# **服务方案**

## 售后服务体系

### 遵循标准

中国联通集团在本项目的实施和服务过程中遵循ISO9001：2000质量管理体系要求。

联通公司的IT服务管理遵循ITIL最佳实践和ISO/IEC 20000国际标准体系，覆盖服务管理、战略规划、服务设计、服务转换、服务交付和持续改进的全生命周期。

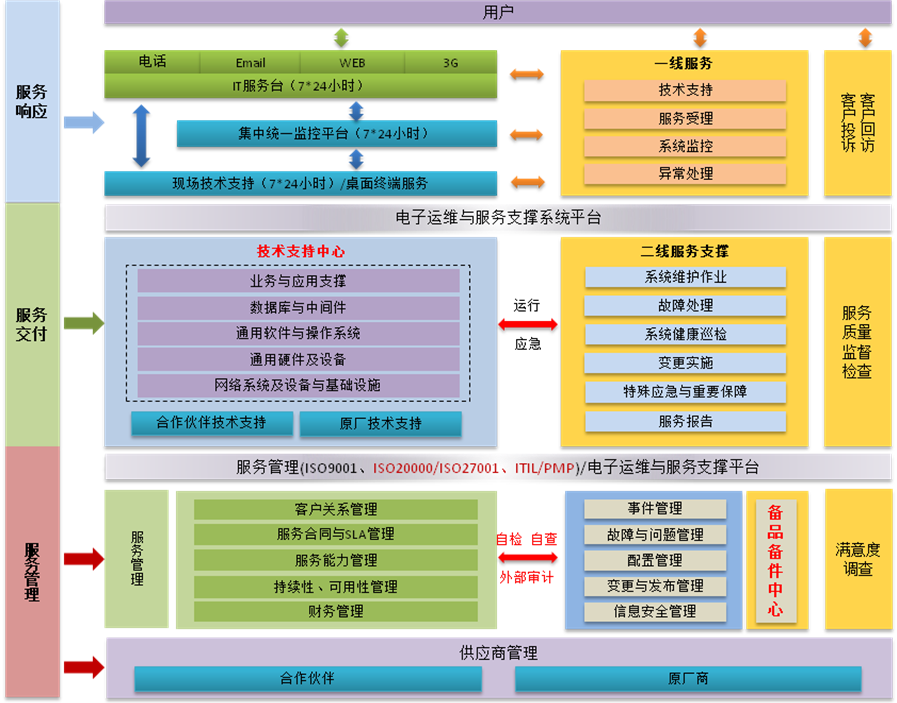
联通公司的信息安全管理遵循ISO/IEC27001国际标准，建立、实施和维护信息安全管理系统。制定信息安全策略，确定体系范围，明确管理职责，通过风险评估确定控制目标和控制方式。覆盖安全策略、信息安全组织、资产管理、人力资源安全、物理和环境安全、通信和操作管理、访问控制、信息系统获取、开发和维护、信息安全事件管理、业务连续性管理、符合性等多个主题，定义了多个安全控制项。

### 服务体系

在IT服务生命周期中，联通公司根据客户需求，为客户提供标准化服务、高级服务、定制服务等分级服务。提供信息及通讯技术系统集成服务、基础设施和信息系统维护、维保服务。

在IT服务管理中，联通公司遵循创造IT服务价值、提升服务质量和降低运营成本的服务方针，为客户提供IT服务咨询、信息系统运行维护、通用软件与设备维保、信息安全评估与系统加固、系统优化改造与测试等服务。

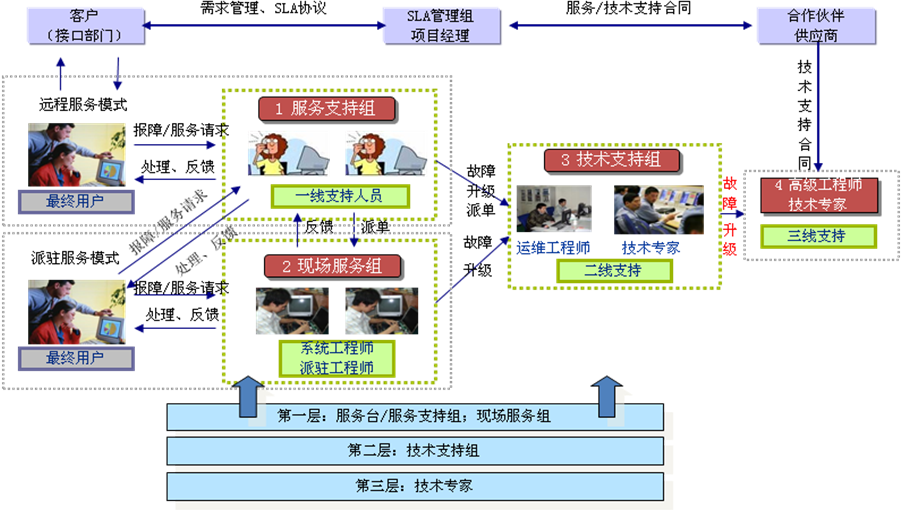
联通公司为客户建立成熟的、符合客户需求的服务体系，覆盖服务响应、服务交付、服务管理的IT服务管理全过程。以IT服务台作为IT服务用户的唯一接触窗口，响应用户服务需求，跟踪服务过程，作为服务闭环反馈服务结果。建立物理和人员集中的统一监控平台，利用客户已有监控平台或工具，提供7\*24小时的系统值班监控，做到主动维护、主动发现、主动处理的主动IT服务。“应用牵头，专业支撑”，实现IT服务交付，完成日常的信息系统运行维护，保证IT服务的连续性和可用性。建立“内部自查，外部审计”的服务管理系统，完成IT服务的业务管理和服务质量管理，保证客户满意度和服务感知。联通公司的服务体系如下图所示：



