**报告编号：2018-XAPG-LTZX-01**

互联网新技术新业务信息安全评估报告

|  |  |
| --- | --- |
| **委托单位：** | **联通在线信息科技有限公司** |
| **业务名称：** | **联通家庭卫士·亲子守护业务** |

**评估单位：国家计算机网络与信息安全管理中心**

**2019年4月**

目 录

[1 业务基本情况介绍 1](#_Toc529524252)

[1.1 业务名称 1](#_Toc529524253)

[1.2 业务功能介绍 1](#_Toc529524254)

[1.3 技术实现方式介绍 2](#_Toc529524255)

[1.4 （预期）用户规模及市场发展情况 3](#_Toc529524256)

[2 安全评估情况 4](#_Toc529524257)

[2.1 安全评估情况概述 4](#_Toc529524258)

[2.1.1 总体情况 4](#_Toc529524259)

[2.1.2 评估目的 4](#_Toc529524260)

[2.1.3 评估内容 5](#_Toc529524261)

[2.1.4 评估依据 5](#_Toc529524262)

[2.1.5 评估方式 6](#_Toc529524263)

[2.2 评估人员组成 7](#_Toc529524264)

[2.3 评估实施流程 7](#_Toc529524265)

[3 业务安全风险分析 9](#_Toc529524266)

[3.1 安全风险分析表 9](#_Toc529524267)

[3.2 风险说明 14](#_Toc529524268)

[4 配套安全管理措施 16](#_Toc529524269)

[4.1 整体安全保障能力分析表 16](#_Toc529524270)

[4.2 日常安全管理介绍 30](#_Toc529524271)

[4.3 应急管理措施介绍 31](#_Toc529524272)

[4.4 低安全保障能力说明 32](#_Toc529524273)

[5 评估结果及整改建议 33](#_Toc529524274)

[5.1 信息安全管理风险评估结果 33](#_Toc529524275)

[5.2 信息内容安全风险评估结果 33](#_Toc529524276)

[5.3 业务平台安全风险评估结果 35](#_Toc529524277)

[5.4 业务运行安全风险评估结果 36](#_Toc529524278)

[6 安全评估结论意见 39](#_Toc529524279)

[附件一：评估结果签字确认表 40](#_Toc529524280)

[附件二：业务平台安全风险评估结果 41](#_Toc529524281)

[附件三：安全风险整改落实情况 44](#_Toc529524282)

# 业务基本情况介绍

“联通家庭卫士•亲子守护” 是一款面向家庭用户的保护孩子安全上网的产品，可为孩子打造健康的上网环境，提供上网行为监测、上网时长管理、实时位置查询等安全防护功能，全方位的帮助家长守护孩子成长。

## 业务名称

联通家庭卫士•亲子守护业务

## 业务功能介绍

联通家庭卫士•亲子守护业务入口为“联通家庭卫士”微信公众号，用户关注公众号后需要绑定联通手机号码才能登陆使用，登陆后可以添加孩子手机号并授权同意后，可实现号码守护，其主要功能包括：位置定位、上网行为数据分析、上网管理和上网安全防护，同时提供了教育咨询信息等。

位置定位：家长可随时查看孩子定位的位置（此位置是被绑定人使用流量时通过基站测量的位置），也可查询孩子的历史位置，如下图所示。

上网行为数据分析：分析展示孩子上网行为情况，包含： APP使用占比、上网流量情况、上网流量对比、本月APP使用情况、本月上网流量情况、本月新使用APP情况等。

上网管理：家长可实时对孩子进行上网管理，选择禁止或允许孩子上网，也可自定义孩子上网时段。

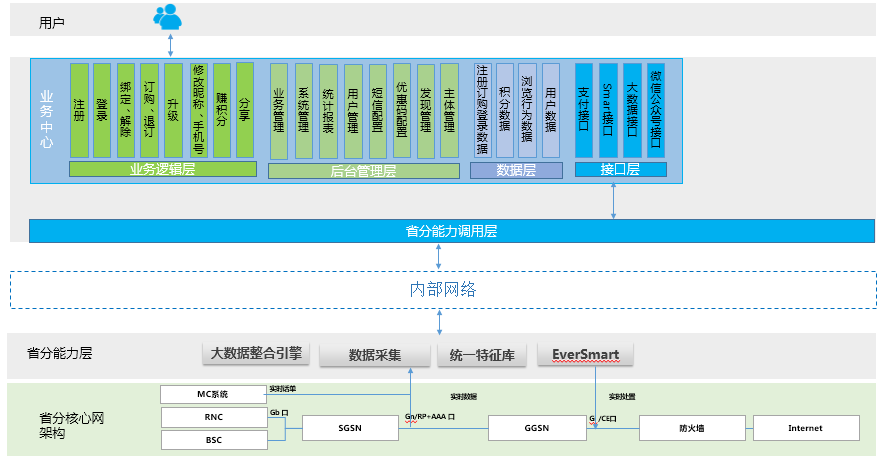
上网安全防护：可在孩子上网过程中检测、阻止访问涉黄赌毒的危险网站。



## 技术实现方式介绍

联通家庭卫士•亲子守护业务平台主要基于管道侧处置能力、恶意地址检测能力、APP识别能力等，将多种优势能力进行扩展。同时结合自身大数据、安全监测技术储备，建设了亲子守护平台，通过划分软件层级结构，层级结构相对独立，每层之间通过接口可灵活调用。

系统全国架构主要采用了中心平台+分布式结构，省系统架构采用了大数据DMP（EverData）、统一特征库、安全资源库、数据采集及EverSmart平台等，系统层级结构如下图所示：



## （预期）用户规模及市场发展情况

目前联通家庭卫士•亲子守护业务尚处于试运营时期，已绑定注册联通用户为XX，日活跃用户数量为XX，预期用户规模在10万至100万左右，用户主要为学生家长。

# 安全评估情况

## 安全评估情况概述

### 总体情况

2019年4月9日，国家计算机网络与信息安全管理中心对对联通在线信息科技有限公司（以下简称联通在线）“联通家庭卫士•亲子守护”业务开展了新技术新业务信息安全现场评估。

