜任的，以保证：

建立、实施、运作无锡芯软智控系统有限公司保持和改进信息安全管理体系；

确保信息安全程序支持业务要求；

识别并指出法律法规要求和合同安全责任；

通过正确应用所实施的所有控制来保持充分的安全；

必要时，进行评审，并对评审的结果采取适当措施；

需要时，改进信息安全管理体系的有效性。

## 能力

信息安全小组制定并实施《人力资源管理程序》文件，确保被分配信息安全管理体系规定职责的所有人员，都必须有能力执行所要求的任务。可以通过：

确定承担信息安全管理体系各工作岗位的职工所必要的能力；

提供职业技术教育和技能培训或采取其他的措施来满足这些需求；

评价所采取措施的有效性；

保留教育、培训、技能、经验和资格的记录。

本公司还确保所有相关人员意识到其所从事的信息安全活动的相关性和重要性，以及如何为实现信息安全管理体系目标做出贡献。

## 意识

对公司全体人员通过培训、学习、宣传等方式提高人员信息安全意识，需了解到：

a) 信息安全方针;

b) 他们对信息安全管理体系有效性的贡献，包括提高信息安全绩效的收益;

c）不符合信息安全管理体系要求所带来的影响，。

## 沟通

公司需通过适当的手段保持在内部和外部在信息安全要求进行有效的沟通。包括获取外部信息安全专家的建议、信息安全政府行政主管部门的联系及识别顾客对信息安全的要求等，沟通方式在《信息安全组织管理程序》进行规定。

## 文档化信息

### 总则

本公司信息安全管理体系文件包括：

文件化的信息安全方针，在《信息安全管理体系手册》中描述,选择的控制目标在《信息安全适用性声明SoA》中描述；

《信息安全管理体系手册》（本手册，包括信息安全适用范围及引用的标准）；

ISO/IEC 27001:2013标准中规定需文件化的程序；

本手册涉及的相关支持性程序性文件，例如《信息安全风险管理程序》；

为确保有效策划、运作和控制信息安全过程所制定的文件化操作程序；

《风险处理计划》以及信息安全管理体系要求的记录类；

相关的法律、法规和信息安全标准；

《信息安全适用性声明SOA》。

### 创建和更新

信息安全小组按《文件控制程序》的要求，对信息安全管理体系所要求的文件进行管理。对《信息安全管理体系手册》、程序文件、管理规定、作业指导书和为保证信息安全管理体系有效策划、运行和控制所需的受控文件的编制、评审、批准、标识、发放、使用、修订、作废、回收等工作实施控制，以确保在使用场所能够及时获得适用文件的有效版本。

文件的创建和更新应确保：

识别或描述文件时需包含标题、日期、作者、编号等

文件格式可以是表、单、卡、台帐、记录本、报告、纪要、证、图等多种适用的形式，可以是书面的或电子媒体的。

文件发布前得到批准，以确保文件是充分的；

必要时对文件进行评审、更新并再次批准；

### 文档化信息的控制

文件控制应保证：

确保文件的更改和现行修订状态得到识别；

确保在使用时，可获得相关文件的最新版本；

确保文件可以为需要者所获得，并根据适用于他们类别的程序进行标识、保护、检索、转移、存储和最终的销毁；

确保外来文件得到识别；

确保文件的分发得到控制；

防止作废文件的非预期使用；

若因任何目的需保留作废文件时，应对其进行适当的标识。

### 外来文件管理

外来文件包括信息安全法律、行政法规、部门规章、地方法规，按以下规定执行：

信息安全适用的法律法规按照《信息安全法律法规管理程序》规定执行；

外来的文件按照《文件控制程序》和其他相关规定执行；

外来标准按本公司标准化管理的相关规定进行。

1. 运行

## 运行计划及控制

为确保信息安全管理体系有效实施，对已识别的风险进行有效处理，本公司开展以下活动：

形成《信息安全风险处理计划》，以确定适当的管理措施、职责及安全控制措施的优先级；

为实现已确定的安全目标、实施《信息安全风险处理计划》，明确各岗位的信息安全职责；

实施所选择的控制措施，以实现控制目标的要求；

确定如何测量所选择的控制措施的有效性，并规定这些测量措施如何用于评估控制的有效性以得出可比较的、可重复的结果；

对运行过程中发生的非计划的变更进行规划，以减轻不良的影响。

## 信息安全风险评估

信息安全管理小组每年应组织对信息安全风险重新评估一次，以适应信息资产的变化，确定是否存在新的风险及是否需要增加新的控制措施。

信息安全小组组织有关部门按照《信息安全风险管理程序》的要求，对风险处理后的残余风险进行定期评审，以验证残余风险是否达到可接受的水平，对以下方面变更情况应及时进行风险评估：

