

内部文件
注意保密



三胞集团有限公司

信息安全管理制

度
2018 年 1 月

修订跟踪表

版本号	建设类型			拟订背景	建设内容	拟订部门	拟订人	拟订时间
	新编	修订	废止					
三集信企 [2015]第 一版	√			/	/	IT&企业管理中心	/	2015.10
三集信 [2018]第 一版		√		IT 制度需要梳理且制度部分内容不能适应现有状况	修订框架 修改相关管理要求 修订格式	信息管理中心	姜兵	2018.1

三胞集团信息安全管理制度的

(三集信[2018]第一版)

第一章 总则

第一条 目的

为加强三胞集团的信息安全管理,保护企业信息的保密性、完整性和有效性,强化全体员工的信息安全意识,满足三胞集团的业务可持续发展需求,根据国家有关法律、法规,特制定三胞集团信息安全管理制度的。

第二条 适用范围

本制度的范围是根据三胞集团的组织特性、地理位置、资产和技术来进行界定的,主要包括:

- (一) 服务器、网络、数据、信息系统、资产和技术;
- (二) 物理环境(机房、弱电间等);
- (三) 信息终端包括办公电脑、电话、打印机等;
- (四) 三胞集团员工,包括三胞集团总部、产业集团、下属企业以及相关第三方组织或个人。

第三条 定义与术语

- (一) 信息安全:指对于信息的保密性、完整性和可用性的保持;
- (二) 保密性:确保只有经过授权的人才能访问信息;
- (三) 完整性:保护信息和信息的处理方法准确而完整;
- (四) 可用性:确保经过授权的用户在需要时可以访问信息并使用相关的信息资产。

第二章 管理原则及职责

第四条 信息安全的管理工作一般需要遵循以下原则:

- (一) 制定信息安全总则,为信息安全管理提供导向和支持;
- (二) 信息安全政策与标准的制定建立在风险评估的基础之上;

（三）考虑控制费用、业务开展与风险平衡的原则，将风险降至三胞集团可接受的水平；

（四）以预防控制为主的思想原则；

（五）业务持续性原则，即从故障与灾难中恢复业务运作，减少故障与灾难对关键业务过程的影响；

（六）动态管理原则，即对风险实施动态管理；

（七）全员参与的原则；

（八）整体规划、分步实施、逐步完善；

（九）保护三胞集团核心数据资产是信息安全最重要的工作之一。

第五条 信息管理中心在信息安全管理方面的主要职责包括：

（一）牵头三胞集团信息安全政策、实践标准的编制、修订及发布工作，确保信息安全；

（二）负责三胞集团信息类物理安全与维护；

（三）负责三胞集团网络系统安全与维护；

（四）负责三胞集团数据安全策略的制定；

（五）负责审核三胞集团管理与业务系统的安全合规；

（六）负责制定与第三方系统接口的安全政策、规范与实施；

（七）负责制定终端安全方面的政策、规范与实施。

第三章 员工须遵守的信息安全内容

第六条 机房安全

（一）机房钥匙、门禁卡配发由信息管理中心管理，不得私自配制或借给他人使用。来访人员因工作需要进入机房须经信息管理中心同意后由机房管理人员陪同进入，并做好记录。任何人未经许可，严禁在机房内随意触摸设备、拍照或录像。

（二）信息管理中心管理人员需定期检查机房内烟感、温感、灭火器等机房环境及其相关管理设备，确保运行正常。

（三）机房内严禁存放和使用易燃易爆物品，严禁吸烟和使用明火，严禁在消防设备周围堆放杂物。

（四）信息管理中心管理人员需定期检查机房配电柜、UPS 设备、精密空调的运行状况，检测输入输出电流、电压是否正常、有无异常噪音及声、广报警以及监控电池间的运行环境。

第七条 设备安全

（一）员工领用或借用的 IT 设备需具有完整的手续。员工在设备的使用期间需妥善保管，不得人为损坏、不得私自将设备转让给他人使用、严禁将设备提供给陌生人使用；

（二）员工对于领用或借用的 IT 设备需定期清洁清理、设备表面应无明显灰尘、飞绒等，以免影响设备使用；

（三）因员工个人原因造成设备损坏、损坏的情况，需按相关规定进行赔偿；

第八条 数据安全要求

三胞集团的机密、资料、合同、数据、文档等信息是核心保护对象，所有人员需做到：

（一）禁止员工把三胞集团的保密信息数据透露及传递给非授权人员；

（二）妥善保管个人掌握的三胞集团核心信息数据；

（三）备份个人工作使用的重要数据信息；

（四）在操作及使用三胞集团数据信息时，需谨慎操作以免带来损失。

第九条 网络安全访问要求

（一）公司决不允许任何员工参与入侵和攻击服务器的“黑客”行为，或者发布任何形式的病毒、木马、恶意软件、恶意代码等。如有违反，将交由公司处理。

（二）任何部门和个人、不得利用联网计算机从事危害本地局域网服务器、工作站及其他相关网络设备的活动，不得危害或侵入未授权的服务器、工作站及其他相关网络设备。

（三）任何部门及员工不得利用互联网及各种设备或软件技术，从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动。

（四）员工从互联网上下载的资源，必须确认下载源的可靠性；严禁从互联网上下载并使用来历不明、有安全隐患的软件；对来历不明有安全隐患的软件应使用集团规定使用的杀毒软件检查、杀毒。

（五）任何部门和个人不得利用互联网危害网络安全，从事危害国家安全、

荣誉和利益，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

（六）禁止通过互联网访问如下类型网站：视频网站、游戏类网站、BBS 及聊天室类网站、购物网站（不含集团下属企业）、P2P 下载、涉黄、涉赌、涉毒、钓鱼网站，以及其他违反国家法律法规或公司规章制度的网站。