评估主要内容包括管理体系评估、业务风险评估和信息安全保障能力评估三个部分。评估方法包括人员访谈、制度文档核实、业务功能验证、内容安全测试、数据安全检测、漏洞扫描、渗透测试等。

本报告主要给出联通家庭卫士•亲子守护业务的信息安全评估情况。

### 评估目的

为进一步提升联通在线公司新技术新业务的信息安全防护和处置能力，依据新技术新业务信息安全评估相关政策文件，结合通信安全分级保护、风险评估的基本方法和标准，发现并找出新技术新业务相关的管理制度、业务流程、网络系统、服务器以及应用系统等方面存在的安全漏洞和隐患。目的是为企业健全互联网新技术新业务管理制度、完善业务流程、提早启动保障措施、加固系统和网络漏洞提供参考和依据，进而提高业务系统的安全防护水平，为业务的发展创造安全可靠的环境。

### 评估内容

新技术新业务安全评估工作主要涉及管理、业务和信息安全保障等方面的安全因素。管理方面，主要采用访谈调研、相关文件查阅的方式，查找管理方面存在的漏洞；业务方面，主要采用人员访谈、功能演示、业务试用、流程梳理等方式，查找业务方面存在的漏洞或隐患；信息安全保障能力方面，主要通过内容测试、漏洞扫描、渗透测试等手段，查验现有信息安全技术保障措施是否满足基本要求。各方面的评估重点如下：

（1）管理体系方面：重点评估新技术新业务的信息安全管理体系和业务安全管理措施是否满足电信管理机构的安全管理要求，具体包括机构设置、管理制度、信息安全相关要求和技术标准以及具体执行情况。

（2）业务风险方面：评估新技术新业务的完整业务流程，结合业务功能属性及技术实现，包括内容发布审核、业务边界安全、权限管理、用户信息保护等，评估系统潜在的信息安全风险。

（3）信息安全保障能力方面：评估现有的安全管理措施、技术手段等信息安全保障能力是否能够有效控制业务信息安全风险。开展内容过滤机制测试；对业务系统、操作系统、网络设备进行安全检测；通过渗透测试查看系统安全防护情况等；

（4）其他：评估新技术新业务相关系统的安全性。

### 评估依据

**（1）政策法规依据**

《网络安全法》

《基础电信企业信息安全责任管理办法（试行）》

《互联网新技术新业务信息安全评估管理办法（试行）》

《关于开展基础电信企业网络与信息安全责任考核有关工作指导》

《互联网用户账号名称管理规定》

**（2）安全标准**

《互联网新技术新业务安全评估指南》

《电信网和互联网安全防护管理指南》

《电信网和互联网安全风险评估实施指南》

《电信网和互联网灾难备份及恢复实施指南》

《电信网和互联网物理环境安全等级保护要求》

《电信网和互联网物理环境安全等级保护检测要求》

《电信网和互联网管理安全等级保护要求》

《电信网和互联网管理安全等级保护检测要求》

《2018年省级基础电信企业网络与信息安全工作考核要点与评分标准》

### 评估方式

本次信息安全评估的主要方式包括人员访谈、文档材料核查、业务功能验证、内容安全测试和安全测评等。

人员访谈主要是通过对网络与信息安全管理人员、特定业务管理人员、技术维护人员进行访谈获取企业信息安全管理、业务应用及平台安全、安全保障措施等方面的现状。

文档材料核查主要是指对企业信息安全、业务安全等相关制度的制定情况进行核实。

业务功能验证通过检查业务功能和流程，对业务应用和系统平台潜在的安全风险做出研判。

内容安全测试主要用于评估企业内容安全相关的保障能力，包括违法及不良信息样本的识别检测、传播扩散控制等方面。

安全测评主要针对业务平台安全和数据安全，涉及漏洞分析、渗透测试等技术手段。

## 评估人员组成

|  |  |  |
| --- | --- | --- |
| **姓名** | **职称/职务** | **职责** |
| 李鹏霄 | 高级工程师 | 评估组长 |
| 王 磊 | 工程师 | 评估测试 |
| 王 祥 | 工程师 | 评估测试 |
| 段运强 | 工程师 | 评估测试 |
| 王 鑫 | 工程师 | 远程测试 |

## 评估实施流程

评估实施流程包括评估准备、现场评估、评估总结三个阶段：

（1）评估准备

成立评估小组，确定小组成员，收集业务相关的管理文档、技术文档、业务市场发展情况、业务自身情况、企业现有的安全管理和保障措施等信息，充分了解业务的使用流程。并根据业务网络访问情况开展前期初步测试和预评估。根据业务情况与被评估方进行深入交流，明确评估重点。

（2）现场评估

现场评估包括管理制度核查、业务安全测试、内容安全测试、系统漏洞检测、设备安全检测五个方面内容。采用人员访谈、内容安全测试、网络安全扫描和渗透测试等方式对企业信息安全管理、业务和技术风险、保障能力进行综合评估。