### 服务响应

中国联通已经建立了全国集中统一的7\*24小时技术服务热线，为客户提供咨询、技术支持、服务请求、故障申告、业务变更、服务投诉等服务。

联通公司依托于全国一体化的集团、省、地市、县四级业务维护体系，具备了完善的客户服务支撑能力，可实现全国快速现场响应。形成“一点受理，统一调度，全国响应”的服务响应体系。并且，为了更好的服务客户，我们将合作伙伴、原厂统一纳入服务响应体系。联通公司的服务响应体系如下图所示：



### 系统故障及响应承诺

针对本项目，中国联通承诺故障发生后5分钟响应，0.5小时提出解决方案并提供如下运维保障：

1、数据连接线路年度定期免费检查，每年1次；

2、重大节日、敏感日期提供服务值守人员；

3、线路故障能在无法按合同时间维护时提供免费备用服务；

4、我方主动发起系统或产品升级，将与华夏银行股份有限公司信用卡中心协商一致后，完成升级任务。

针对平台系统发生故障，按照故障级别采取响应措施。

级别描述：

|  |  |  |
| --- | --- | --- |
| 序号 | 故障级别定义 | 故障现象描述 |
| 1 | 一级故障（紧急故障） | 因平台原因使系统运行中断，对用户业务的运行有严重影响 |
| 2 | 二级故障（严重故障） | 因平台原因使系统中重要功能受损、主要性能指标下降 |
| 3 | 三级故障（一般故障） | 在系统主要功能及性能指标运行正常的情况下，系统部分功能与性能受损 |
| 4 | 四级故障 | 在系统无故障或不影响用户业务运行的情况下，用户对系统的功能、安装、配置、性能优化或使用方面提出技术咨询服务要求 |

|  |  |  |  |
| --- | --- | --- | --- |
| 故障级别 | 服务请求时间 | 响应时间 |  |
| 电话/传真/E-mail | 现场服务 |
| 一级故障 | 7\*24小时 | 接到服务请求后立即给予答复，提供初步故障诊断分析和解决方案。 | 0.5小时内解决 |
| 二级故障 | 7\*24小时 | 接到服务请求后5分钟内给予答复，提供故障诊断分析和解决方案 | 0.5小时内解决 |
| 三级故障 | 7\*24小时 | 接到服务请求后10分钟内给予答复，提供故障诊断分析和解决方案 | 1小时内解决 |
| 四级故障 | 7\*24小时 | 接到服务请求后10分钟内给予答复，提供故障诊断分析和解决方案 | 1小时内解决 |

## 服务方案

### 响应时间

（1）我司进行应用系统性能检测、效能分析，确保对问题能够事先预防，避免出现故障和问题。遇到客户问题均在30分钟内响应。

（2）我司提供7\*24小时响应服务，（包括节假日），如需到客户现场，则每天8:00～18:00期间2小时到达故障现场，其余时间3小时内到达故障现场。

（3）我司承诺若出现以下4种情况保障故障恢复时间：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 事件等级 | 优先级 | 服务水平 | | |
| 响应时间 | 解决问题时间 |  |
| 1 | 紧急 | ≤30分钟 | ≤30分钟 |  |
| 2 | 高 | ≤30分钟 | ≤60分钟 |
| 3 | 中 | ≤30分钟 | ≤90分钟 |
| 4 | 低 | ≤30分钟 | ≤120分钟 |

（4）我司承诺在故障发生24小时内向甲方提供故障报告；

### 在线服务

* 热线服务

在我们维护中心，配有热线电话、值班手机和经验丰富的技术人员，常年7\*24小时通过电话解答用户的技术问题和指导用户解决一般性故障。

* 网上服务

我们在Internet网上设有服务网站对于用户其他要求，可以通过互连网，以E-mail的形式与我们联系，咨询中心设有信箱，接收并及时反馈用户问题或意见。

* 远程维护服务

在用户许可的情况下，对于用户出现的系统和应用软件问题，我们的维护人员将通过远程网络提供实时在线服务，为用户排除故障。

* 现场紧急服务

对于突发的系统故障，如果情况紧急或不便于使用远程手段解决，我们将指派具有丰富经验的技术人员赶赴现场，进行现场技术支持服务。

如果系统在试运行阶段或缺陷责任期内发生故障，业主向承包人发出故障通知后，我方7\*24小时响应（包括节假日），如需到客户现场，每天8:00～18:00期间2小时到达故障现场，其余时间3小时内到达故障现场。