组织；

技术；

业务目标和过程；

已识别的威胁；

实施控制的有效性；

外部事件，例如法律或规章环境的变化、合同责任的变化以及社会环境的变化。

## 信息安全风险处置

公司需保留信息安全风险处理计划的执行结果的文档化的记录。

1. 绩效评价

## 监控，度量，分析和评价

本公司通过实施不定期安全检查、内部审核、事故报告调查处理、电子监控、定期技术检查等控制措施并报告结果以实现：

及时发现处理结果中的错误、信息安全管理体系的事故和隐患；

及时了解识别失败的和成功的安全破坏和事件、信息处理系统遭受的各类攻击；

使管理者确认人工或自动执行的安全活动达到预期的结果；

使管理者掌握信息安全活动和解决安全破坏所采取的措施是否有效；

积累信息安全方面的经验。

## 内部审核

### 总则

要求

本公司信息安全小组按《内部审核管理程序》的要求策划和实施信息安全管理体系内部审核以及报告结果和保持记录。

活动

本公司每年进行壹次信息安全管理体系内部审核，以确定其信息安全管理体系的控制目标、控制措施、过程和程序是否：

符合本标准的要求和相关法律法规的要求；

符合已识别的信息安全要求；

得到有效地实施和维护；

按预期执行。

### 内审策划

信息安全小组策划审核的过程、区域的状况、重要性以及以往审核的结果，对审核工作进行策划。应编制《年度内审计划》，确定审核的准则、范围、频次和方法。

每次审核前，信息安全小组应编制《内部审核计划》，确定审核的准则、范围、日程和审核组。审核员的选择和审核的实施应确保审核过程的客观性和公正性。审核员不应审核自己的工作。