（3）评估总结

评估总结阶段对评估结果进行综合分析，形成评估结论，撰写评估报告，并提出合理化的整改建议。

# 业务安全风险分析

## 安全风险分析表

联通家庭卫士•亲子守护业务的整体风险识别过程如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **风险类型** | **FX编号** | **业务安全风险评估要点** | **评估意见** | **评估记录** |
| 业务应用安全风险 | 01-FX-01 | 评估人员通过人员访谈的方式，了解被评估业务的用户规模、用户类型、用户之间的相关性（即用户之间是否存在交互关系） | 涉及 | 当前业务尚处于试运营阶段，用户量为XX，预期用户规模为10万至100万；用户主要为学生家长，用户之间并不存在交互关系。 |
| 01-FX-02 | 评估人员通过人员访谈、演示查验等方式，了解被评估业务是否能够确保用户身份信息真实性，如用户注册过程中是否要求提供真实身份信息等。 | 涉及 | 用户关注微信公众号后，注册时需为联通手机号，并接收短信验证码注册登录。 |
| 01-FX-03 | 评估人员通过测试验证的方式，检查被评估业务是否具备用户真实身份鉴别功能，是否存在身份仿冒或欺骗的可能。 | 涉及 | 在业务使用过程中，主要通过绑定手机号及手机动态验证码方式来判别用户真实身份。 |
| 01-FX-04 | 评估人员通过人员访谈的方式，检查是否制定了会话失效机制、身份认证失效机制。 | 涉及 | 建有会话失效机制以及身份认证失效机制 |
| 01-FX-05 | 评估人员通过人员访谈、演示查验等方式，了解被评估业务中公共信息的可审核性，承载的信息格式是否包括简单文本，以及文本、图片、语音、视频等审核难度较高的信息格式或文件。 | 涉及 | 在业务栏目中设置有热点新闻推荐，包括文本、图片等格式。 |
| 01-FX-06 | 评估人员通过人员访谈、文件审查等方式，了解业务发布的公共信息是否具有多样性属性（即是否包含多类主题信息）。 | 涉及 | 所涉及公共信息不具备多样性的特点 |
| 01-FX-07 | 评估人员通过人员访谈、文件审查、测试验证等方式，了解业务公共信息内容的相关性（即信息内容是否围绕相近的主题）。 | 涉及 | 所涉及公共信息主要为教育资讯 |
| 01-FX-08 | 评估人员通过人员访谈、演示查验等方式，了解业务语言类型是否包含小语种信息。 | 不涉及 | 不涉及小语种信息 |
| 01-FX-09 | 评估人员通过人员访谈、演示查验等方式，了解业务中公共信息产生方式，即确认是否包含第三方或用户发布的信息。 | 涉及 | 在业务栏目中设置有热点新闻推荐，但不包括用户发布信息 |
| 01-FX-10 | 评估人员通过人员访谈、演示查验等方式，了解业务平台支持的信息传播方式，是否支持点对点、点对多点、多点对多点及裂变式传播。 | 不涉及 | 该业务不包含该功能属性 |
| 01-FX-11 | 评估人员通过人员访谈、演示查验等方式，了解业务支持的通信媒介，即业务平台的信息是否可以分享至其他平台，或可跨越网络类型传播。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-FX-12 | 评估人员通过人员访谈、演示查验等方式，了解业务平台信息传递实时性属性，即在向用户推送新消息时是否是直接明示信息内容，是否允许用户修改系统设置实现信息的隐藏。 | 不涉及 | 该业务不包含该功能属性 |
| 01-FX-13 | 评估人员通过人员访谈、演示查验等方式，了解业务中信息收取方式，即用户获取信息包含的类型有如下几种：用户主动订阅或申请，系统主动推送等。 | 不涉及 | 该业务不包含该功能属性 |
| 业务平台安全风险 | 02-FX-01 | 评估人员通过人员访谈、文件审查等方式，了解业务系统网络拓扑结构中设备位置分布情况。 | 涉及 | 业务涉及的服务器位置均位于境内 |
| 02-FX-02 | 评估人员通过人员访谈、文件审查等方式，了解业务平台系统资源调度方式，是否采用云计算技术或云服务方式。 | 涉及 | 云主机所在物理机房为沃云杭州资源池 |
| 02-FX-03 | 评估人员通过人员访谈、文件审查等方式，了解业务平台系统资源调度方式，是否采取了内容分发网络（CDN）技术情况。 | 不涉及 | 未采用CDN技术 |
| 02-FX-04 | 评估人员通过人员访谈、文件审查等方式，了解业务合作模式/服务模式是否满足合规性要求，即核实业务合作模式/服务模式是否满足相关行业管理规定，或合作/用户是否具备开办业务的相关资质。 | 涉及 | 联通在线具有增值许可等相关资质 |
| 02-FX-05 | 评估人员通过人员访谈、文件审查等方式，了解业务运营在合作（技术合作和服务合作）开展前是否对合作方信息安全保障能力（管理制度和技术手段）进行了评估，并形成了相关文档。 | 涉及 | 亲子守护业务由联通在线公司运营，并与恒安嘉新开展了技术和服务合作。本次评估未见到对合作方安全保障能力评估文档。 |
| 02-FX-06 | 评估人员通过人员访谈、文件审查等方式，了解业务系统是否开放API接口。 | 涉及 | 业务系统未开放API接口 |
| Web应用安全风险 | 03-FX-01 | 评估人员通过人员访谈的方式，检查该业务应用是否存在多级账号，导致越权的风险及特权账号滥用等问题。 | 涉及 | 后台管理系统涉及到多级账号，但是对于不同账号和角色分别指定有相应的权限 |
| 03-FX-02 | 评估人员通过人员访谈的方式，查看是否制定有日志记录规范，且承诺能够在运营过程中按系统威胁日志留存管理规范进行日志记录与管理工作。 | 涉及 | 按照规范进行日志记录与管理 |
| 03-FX-03 | 评估人员通过文件审查和人员访谈的方式，检查是否制定有应用系统与安全设备配置安全规范或软件安全开发规范并且承诺能够对相关系统的Web应用服务及相关协议及时修复已公布的漏洞。 | 涉及 | 按规范对漏洞进行及时修复 |
| 客户端安全风险 | 04-FX-01 | 评估人员通过人员访谈的方式，查询是否有客户端软件版本管理、版本更新发布机制。 | 不涉及 | 该业务不包含该功能属性 |
| 04-FX-02 | 评估人员通过人员访谈的方式，查询是否有相关的软件安装、更新、运行、卸载相关的开发规范与用户告知说明。 | 不涉及 | 该业务不包含该功能属性 |
