**信息技术服务管理**

**体系文件**

**信息安全管理程序**

**ZRXX-20000-IS-P-01**

**logo**

广东科技有限公司

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 发布版本 | V1.0 | 文件密级 | 🞏 普通 | 🗹 敏感 |
| 受控状态 | 受控 | 实施日期 | 2018年01月01日 | |

**变更记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **版本** | **变更履历** | **变更人/变更日期** | **审核人/审核日期** | **批准人/批准日期** | **发布人/发布日期** |
| V0.1 | 新建 | **2017-11-15**  **邓全** |  |  |  |
| V1.0 | 正式发布 | **2017-12-13**  **邓全** | **2017-12-14**  **张震** | **2017-12-15**  **李南** | **2017-12-15**  **林欣** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**目 录**

[1 文档介绍 3](#_Toc375643020)

[2 术语、定义和缩略语 3](#_Toc375643021)

[3 内容 3](#_Toc375643022)

[3.1 角色及职责 3](#_Toc375643023)

[3.2 信息安全政策 3](#_Toc375643024)

[3.3 资产分类和风险评估 3](#_Toc375643025)

[3.4 人力资源安全 4](#_Toc375643026)

[3.5 物理与环境安全 4](#_Toc375643027)

[3.6 通讯、操作及访问控制 5](#_Toc375643028)

[3.7 法律法规符合性 5](#_Toc375643029)

[3.8 IT服务过程信息安全管理 5](#_Toc375643030)

[4 文件记录 6](#_Toc375643031)

# 文档介绍

本文档编写的目的是保护公司为客户所维护的基础设施、信息系统及其所存储的信息资产，确保其机密性、完整性和可用性，增强公司IT服务人员的信息安全意识。

# 术语、定义和缩略语

|  |  |
| --- | --- |
| **术语/定义** | **说 明** |
| 资产 | 任何对组织有价值的事物 |
| 信息安全 | 对信息机密性、完整性和可用性的保护 |
| 机密性 | 确保信息只能由那些被授权的人访问 |
| 完整性 | 确保信息的正确性和未经破坏 |
| 可用性 | 保证经授权的用户可以在需要时访问到信息和相关的资产 |

# 内容

## 角色及职责

|  |  |
| --- | --- |
| **角色** | **职责** |
| 信息安全管理经理 | 负责信息安全管理 |
| 信息安全员 | 执行信息安全管理经理分派的任务 |

## 信息安全政策

信息安全规范文件应由公司负责人审核批准，并公布与传达给公司所有员工与相关外部团体。

信息安全规范文件应定期回顾，如果公司的业务活动、基础设施或外部相关的政策法规发生了重大的改变，需要立即重新进行信息安全政策文件的检查和评估，并通过管理层的审核，以确保其持续的适用性、可操作性及有效性。

## 资产分类和风险评估

应明确公司所有重要信息资产及对资产进行风险评估，所有者要确保资产受到合适的保护，对于不可接受风险需要采取纠正措施，公司规定风险值高于12为不可接受风险。资产分类及风险评估参见相关指南，资产分类及风险评估记录在《信息安全资产清单及风险评估报告》。

信息安全管理经理应根据信息资产的价值、法规要求、敏感度和对组织的重要程度不同对其进行分类，不同级别的信息资产要有适合其相应安全保护要求的控制措施。

## 人力资源安全

建立并将信息安全相关的控制贯穿于公司的人力资源流程中，对于关键岗位需要建立相关的安全监督机制；确保员工、合同方和第三方人员在雇佣前、雇佣中或离职以及雇佣关系变更时都以一种有序的方式进行。

应根据公司的信息安全管理要求明确定义员工、第三方人员的安全角色和责任，并记录在职责描述中；并且根据相关的职责，制定相关的信息安全基本行为准则和安全操作准则。

对所有员工、第三方人员要开展合适的安全意识培训和教育，确保其了解公司的信息安全管理流程，以减少人为错误、偷窃、欺诈及滥用设施所带来的安全风险。如果出现了任何违反信息安全政策的行为并造成损失的，要依照公司规定和国家相关的法律法规进行处罚。