《内部审核计划》，经管理者代表批准，提前3天通知被审核部门，被审核部门到时应选派有关人员配合审核。

### 内审员

内部审核员必须是熟悉本公司信息安全管理情况，参加内部审核员培训并考核合格的人员。

内部审核员应来自于不同的部门，审核人员应与被审活动无直接责任，以保持工作的独立性。

各部门选择符合内部审核员条件的候选人，参加内部审核员培训并考试合格，填写《内部审核员评定表》，经管理者代表批准，方取得内部审核员资格。

### 内审实施

活动

应按审核计划的要求实施审核，包括：

进行首次会议，明确审核的目的和范围，采用的方法和程序；

实施现场审核，检查相关文件、记录和凭证，与相关人员进行交流，填写审核发现；

对检查内容进行分析，对审核发现的问题在《不符合项报告及纠正报告单》中开出不符合项；

审核组长编制《内部审核报告》。

不符合处理

对审核中提出的不符合项，责任部门应制定纠正措施，由信息安全小组对纠正措施的实施情况进行跟踪、验证，将结果记入《不符合项报告及纠正报告单》。

记录

内部审核记录由信息安全小组保存，并作为管理评审的输入之一。

## 管理评审

总经理应每年进行一次管理评审，以确保信息安全管理体系持续的适宜性、充分性和有效性，管理评审按《管理评审程序》进行。

管理评审应包括评价信息安全管理体系改进的机会和变更的需要，包括信息安全方针和信息安全目标。

管理评审的结果应清晰地形成文件，记录应加以保持。

管理评审应考虑：

以往管理评审的跟踪措施；

任何可能影响信息安全管理体系的变更；

不符合项和纠正措施的状况；

有效性测量的结果；

信息安全管理体系审核和评审的结果；

信息安全目标的实现情况；

相关方的反馈；

风险评估的结果和风险处置的状态；

改进的机会和建议。

1. 改进

## 不符合及纠正措施

本公司信息安全小组管理纠正措施，不符合事项的责任部门负责采取纠正措施，以消除与信息安全管理体系要求不符合的原因，以防止再发生。

纠正措施的实施按《持续改进控制程序》进行。

纠正措施的制定和实施程序如下：

识别信息安全事件及不符合；

确定信息安全事件及不符合的原因；

确定是否存在类似的不符合和发生的可能；

评价确保不符合不再发生的措施要求；

确定和实施所需的纠正措施；

记录所采取措施的结果；

评审所采取的纠正措施。

我公司信息安全小组定期组织进行风险评估，以识别变化的风险，并通过关注变化显著的风险来识别纠正措施要求。纠正措施的优先级应基于风险评估结果来确定。

## 持续改进

本公司依据《持续改进控制程序》的要求,通过使用信息安全方针、信息安全目标、审核结果、监控事件的分析、纠正和预防措施以及管理评审，持续改进信息安全管理体系的适宜性，充分性和有效性。

我公司开展以下活动，以确保信息安全管理体系的持续改进：

实施每年管理评审、内部审核、安全检查等活动以确定需改进的项目；

按照本手册的要求采取适当的纠正和预防措施；吸取其他组织及本公司安全事故的经验教训，不断改进安全措施的有效性；

通过适当的手段保持在内部对信息安全措施的执行情况与结果进行有效的沟通。包括获取外部信息安全专家的建议、信息安全政府行政主管部门的联系及识别顾客对信息安全的要求等；

对信息安全目标及分解进行适当的管理，确保改进达到预期的效果。

# 附录1-组织简介

企业概况

证优客（以下称“蝉鸣科技”），成立于2014年6月24日，注册资本1070.5789万元人民币，注册地址为陕西省西安市高新区细柳街办天谷七路996号数字出版基地B座19层。

蝉鸣科技旗下拥有“学加家”品牌，始终坚持“提升教育价值，成就美好未来”的使命，以学生为中心，以家庭为单位，连接学校与商业，用科技的力量为校园、师生和家庭创造美好教育生活，实现教育公平的美好愿景。

学加家在教育信息化2.0行动计划引领下，以5G、人工智能、大数据、云计算、物联网等关键技术为支撑，以智能基础设施为依托，提供校园智能教育与智能管理服务，建设具有智能感知与智能分析力的智能幼儿园、智能中小学、智能大学及智能教培，助力教育行业实现数字化转型。