| 04-FX-03 | 评估人员通过人员访谈的方式，了解客户端软件是否具备联网功能。 | 不涉及 | 该业务不包含该功能属性 |
| 04-FX-04 | 评估人员通过人员、演示查验的方式，了解客户端软件是否存在恶意行为，如系统提权、监听用户操作、窃取用户隐私等。 | 不涉及 | 该业务不包含该功能属性 |
| 04-FX-05 | 评估人员通过人员访谈的方式，了解是否定期对客户端业务系统进行安全检测并定期修复漏洞。 | 不涉及 | 该业务不包含该功能属性 |
| 业务逻辑安全风险 | 05-FX-01 | 评估人员通过人员访谈的方式，查询业务是否具有业务订购功能。 | 涉及 | 可订购亲子守护基础版 |
| 05-FX-02 | 评估人员通过人员访谈的方式，查看是否制定了业务认证机制。 | 涉及 | 在业务订购、守护号码绑定过程中均有短信认证通知  待补充 |
| 05-FX-03 | 评估人员通过人员访谈的方式，检查是否制定有业务安全使用的开发相关规范并且承诺在应用开发阶段严格遵守该规范。 | 涉及 | 按规范要求安全开发 |
| 非授权采集风险 | 06-FX-01 | 评估人员通过文件审查的方式，检查与用户签订的用户协议中是否包含收集用户信息的范围、类型及使用目的等内容。 | 涉及 | 协议中声明收集如下信息：  1、家长用户手机号码；  2、被守护用户手机号码及上网数据。 |
| 06-FX-02 | 评估人员通过人员访谈的方式，检查业务系统采集的数据结果是否包含超出明确告知给用户的信息收集范围、类型及使用目的等内容。 | 涉及 | 不包含超范围信息收集或使用 |
| 数据存储风险 | 07-FX-01 | 评估人员通过人员访谈的方式，了解业务系统是否提供面向外部用户的服务。 | 涉及 | 面向个人用户提供服务 |
| 07-FX-02 | 评估人员通过人员访谈的方式，了解业务系统是否存在与公网的访问接口。 | 涉及 | 业务的微信公众号涉及与公网的接口 |
| 07-FX-03 | 评估人员通过文件审查的方式，检查针对业务系统是否制定了网络设备与安全设备配置安全规范。 | 涉及 | 制定了相关规范 |
| 07-FX-04 | 评估人员通过人员访谈的方式，检查在保持系统运行稳定的前提下，针对业务系统是否承诺能够对相关设备的操作系统和关键服务协议及时安装更新或补丁。 | 涉及 | 根据相关的安全规范要求对相关操作系统及关键服务协议进行更新 |
| 数据管理风险 | 08-FX-01 | 评估人员通过人员访谈的方式，检查是否对数据信息的访问进行权限管理。 | 涉及 | 对数据信息访问进行权限管理 |
| 08-FX-02 | 评估人员通过文件审查的方式，检查是否制定了相应的应急处置计划和配套的处置措施。 | 涉及 | 制定了应急处置计划 |
| 08-FX-03 | 评估人员通过文件审查、人员访谈的方式，检查是否制定了数据安全监督的相关管理办法。 | 涉及 | 待补充 |
| 数据传输风险 | 09-FX-01 | 评估人员通过人员访谈的方式，查看是否对内部数据传输链路采取了技术防护手段。 | 涉及 | 内部传输链路采取了相应的防护手段 |
| 数据加工风险 | 10-FX-01 | 评估人员通过人员访谈的方式，询问采取的数据加工方式。 | 涉及 | 用户上网数据分析 |
| 10-FX-02 | 评估人员通过人员访谈的方式，询问数据加工中使用的用户数据类型，并与明确告知给用户的数据挖掘范围进行对比 | 涉及 | 上网流量、APP使用情况分析，已明确告知用户数据挖掘范围。 |
| 10-FX-03 | 评估人员通过人员访谈的方式，询问在进行数据分析和挖掘的过程中，是否进行了数据脱敏。 | 涉及 | 数据进行了脱敏处理，数据分析不涉及用户访问内容等 |
| 10-FX-04 | 评估人员需通过人员访谈的方式，询问数据挖掘分析后是否会形成国家关键数据，是否具备相应的保障能力。 | 不涉及 | 不涉及国家关键数据 |
| 数据转移风险 | 11-FX-01 | 评估人员通过人员访谈和文件审查的方式，询问接收数据的第三方的安全防护能力情况。 | 不涉及 | 不涉及数据向第三方转移 |
| 11-FX-02 | 评估人员采用人员访谈和文件审查的方式，询问提供给第三方的数据类型。 | 不涉及 | 不涉及数据向第三方转移 |
| 11-FX-03 | 评估人员采取人员访谈和文件审查的方式，查看与第三方签订的协议中是否包含数据使用权限的内容，以及第三方对数据使用情况调查。 | 不涉及 | 不涉及数据向第三方转移 |
| 11-FX-04 | 评估人员采取人员访谈和文件审查的方式，询问是否对第三方进行必要的安全监督管理，并查阅相关记录。 | 不涉及 | 不涉及数据向第三方转移 |
| 数据删除风险 | 12-FX-01 | 评估人员采取人员访谈和文件审查的方式，询问是否为用户提供删除个人信息的服务。 | 涉及 | 提供账号解除绑定、删除个人信息服务 |
| 业务运行安全风险 | 13-FX-01 | 评估人员通过人员访谈、演示查验等方式，了解被评估业务是否采集、存储、管理、传输、加工、转移、删除能够识别自然人个人身份或反应自然人活动的用户个人信息。 | 涉及 | 传输数据包括用户手机号、位置信息（非精确位置信息，仅为基站大致覆盖范围）等，其中用户手机号传输采用加密的方式，用户位置信息通过接口调用传输给业务系统，业务系统不做存储。， |
| 13-FX-02 | 评估人员通过人员访谈的方式，了解被评估业务的业务逻辑，包括业务规则、业务流程等的合规性和合理性。 | 涉及 | 在业务规则、业务流程合规性方面存在风险，因涉及用户上网隐私行为，应明确该业务添加守护号码是否注册在用户同一身份证号下；且不同手机号可以相互添加守护，与该业务规则不符合。 |
| 13-FX-03 | 评估人员通过人员访谈的方式，了解被评估业务是否包含电信业务涉及的电信网码号资源、电信线路等。 | 不涉及 | 该业务不包含该功能属性 |
| 13-FX-04 | 评估人员通过人员访谈的方式，了解业务是否具有并发语音呼叫、话务转接等功能。 | 不涉及 | 该业务不包含该功能属性 |
| 13-FX-05 | 评估人员通过人员访谈、演示查验等方式，了解业务是否租用语音专线外呼。 | 不涉及 | 该业务不包含该功能属性 |
| 13-FX-06 | 评估人员通过人员访谈的方式，了解被评估业务是否包含码号传送功能。 | 不涉及 | 该业务不包含该功能属性 |