（七）未经授权，任何人不得随意更改设备的 IP 或盗用他人 IP；

（八）访问互联网时，禁止使用和三胞集团相关的信息注册各类网络账号；

（九）因工作需要，需在外部通过互联网访问集团内网应用时，按照相关规定进行申请。

（十）任何使用集团无线 WIFI 的外部人员均需通过手机号、微信号或信息管理中心授权的账号访问因特网，且禁止访问集团内网。如访客有访问集团内网的需要，由接待人员向信息管理中心提出申请，申请通过后开通相关权限。

第十条 软件的使用要求

（一）禁止在公司运行任何游戏、娱乐软件；

（二）禁止私自在电脑安装未知或个人下载的不明软件；

（三）未经授权，严禁任何人修改、卸载、删除、增加、破坏系统的功能、程序及数据。

第十一条 应用系统的安全使用要求

（一）应用系统需设置复杂的密码，需满足密码安全要求；

（二）严禁员工将应用系统的账号密码告知其他人，需自行妥善保管；

（三）禁止员工在未知的公共场所网络或其他不安全的网络环境下访问应用系统，以免造成账号泄露等安全问题。

（四）禁止使用各系统进行不正当、非法的行为，包括骚扰、诽谤、传播不利于三胞集团的信息等。

（五）禁止员工发送以下类型的邮件：垃圾邮件、病毒邮件以及重复发送某一份邮件；

（六）收发和三胞集团信息有关的邮件时，禁止使用非公司的个人邮箱；

（七）各应用系统资料为三胞集团所属信息资源，并非私人拥有，需谨慎使用。

第十二条 病毒防控

- (一) 只允许使用三胞集团指定的标准杀毒软件；
- (二) 杀毒软件需定期升级；
- (三) 三胞集团会监测互联网病毒爆发情况，制定病毒爆发应急预案。当出现大面积病毒爆发时，保证员工电脑不被病毒木马入侵。如果发现个人电脑被病毒木马入侵时，员工需做到：

- 1) 立刻联系信息管理中心进行处理；
- 2) 立刻拔掉U盘、网线；
- 3) 立刻关机。

第十三条 密码安全

三胞集团要求所有员工使用应用系统时，需及时修改初始密码。要求如下：

- 1) 长度不小于8位；
- 2) 包含数字、大小写英文或特殊符号；
- 3) 密码需定期更换；
- 4) 不和任何人分享密码；
- 5) 禁止将密码记录在纸上或其他易于泄露的位置。

第十四条 安全意识

新员工加入三胞集团后需提高自己的信息安全意识，内容主要包括：

- (一) 所有员工必须知道最核心的一点：任何恶意将公司核心数据信息外泄的行为，均为违法行为，请保护自己的行为；
- (二) 请养成保护个人密码的习惯，并设置复杂性较高的密码；
- (三) 如需进行信息及数据的交互，需先核实对方身份，谨慎处理；
- (四) 离开座位时，请锁屏；下班时，请关机；
- (五) 垃圾邮件、病毒邮件请及时删除；
- (六) 请谨慎下载互联网上未知、有风险的程序软件；
- (七) 请勿随意安装软件，以免病毒入侵。

第十五条 提报政策

每位员工应谨慎对待公司的信息资产，当发现有可疑的泄露、窃取公司信息行为或发现网络、系统遭受攻击时，需在第一时间向信息管理中心进行汇报。

第四章 附则

第十六条 责任岗

- (一) 执行责任岗：集团及下属所有员工；
- (二) 培训责任岗：集团信息管理中心；
- (三) 检查责任岗：集团信息管理中心。

第十七条 罚则

(一) 违反以上政策中要求的内容，一经发现，行为人将受到首次 5 分，之后每次递加 5 分的扣罚；

(二) 任何泄露、窃取、丢失公司核心信息、数据、机密等，但未造成三胞集团经济、客户、社会影响等损失的行为，行为人将受到 20 分的扣罚，另三胞集团有权对行为人进行开除处理；

(三) 任何泄露、窃取、丢失公司核心信息、数据、机密等，并造成三胞集团经济、客户、社会影响等重大损失的行为，行为人将受到 50 分的扣罚，另三胞集团有权对行为人进行开除处理并报案；

(四) 任何故意破坏三胞集团系统、网络，造成重大断网事故，影响三胞集团正常业务开展的行为，行为人将受到 50 分的扣罚，另三胞集团有权对行为人进行开除处理；

(五) 任何利用社会网络资源攻击三胞集团网络系统，及利用公司网络系统攻击社会网络资源的行为，行为人将受到 50 分的扣罚，另三胞集团有权对行为人进行开除处理并报案；

(六) 任何在网络上恶语诋毁公司，造成三胞集团经济、客户、社会形象损失的行为，行为人将受到 50 分的扣罚，另三胞集团有权对行为人进行开除并报案；

(七) 任何因个人信息安全意识薄弱间接造成三胞集团重大损失的行为，行为人将受到 5 分，之后每次递加 5 分的扣罚。另三胞集团有权对行为人进行开除处理；

(八) 任何发现他人有以上违反行为的员工，经信息管理中心核实他人确实有违反行为后，将受到首次 5 分，之后每次递加 5 分的奖励。

第十八条 本制度自发布之日起生效，以下制度废止：

- （一）《三胞集团信息安全政策（试行）》三集信企[2015] 第一版；
- （二）《三胞集团互联网使用管理办法》三集信[2016]第一版；
- （三）《三胞集团机房管理制度（试行）》三集信企[2012]第一版；
- （四）《三胞集团数据库使用的管理制度》三集信企[2011]第一版。

第十九条 本制度的解释权归集团信息管理中心。