目前蝉鸣科技公司产品覆盖30000+幼儿园，5000+中小学，25000+教培机构，累计处理教育缴费交易流水超过人民币500亿元

# 附录2-组织机构图

管理层

管理者代表

人力行政中心

研发中心

销售中心

法务合规部

财务中心

投资部

商业化中心

市场运营部

数据效能中心

中心

产品运营中心

# 附录3-职能分配表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **部门** | **管理层** | | **人力行政中心** | **产品运营中心** | **研发中心** | **销售中心** |
| **4.1**组织及背景 | ▲ | | △ | △ | △ | △ |
| **4.2** 理解相关方的需求和期望 | ▲ | | △ | △ | △ | △ |
| **4.3** 确定 **ISMS** 的范围 | ▲ | | △ | △ | △ | △ |
| **4.4 ISMS** | ▲ | | △ | △ | △ | △ |
| **5.1** 领导力和承诺 | ▲ | | △ | △ | △ | △ |
| **5.2** 方针 | ▲ | | △ | △ | △ | △ |
| **5.3** 角色，责任和承诺 | ▲ | | △ | △ | △ | △ |
| **6.1** 处理风险和机遇的行动 | △ | | ▲ | △ | △ | △ |
| **6.2** 可实现的信息安全目标和计划 | △ | | ▲ | △ | △ | △ |
| **7.1** 资源 | ▲ | | △ | △ | △ | △ |
| **7.2** 能力 | △ | | ▲ | △ | △ | △ |
| **7.3** 意识 | △ | | ▲ | △ | △ | △ |
| **7.4** 沟通 | △ | | ▲ | △ | △ | △ |
| **7.5** 文档化信息 | △ | | ▲ | △ | △ | △ |
| **8.1** 运行计划及控制 | △ | | ▲ | △ | △ | △ |
| **8.2** 信息安全风险评估 | △ | | ▲ | △ | △ | △ |
| **8.3** 信息安全风险处置 | △ | | ▲ | △ | △ | △ |
| **9.1** 监控，度量，分析和评价 | △ | | ▲ | △ | △ | △ |
| **9.2** 内部审核 | △ | | ▲ | △ | △ | △ |
| **9.3** 管理评审 | ▲ | | △ | △ | △ | △ |
| **10.1** 不符合及纠正措施 | △ | | ▲ | △ | △ | △ |
| **10.2** 持续改进 | △ | | ▲ | △ | △ | △ |
| **A.5** 安全方针 | ▲ | | △ | △ | △ | △ |
| **A.6.1** 内部组织 | ▲ | | ▲ | ▲ | ▲ | ▲ |
| **A.6.2** 移动设备和远程办公 | △ | | △ | ▲ | △ | △ |
| **A.7.1** 任用之前 | △ | | ▲ | △ | △ | △ |
| **A.7.2** 任用中 | △ | | ▲ | △ | △ | △ |
| **A.7.3** 任用的终止或变化 | △ | | ▲ | △ | △ | △ |
| **A.8.1** 对资产负责 | ▲ | | ▲ | ▲ | ▲ | ▲ |
| **A.8.2** 信息分类 | △ | | △ | ▲ | ▲ | △ |
| **A.8.3** 介质处理 | △ | | △ | △ | ▲ | △ |
| **A.9.1** 访问控制的业务要求 | △ | | △ | △ | ▲ | △ |
| **A.9.2** 用户访问管理 | △ | | △ | △ | ▲ | △ |
| **A.9.3** 用户职责 | | ▲ | ▲ | ▲ | ▲ | ▲ |
| **A.9.4** 系统和应用程序的访问控制 | | △ | △ | △ | ▲ | △ |
| **A.10.1** 密码控制 | | △ | △ | △ | ▲ | △ |
| **A.11.1** 安全区域 | △ | △ | △ | △ | ▲ | △ |
| **A.11.2** 设备 | △ | △ | △ | △ | ▲ | △ |
| **A.12.1** 操作程序和职责 | △ | △ | △ | △ | ▲ | △ |
| **A.12.2** 恶意软件防护 | ▲ | | ▲ | ▲ | ▲ | ▲ |
| **A.12.3** 备份 | ▲ | | ▲ | ▲ | ▲ | ▲ |
| **A.12.4** 记录和监控 | △ | | △ | △ | ▲ | △ |
| **A.12.5** 操作软件的控制 | △ | | △ | △ | ▲ | △ |
| **A.12.6** 技术漏洞管理 | △ | | △ | △ | ▲ | △ |
| **A.12.7** 信息系统审计考虑 | △ | | △ | △ | ▲ | △ |
| **A.13.1** 网络安全管理 | △ | | △ | △ | ▲ | △ |
| **A.13.2** 信息传输 | △ | | ▲ | △ | ▲ | ▲ |
| **A.14.1** 信息系统的安全要求 | △ | | △ | △ | ▲ | △ |
| **A.14.1.3**保护应用服务交易 | - | | - | - | - | - |
| **A.14.2** 开发和支持过程中的安全 | △ | | △ | △ | ▲ | △ |
| A.14.2.7软件外包开发 | - | | - | - | - | - |
| **A.14.3** 测试数据 | △ | | △ | △ | ▲ | △ |
| **A.15.1** 供应关系的安全 | △ | | △ | △ | ▲ | △ |
| **A.15.2** 供应商服务交付管理 | △ | | △ | △ | ▲ | △ |
| **A.16.1** 信息安全事件管理和持续改进 | △ | | △ | △ | ▲ | △ |
| **A.17.1** 信息安全连续性 | △ | | △ | △ | ▲ | △ |
| **A.17.2** 冗余 | △ | | △ | △ | ▲ | △ |
| **A.18.1** 信息安全审查 | ▲ | | ▲ | ▲ | ▲ | ▲ |
| **A.18.2** 符合法律和合同的要求 | △ | | ▲ | △ | △ | △ |