## 风险说明

通过梳理联通家庭卫士•亲子守护业务的应用安全风险、业务平台安全风险、Web应用安全风险、客户端安全风险、业务逻辑安全风险、非授权采集风险、数据存储风险、数据管理风险、数据传输风险、数据加工风险、数据转移风险、数据删除风险，可识别出联通家庭卫士•亲子守护业务主要风险点在于：

（1）01-FX-05、01-FX-09 信息承载格式多样新及信息生成风险：联通家庭卫士•亲子守护业务中发布展示的教育资讯推荐包含有文本、图片等多种信息承载格式，审核难度较高；同时，业务发布信息源由第三方引入（如千龙网等），生成发布的信息不是由运营企业产生，且来源不唯一，给违法信息监测处置带来风险。

（2）02-FX-05 合作风险：本次评估过程中未见到联通在线公司制定对第三方合作单位安全管理办法，同时缺少对联通家庭卫士•亲子守护业务第三方合作单位信息安全责任划分，未发现对合作单位恒安嘉新的信息安全保障能力评估文档。

（3）13-FX-02 业务规则、流程风险：联通家庭卫士•亲子守护业务不同手机号之间可以相互添加为守护号码，能够相互监看手机上网行为，与业务规则要求存在一定差别；同时，由于因涉及用户上网行为分析、上网管理、位置定位等用户个人隐私信息（用户为孩子家长），建议应明确该业务添加守护号码注册在同一用户身份证号下，以避免产生用户隐私信息泄露风险。