具体见《人员聘用管理制度》、《培训教育管理制度》、《工员离职管理程序》。

## 物理与环境安全

员工上下班出入公司应佩挂员工卡。对未按规定佩挂员工卡者，公司管理部门有权纠正。

办公区域大门常闭。

公司管理部门人员要忠于职守，严格岗位责任制，努力增强服务意识，对来访客人礼貌服务，在不能确认是否公司员工时，必须进行询问。

外来人员在前台《来访登记一览表》上登记后等待接待部门接待，若需进入公司办公区域，由接待人员陪同方可进入办公区。

快递、送货人员、运输公司提货人员、垃圾清运人员不得进入公司工作区域，若需进入办公区域在《来访登记一览表》上登记后由公司管理部门相关人员陪同方可进入指定区域搬运相关物品。公司管理部门相关人员应注意跟踪管理。

机房或机柜的访问必须有系统管理员陪同，并填写《机房访问记录单》。

## 通讯、操作及访问控制

网络自身的设计、构建和使用应满足安全控制的要求，并部署必要的基于网络的安全技术和手段。公司网络结构见《网络拓扑图》。

网络设备在运行维护过程中应严格遵照安全技术规范和操作指南，所有网络设备接入、配置变更、设备废弃或更换应遵循变更流程，所有变更实施过程都必须记录在案。

第三方组织人员必须在公司网络管理员陪同下才能操作相关设备，并做好相关记录。

应保障存储介质使用和保管的安全。废弃的存储介质应确保被安全销毁，其中存储的敏感信息被彻底消除或覆盖，不会造成信息泄漏。将任何含有敏感信息的信息系统设备或存储介质带到公司以外之前必须得到授权，并保障其处于妥善保管和安全控制之中，移动介质的使用需要填写《可移动介质涉密使用记录》。

基础设施及信息系统都必须具备访问控制机制，防止未经授权的访问和信息泄漏。

对信息系统的访问授权，不能超过员工工作所需的范围，以减少信息被滥用的风险。访问必须授权，需要填写《用户授权申请表》。公司需要做好访问授权控制的记录，需要及时更新《访问控制列表》。

公司个人电脑和服务器必须安装防火墙和杀毒软件，且开启自动更新，所有设备必须设置屏保。信息安全管理人员必须每年进行一次信息安全检查，对设备病毒防护，容量管理，配置等进行检查。记录在《信息安全检查记录单》中。

## 法律法规符合性

公司的管理必须遵守信息安全相关的国家法律法规、行业规范和组织的相关规定。相关法律法规见《法律法规清单》。

## IT服务过程信息安全管理

针对每个IT服务整理服务级别需求，在服务级别需求中整理信息安全需求和实施范围，对客户IT服务进行风险评估，并记录客户相关IT资产和风险分析信息在《可用性计划》中，根据风险分析结果为每个IT服务设计《IT服务信息安全实施规范》，在IT服务过程中遵守规范实施，并按《服务报告管理程序》监控和记录安全状态，在《可用性报告》中提交信息安全报告内容。

在服务过程中发生信息安全事件，按《事件管理程序》要求实施管理。

IT服务信息安全实施规范的更新通过变更管理实施。参照《变更管理程序》。

# 文件记录

ZRXX-20000-IS-G-01《资产识别指南》

ZRXX-20000-IS-G-02《风险分析指南》

ZRXX-20000-IS-R-01《信息资产登记表》

ZRXX-20000-IS-R-02《来访登记一览表》

ZRXX-20000-IS-R-03《机房访问记录单》

ZRXX-20000-IS-R-04《网络拓扑图》

ZRXX-20000-IS-R-05《可移动介质涉密使用记录》

ZRXX-20000-IS-R-06《用户授权申请表》

ZRXX-20000-IS-R-07《访问控制列表》

ZRXX-20000-IS-R-08《信息安全检查记录单》

ZRXX-20000-IS-R-09《IT服务信息安全实施规范》