**信息安全职责：**

| 序号 | 角色 | 信息安全职责 |
| --- | --- | --- |
| 2 | 总经理 | 1) 任命管理者代表，明确管理者代表的职责和权限；  2) 确保在内部传达满足客户和法律法规的符合性；  3) 为信息安全管理体系配备必要的资源；  4) 主持管理评审；  5) 负责公司信息安全管理和企业管理的计划、组织、协调、监督、控制和考核工作；  6) 遵守公司信息安全的相关规定以及本岗位相关的保密要求。 |
| 3 | 管理者代表 | 1) 负责建立、实施、保持和改进信息安全管理体系，保证信息安全体系的有效运行；  2) 负责公司信息安全管理手册的审核，程序文件的批准，组织并领导公司内部审核工作；  3) 负责向总经理报告信息安全体系运行的业绩和任何改进的需求；  4) 负责就信息安全管理体系有关事宜的对外联络。 |
| 7 | 内部员工 | 1. 严格遵守所有与信息安全相关的国家法律、法规和政策，遵守公司所有的信息安全政策，并签字承诺遵守保密协议的有关规定； 2. 以安全负责的方式使用公司的信息资产； 3. 遵守公司员工手册所有规定； 4. 认真执行公司信息安全管理流程； 5. 积极参加信息安全教育与培训，提高信息安全意识； 6. 有责任将违反信息安全政策的事件与行为及时报告给本部门信息安全管理员及其他相关人员。 |
| 8 | 人力行政中心 | 1. 负责公司日常行政管理，组织建立执行公司各项行政制度，参与公司发展战略规划的制订。 2. 负责公司的日常法律事务，组织法律合同年检、知识产权保护等工作，协调、处理法律咨询、法律纠纷。 3. 负责公司行政部设施环境、固定资产（包括租赁资产）的实物管理，负责公司日常性办公用品采购工作。 4. 负责公司的企业文化建设。 5. 负责制定公司人事管理制度，研究、分析并提出改进工作意见和建议。 6. 负责人事考核、考查工作，建立人才库，规范人才培养。 7. 负责编制用工计划和工资计划。负责编制员工培训大纲、课程计划，组织员工培训工作。 8. 负责招聘、录用、辞退工作。 9. 负责拟制员工劳动纪律管理制度，负责考勤、奖惩、差假、调动等管理工作。 10. 制定公司资金运营计划，对公司生产经营活动所需要的资金筹措方式进行成本计算，监督资金管理报告和预、决算。 11. 根据法律法规、会计准则、公司政策以及上级主管部门的要求，组织制订公司财务管理制度。 12. 协调公司同银行、工商、税务等政府部门的关系，维护公司权益。 13. 向上级主管单位汇报公司经营状况、经营成果、财务收支及计划的具体情况，对公司经营状况和预算执行情况进行分析。 |
| 9 | 产品运营中心 | 1. 负责项目的交付的实施策划及执行。 2. 负责公司产品的整体规划、设计，同时通过产品运营和数据运营，驱动前线，并负责产品的生命周期演化。 3. 负责已交付项目的定期维护，并建立长期维护关系，为客户通提供满意的维护服务。 4. 负责采集客户的新的需求，交付给开发部门进行研发。 5. 负责公司计算机及网络设备的管理和维护； 6. 负责应用系统软件的管理和维护； 7. 负责公司网络及信息系统权限的管理和维护； 8. 负责公司IT方面的信息安全建设； 9. 负责了解世界计算机及网络技术的发展趋势，为公司计算机及网络设备的更新和升级提出建议并予以实施； 10. 负责公司网站的管理、维护和内容更新。 |
| 10 | 研发中心 | 1. 负责软件项目开发部编制设计文件和产品质量计划，并对其实施、控制负责； 2. 完成公司日常在软件需求方面的开发工作，并配合公司其他部门在软件方面的技术需求支持。 3. 负责软件产品技术标准的制订、修改和完善； 4. 参与技术管理工作及对技术问题的决策、攻关、协调； 5. 负责软件项目所需材料的验收和项目实施质量检验，并负责不合格的控制。 |
| 11 | 销售中心 | 1. 建立和完善营销信息收集、处理、交流及保密系统。 2. 对消费者购买心理和行为的调查。 3. 做出销售预测，提出未来市场的分析、发展方向和规划。 4. 制定产品价格。 5. 促销活动的策划及组织。 6. 负责公司销售目标的完成以及客户关系的维护。 |