# 配套安全管理措施

## 整体安全保障能力分析表

联通家庭卫士•亲子守护整体保障能力分析过程如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **保障能力类型** | **BZ编号** | **企业保障能力评估要点** | **评估**  **意见** | **评估记录** |
| 业务应用安全保障 | 01-BZ-01 | 评估人员通过人员访谈、文件审查等方式，了解是否建立了业务上线前、或用户规模发生较大变化时及时开展评估工作的管理制度，并查看历史评估报告。 | 不合格 | 联通在线建立了相关管理制度，本次未见到历史评估报告。  待补充 |
| 01-BZ-02 | 评估人员通过人员访谈、文件审查等方式，了解是否建立了业务上线前、或用户规模、或业务功能、或基础资源配置、或技术实现方式发生较大变化时及时开展评估工作的管理制度，并查看评估报告。 | 不合格 | 联通在线建立了相关管理制度，本次未见到历史评估报告。  待补充 |
| 01-BZ-03 | 评估人员通过使用验证，针对存在信息发布功能的业务，完成一次用户注册操作，确认是否在注册环节要求用户提供真实身份信息，并通过短信等方式进行验证。 | 合格 | 注册环节通过手机短信进行验证 |
| 01-BZ-04 | 评估人员通过演示查验方式，模拟普通用户变更身份相关信息（如手机号码等），查看是否进行验证。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-05 | 评估人员需查看系统后台记录，是否留存用户身份信息变更日志记录及日志记录内容。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-06 | 评估人员通过测试验证的方式，访问应用的登录界面，查看登录时是否采用人机交互验证策略和机制。 | 合格 | 公众号登录采用短信验证码；  后台管理系统采用图形验证码 |
| 01-BZ-07 | 评估人员通过测试验证的方式，使用网络抓包分析工具抓取登录数据包，查看是否在登录操作的通信过程中是否采用SSL/TLS协议或者其他加密协议或方法确保用户密码的传输安全。 | 合格 | 公众号访问采用了加密传输；  后台管理系统登录账号密码为加密传输；登录时，用户名密码错误提示信息模糊化，如：用户名或密码不正确。 |
| 01-BZ-08 | 评估人员通过测试验证的方式，使用网页分析工具查看是否在COOKIE中保存用户密码。 | 合格 | Cookie未保存用户密码 |
| 01-BZ-09 | 评估人员通过测试验证的方式，检查是否存在用户弱口令。 | 合格 | 后台管理系统密码已具备复杂度，为字母，数据加特殊字符组合 |
| 01-BZ-10 | 评估人员通过访谈、日志查验或测试验证的方式，检查业务系统的身份认证失效机制是否能够按照制定的密码更换周期进行有效提示更新。 | 合格 | 周期性修改密码90天，有提醒 |
| 01-BZ-11 | 评估人员通过访谈或测试验证的方式，检查业务系统的会话失效机制是否能够按照制定的失效时间进行有效执行。 | 合格 | 实际测试，后台管理系统会话失效机制按照制定的失效时间进行有效执行，后台用户登录会话有效期为30min |
| 01-BZ-12 | 评估人员通过测试验证的方式，使用错误的或禁用的账号密码/其他认证/验证码等登录，尝试访问先前正常登陆账号能访问的页面，检查身份认证失效机制和会话失效机制能否仍能有效执行。 | 合格 | 后台管理系统身份认证失效机制和会话失效机制可有效执行，后台用户登录会话有效期30min，验证码有效时间（比如180秒）内，会话提交时，需要检验当前账号的有效性 |
| 01-BZ-13 | 评估人员通过测试验证的方式，查看认证错误提示是否存在泄露信息，当认证失败时，向用户提供的错误信息不应该区分是账号错误还是密码错误，而是通用的提示信息。 | 合格 | 模糊提示 |
| 01-BZ-14 | 评估人员通过人员访谈、文件审查等方式，查看是否建立了用户身份信息保护相关管理制度。 | 合格 | 联通在线建立了相关管理制度 |
| 01-BZ-15 | 评估人员通过人员访谈、使用验证等方式，查看是否配套了必要的技术手段保障用户身份信息的保密性和完整性。 | 合格 | 在用户信息安全保护管理办法中有规定配套建立保障用户身份信息的保密性和完整性 |
| 01-BZ-16 | 评估人员通过人员访谈等方式，了解是否建立覆盖业务所有内容及信息格式的违法信息监测处置的工作机制和技术手段；如是，询问技术手段实现途径与违法信息监测处置流程。 | 合格 | 建立了相关保障制度，同时依托在管道侧部署恶意内容过滤设备对指定上网流量进行安全过滤，对用户浏览的恶意网址进行拦截。 |
| 01-BZ-17 | 评估人员通过演示查验等方式，查看是否留存删除日志记录，查看是否能够调取相关记录。 | 合格 | 能够调取相关记录  待补充 |
| 01-BZ-18 | 评估人员查看是否建立违法信息样本库，查看违法信息样本库的更新记录。 | 合格 | 建立有违法信息样本库 |
| 01-BZ-19 | 评估人员注册账号，以用户身份发送含有违法信息的文字、图像、音频、视频等，确认信息能否发送成功。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-20 | 评估人员通过人员访谈、演示查验等方式，检查是否对图片、语音、视频或小语种等公共信息建立了先审后发机制。 | 不合格 | 未对第三方引入的新闻推荐信息进行审核后发布 |
| 01-BZ-21 | 评估人员通过人员访谈、演示查验等方式，检查公共信息的审核是否采用了技术加人工方式。 | 不合格 | 尚未建立第三方引入公共信息审核机制 |
| 01-BZ-22 | 评估人员通过人员访谈、使用测试等方式，查看在业务使用过程中，是否配备了用户真实身份鉴别管理制度和技术手段。 | 合格 | 通过手机号码与用户进行身份绑定，并采用手机短信验证 |
| 01-BZ-23 | 评估人员通过测试验证方式，针对具备第三方/用户发布信息功能的业务，实际完成一次注册操作，查看在注册环节，是否明确告知用户禁止发布、复制、传播违法信息，是否明确要求用户承诺遵守法律法规(《互联网信息服务管理办法》第十五条)、社会主义制度、国家利益、公民合法权益、公共秩序、社会道德风尚和信息真实性等七条底线。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-24 | 评估人员对用户管理人员进行访谈，针对具备第三方/用户发布信息功能的业务，询问是否根据累计发送违法信息次数等参数对个人账号、公众账号、聊天群组进行安全等级划分；如是，询问等级划分梯度、各等级违法信息处置机制及实现方式等。针对个人账号、公众账号、聊天群组后台数据中是否有安全等级划分及配置相应的处置策略。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-25 | 评估人员查看人员配备文件，针对具备第三方/用户发布信息功能的业务，查看是否配备专门人员管理公众账号，文件中是否含有人员名单和工作联系方式。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-26 | 评估人员查看制度文件、工作手册等，针对具备第三方/用户发布信息功能的业务，是否含有针对公众账号发布的公开信息内容作违法信息日常监测巡查的机制和管理要求。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-27 | 评估人员对公众账号管理人员进行访谈，针对具备第三方/用户发布信息功能的业务，询问违法信息处置方式和流程，是否有相关处置工作的记录。 | 合格 | 联通在线建立了违法信息监测处置工作机制和手段 |