### 技术支持服务

我们将根据要求，提供下列服务：

* 由技术支持部组成专门小组负责客户系统维护支持，如果需要，我公司可委派专门小组长驻现场进行支持。
* 协助客户全部业务网点（单位）上的工作。
* 以技术培训、交流会、合作开发、外出考察等多种形式为客户培养一支精通业务和大数据技术的队伍，并协助用户开发新的大数据应用系统。
* 我司在项目开展前提供开发所需的所有相关技术文档。

### 定期回访

定期回访，了解用户使用情况，解答用户疑问，排除故障。

### 定期升级

在质保期内我公司免费提供质量保证和软件升级、功能完善，并提供现场服务。质保期内我公司承诺将向招标人免费提供对系统软件有所改进、增加新功能以及为适应新标准所做修改的最新版本，供招标人使用，并保证升级后的系统能够稳定的运行。质保期内我公司承诺将根据国家有关管理要求的变化，免费对接口系统软件进行修改、调整。

### 服务档案

从项目启动开始，单独为本项目建立服务档案，包括设计、使用、维护情况等，并由专人管理，以保证提供的售后服务准确、周到、及时。

# **数据安全性**

## **稳定性保障**

1)对系统间的数据传输，保证数据的一致性，完整性，准确性要求达到99%；

2)对客户输入的数据进行合法性检查，确保流程的通畅性；

3)系统整体连续7x24小时不间断向合作方提供服务。基于高并发、高可用分布式集群技术，保证关键业务服务24小时不中断，满足各行业客户的需求；

4)如因数据源对系统进行调整、升级、扩容等措施而导致服务中断，以及因为网络、设备等因素，造成服务的延时、修改以及暂停等情况，风控运维团队保证在获知前述情况的24小时内通知合作方。通过高质量的运维能力，提供平台、数据、业务三位一体的全方位支撑与防护能力。

## **安全性保障**

通过数据分析、数据清洗、数据转换、数据校验、数据冲突、数据标准、数据安全错误预警等过程，对数据质量进行全程管理，保证数据完整性，提高数据准确性和鲜活性，建立数据的权威性。

### **安全性保障**

1)全平台安全审计、权限隔离、完整性、隐私保护；

2)应用数据与发布数据隔离存放、独立控制；

3)数据脱敏分析，本地加密；

4)互联网通信加密、鉴权认证。平台搭建在联通私有云环境，合作伙伴接入开放平台时，需要通过统一接入平台并经过4A认证，操作痕迹可查可溯；

5)大数据运维团队提供7x24小时的运维保障，依靠完整的监控预警体系，可对各个层面进行监控和预警；

6)大数据安全团队每天都会对开放平台租户访问痕迹进行安全审计，对于可疑路径进行专项排查。

7）我司确保技术应用设置防恶意攻击、跨站攻击、注入漏洞等安全规则。

### **数据脱敏**

对敏感信息姓名、手机号、身份证等通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。采用掩码方式保留了部分信息，并且保证了信息的长度不变，对信息持有者更易辨别。

### **访问授权安全**

接口访问需要先进行鉴权，由发起端提供公网出口网络IP地址，进行IP地址网络侧、应用侧导白。未许可的IP地址访问会在网络侧直接拦截。使用HTTPS协议和域名方式进行访问，。

### **数据传输安全**

信息数据以实时、同步方式进行传输，通过HTTPS加密协议，提高信息数据在传输过程中的安全性。相比与HTTP方式的明文传输方式,可以避免出现由于攻击者截取传输报文，直接读懂其中的信息，造成敏感信息泄露的情况；

我司需确保数据双向需实施加密传输机制（使用国密加密算法）。数据传输过程中需使用国密加密算法对数据进行加密，保障数据传输安全性。

### **数据存储安全**

使用集群服务器保存提交日志和接口响应信息，实现提交的时间点和返回结果追溯，便于问题排除和解决。多节点服务提高查询性能，避免单点故障（注：接口层级不支持回溯）。

### **数据合规安全**

联通产品涉及到的数据、服务规范均在国家相关法律法规与政策所许可的范围内与合作方进行合作，并承诺严格遵守工业和信息化部、企业内部制定的规范性文件的要求。

### **数据不沉淀**

我司不可保存采购人传输的用户基本信息，同时数据不可用于除认证服务外的其他非必要应用场景，因我司违规使用采购人数据产生的纠纷、责任等，由我司独立承担责任。