| 01-BZ-28 | 评估人员实际完成一次群组创建，检查是否明示群组人数上限，是否明确告知：a) 不得复制、发布、传播违法信息；b) 群创建者和群管理者对群组负有管理责任，需承诺本群组不发布、传播违法信息。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-29 | 评估人员查验系统配置，是否对群组人数设置上限，是否对群组违法信息的发布、传播进行监测和处置。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-30 | 评估人员通过人员访谈、文件审查等方式，针对具备第三方/用户发布信息功能的业务，检查是否针对信息发布环节的链接转发、添加评论转发、跨平台分享等功能配套了违法信息监测和处置的管理机制和技术手段。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-31 | 针对具备第三方/用户发布信息功能的业务，评估人员分别实际使用一次链接转发、添加评论转发、跨平台分享功能，在有关位置输入违法信息关键字，验证信息是否发送成功。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-32 | 针对具备第三方/用户发布信息功能的业务，评估人员需使用业务，尝试在具有信息联动发布功能的业务平台上发布违法信息，或将违法有害信息分享至其他业务平台上，查看是否具备迅速切断同步或关联关系，并联动删除各关联平台上的违法信息的能力。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-33 | 评估人员需查看系统后台记录，查阅是否留存违法信息联动删除操作日志及日志记录内容 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-34 | 评估人员需使用业务，查看在业务使用前，是否明确告知用户业务推送信息的种类，用户可自主选择是否接收信息，或在业务系统设置是否包含信息推送功能管理的选项 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-35 | 评估人员使用业务，在不同时间段针对业务平台进行若干次访问，或发布若干条公众信息，随后请导出相关的访问记录；或从日志留存系统页面展示相关记录。评估人员需提供一定查询条件，由相关人员在日志留存系统进行操作演示，验证日志留存系统的查询、检索和审计功能。 | 不涉及 | 该业务不包含相关功能属性 |
| 01-BZ-36 | 对于已上线的业务，需请提供满足留存时间要求的日志记录；针对未上线的业务，需请提供日志留存系统设计文件，证明其能够满足留存时间要求。 | 合格 | 满足日志留存时间要求 |
| 业务平台安全保障 | 02-BZ-01 | 评估人员需查看上报给主管部门的业务开办信息，包括业务机房/节点列表、占用机房位置等，并与实际情况进行核对。 | 合格 | 业务涉及的服务器位置均位于境内，云主机所在物理机房为沃云杭州资源池 |
| 02-BZ-02 | 评估人员需查看业务系统拓扑图，并访谈相关负责人员，询问针对境内外交互数据的管理制度，以及配套的技术监管手段。 | 不涉及 | 该业务不包含相关功能属性 |
| 02-BZ-03 | 评估人员需查看业务后台系统实时运行数据和日志记录，核实是对资源分配使用情况进行实时监控和日志记录。 | 合格 | 进行了实时监控和日志记录 |
| 02-BZ-04 | 评估人员需查看关于违法信息监测处置制度文件和技术手段配备情况，核验侧是否可执行行业主管部门下发的违法信息监测和处置指令。 | 合格 | 待补充 |
| 02-BZ-05 | 评估人员需查看留存业务相关日志记录，核实日志的类型、内容和留存时间是否满足相关法律法规要求。 | 合格 | 满足相关法律法规要求 |
| 02-BZ-06 | 评估人员需向询问，是否对合作/用户的业务经营许可资质进行核实，并留存相关资料； | 合格 | 亲自守护业务与微信平台、千龙网合作，对合作公司的经营许可资质进行审核，留存有合作资质审核材料  待补充 |
| 02-BZ-07 | 评估人员需查看与服务对象签订的协议中，是否包含用户需提供真实身份的内容； | 合格 | 服务协议中要求提供用户手机号码 |
| 02-BZ-08 | 评估人员需访谈相关负责人，询问是否建立了针对合作方信息安全保障能力（管理制度和技术手段）评估机制； | 不合格 | 尚未建立针对合作方信息安全保障能力评估机制 |
| 02-BZ-09 | 评估人员访谈相关负责人，询问是否通过开放接口进行交互的数据建立了安全审核机制和技术保障手段。 | 合格 | 该业务不包含相关功能属性 |
| Web应用安全保障 | 03-BZ-01 | 评估人员通过测试验证的方式，分别登陆不同级账号，检查不同级账号在分级页面的权限区别，以确认是否存在不同级别账号的管控。 | 合格 | 账号权限分为系统管理员、系统监控员、系配置理员等多级账号 |
| 03-BZ-02 | 评估人员通过测试验证的方式，登陆超级账户或高权限账户，查看应用是否使用额外的物理验证设备、限制登陆IP或登陆设备手段等对超级账户或高权限账户的使用做出限制。 | 合格 | 限制登陆IP手段对后台管理系统高权限账户的使用做出限制， |
| 03-BZ-03 | 评估人员通过人员访谈的方式，查看是否对业务应用运行状况进行日志记录。 | 合格 | 系统会对业务的运行情况进行日志记录 |
| 03-BZ-04 | 评估人员通过演示查验的方式，查看是否对用户的关键操作、重要行为、业务资源使用情况等重要事件进行日志记录。 | 合格 | 对用户的关键操作、重要行为、业务资源使用情况等重要事件进行日志记录 |
| 03-BZ-05 | 评估人员通过演示查验的方式，查看日志的留存时间长度是否能追溯到最近的6个月内。 | 合格 | 留存时长符合相关要求 |
| 03-BZ-06 | 评估人员通过测试验证的方式，采用Web应用漏洞扫描工具对系统的Web应用服务及相关协议进行漏洞扫描。 | 合格 | 实际测试，后台管理系统存在高危漏洞，详见正文附件二，  sql注入等漏洞，已修复，目前在测试环境 |
| 03-BZ-07 | 评估人员通过文件审查和测试验证的方式，查看应用系统与安全设备配置安全规范或软件安全开发规范中是否有要求对应用会话并发连接数做出限制，并采用压力测试工具和抓包工具进行测试验证，查看实际并发会话通讯情况是否属实。 | 合格 | 开发规范明确相关要求，应用会话并发连接数做出限制  前台web服务并发数采用loadrunner压测测试环境，后台运营系统并发数限制为10个，符合并发数限制 |
| 客户端安全保障 | 04-BZ-01 | 评估人员通过测试验证的方式，检查客户端软件的应用版本的更新机制是否正常。 | 不涉及 | 该业务不包含相关功能属性 |
| 04-BZ-02 | 评估人员通过验证测试的方式，采用Android分析审计工具，分析移动应用在安装、运行、更新时，是否安装了其他应用。 | 不涉及 | 该业务不包·含相关功能属性 |
| 04-BZ-03 | 评估人员通过测试验证的方式，卸载已安装客户端软件，并检查程序文件是否有残留。 | 不涉及 | 该业务不包含相关功能属性 |
| 04-BZ-04 | 评估人员通过测试验证方式，查看客户端中是否存在插件功能，若存在则应对运行的客户端中提供的插件进行规范性检查，插件应允许用户自主选择是否卸载，并且卸载后无残留。 | 不涉及 | 该业务不包含相关功能属性 |
| 04-BZ-05 | 评估人员通过测试验证的方式，采用网络抓包分析工具（Burpsuite/Wireshark等），分析网络传输过程中的敏感数据信息是否加密。 | 不涉及 | 该业务不包含相关功能属性 |
| 04-BZ-06 | 评估人员通过测试验证的方式，采用网络抓包分析工具（Burpsuite/Wireshark等），分析网络传输过程中客户端软件的网络连接的频次是否进行了合理限制。 | 不涉及 | 该业务不包含相关功能属性 |
| 04-BZ-07 | 评估人员通过测试验证的方式，采用Android分析审计工具，检查客户端的敏感权限使用情况，判断在涉及访问本地资源权限时是否正确提示用户授权情况。 | 不涉及 | 该业务不包含相关功能属性 |
| 04-BZ-08 | 评估人员通过测试验证的方式，采用漏洞扫描工具，检查客户端业务系统是否存在高中危漏洞。 | 不涉及 | 该业务不包含相关功能属性 |
| 业务逻辑安全保障 | 05-BZ-01 | 评估人员通过人员访谈的方式，了解业务订购行为是否需用户认证后才会生效。 | 合格 | 需用户认证后生效 |
| 05-BZ-02 | 评估人员通过访谈或演示查验的方式，检查出现超出业务阈值是否会给出安全提示。例如，若单日用同一手机号完成超过业务阀值的订购数量，应通过短信或邮件等形式给予用户安全提示。 | 不涉及 | 该业务不包含相关功能属性 |
| 05-BZ-03 | 评估人员通过测试验证的方式，检查在业务认证未通过时触发的保护策略是否正常运行。 | 不涉及 | 该业务不包含相关功能属性 |
| 05-BZ-04 | 评估人员通过测试验证的方式，验证规范的措施是否正常履行，例如检查核心业务的保障措施是否设置阈值，超过阈值时是否给予提示。 | 不涉及 | 该业务不包含相关功能属性 |
| 非授权采集保障 | 06-BZ-01 | 评估人员通过文件审查的方式，检查是否建立了用户个人信息收集保护及用户授权告知制度。在收集用户个人信息前，获得用户同意，并向用户明确告知授权范畴和风险提示。 | 合格 | 用户服务协议中明确告知用户个人信息授权范畴和风险提示。 |
| 06-BZ-02 | 评估人员通过演示查验的方式，检查业务数据，判定收集用户个人信息的收集范围和使用范围是否遵循以提供服务的最小必要为标准。 | 合格 | 遵循以提供服务的最小必要为标准 |
| 数据存储保障 | 07-BZ-01 | 评估人员通过人员访谈的方式，检查业务系统是否部署了能够防范网络攻击，检测病毒木马等恶意代码入侵的硬件设备或软件系统。 | 合格 | 业务系统部署了能够防范网络攻击，检测病毒木马等恶意代码入侵的硬件设备或软件系统 |
| 07-BZ-02 | 对于业务系统已部署的防范网络攻击和检测病毒木马等恶意代码入侵的硬件设备或软件系统，评估人员通过测试验证的方式，检查是否及时更新了恶意代码软件版本和恶意代码库。 | 合格 | 及时更新恶意代码软件版本和恶意代码库 |
| 07-BZ-03 | 评估人员通过文件审查的方式，检查网络设备与安全设备配置安全规范是否设置有效策略，要求根据数据级别采用加密、授权、数字水印、数字签名等技术手段对业务系统存储的数据进行了安全存储保护。 | 合格 | 在客户信息安全保护管理办法中，明确了客户信息安全管理、数据存储和备份管理要求 |
| 07-BZ-04 | 评估人员通过测试验证的方式，使用漏洞扫描工具对业务系统进行检测，检查是否已对相关设备的操作系统和关键服务协议及时安装更新或补丁。 | 合格 | 对相关设备的操作系统和关键服务协议及时安装更新或补丁 |
| 07-BZ-05 | 评估人员通过人员访谈的方式，检查对于不同安全级别的数据进行权限管理过程中是否采取了相应的隔离措施和安全保护措施。 | 合格 | 联通在线的用户信息安全管理办法中，明确针对跨互联网或不同等级安全域数据传输采取加密等相应防护措施 |
| 07-BZ-06 | 评估人员通过测试验证的方式，检查对业务系统是否采用加密或其他保护措施实现系统管理数据和重要业务数据存储保密性。 | 合格 | 联通在线的用户信息安全管理办法中，明确了对重要数据采取加密进行安全防护。  后台管理系统中，对用户手机号等信息进行了脱敏处理。 |
| 数据管理保障 | 08-BZ-01 | 评估人员通过访谈方式，检查数据操作行为日志记录应至少包括操作时间、操作对象存储地址、操作指示等关键字段 | 合格 | 数据操作行为日志记录关键字段  关键信息从大数据实时获取，本业务系统不存储 |
| 08-BZ-02 | 评估人员通过访谈的方式，检查本地数据备份与恢复功能。 | 合格 | 日志和数据库备份 |
| 08-BZ-03 | 评估人员通过访谈方式，检查异地数据备份功能，如利用通信网络将关键数据定时批量传送至备用场地。 | 不涉及 | 未采用异地数据备份 |
| 数据传输保障 | 09-BZ-01 | 评估人员通过人员访谈的方式，检查是否对数据传输方式采取了相应的安全防护措施。 | 合格 | 采取了相应的防护措施 |
| 09-BZ-02 | 评估人员通过人员访谈的方式，查看是否对内部不同局域网间数据传输链路采取了技术防护手段。 | 合格 | 采取了相应的防护措施 |
| 09-BZ-03 | 评估人员通过人员访谈的方式，查看数据传输链路是否设置了冗余链路。 | 合格 | 采取了相应的措施 |
| 数据加工保障 | 10-BZ-01 | 评估人员通过人员访谈的方式，查看是否对拟采用公有云进行加工的数据重要性进行评估，判定其是否适合采取公有云服务进行加工。 | 合格 | 采用了联通沃云杭州资源池 |
| 10-BZ-02 | 评估人员通过文件审查的方式，查看与云服务签订的服务合约中，是否明确提出云服务不得违规访问数据。 | 合格 | 明确了相关要求 |
| 10-BZ-03 | 评估人员通过人员访谈和文件审查的方式，询问是否建立了数据加工的管理制度，并且明确提出不得超范围进行数据挖掘。 | 合格 | 制定了数据加工的管理制度，并且明确提出不得超范围进行数据挖掘  待补充 |
| 10-BZ-04 | 评估人员通过人员访谈和文件审查的方式，询问是否建立了数据加工的管理制度，并且明确提出数据加工前应对涉及用户个人敏感信息的内容应进行匿名化、模糊化、脱敏处理。 | 合格 | 制定了相关管理制度，明确了用户个人敏感信息处理要求  待补充 |
| 10-BZ-05 | 评估人员通过人员访谈和演示查验的方式，查看据数据挖掘算法中参数变量的设置，是否包含用户个人敏感信息的输入内容。 | 合格 | 不涉及用户个人敏感信息输入内容  待补充 |
| 10-BZ-06 | 评估人员通过人员访谈的方式，询问对数据挖掘分析后形成的国家关键数据的技术防护措施。 | 不涉及 | 不涉及国家关键数据 |
| 数据转移保障 | 11-BZ-01 | 评估人员需对人员访谈或文件审查的方式，询问将数据提供给第三方前，是否对第三方的数据安全防护能力进行评估，并查阅相关评估报告。 | 不涉及 | 数据未提供给第三方 |
| 11-BZ-02 | 评估人员采取人员访谈或文件审查的方式，询问将数据提供给第三方前，是否对数据的重要性、敏感性评估进行评估，并查阅相关评估报告。 | 不涉及 | 数据未提供给第三方 |
| 11-BZ-03 | 评估人员采取人员访谈或文件审查的方式，查看是否建立了数据转移管理制度，包含明示用户数据转移情况，并明确规范第三方数据使用权限。 | 合格 | 建立了相关管理制度  待补充 |
| 11-BZ-04 | 评估人员采取人员访谈或文件审查的方式，询问是否建立了针对第三方数据使用安全监督管理机制和技术手段。 | 合格 | 建立了数据使用安全监督管理机制  待补充 |
| 数据删除保障 | 12-BZ-01 | 评估人员采取人员访谈和演示查验的方式，询问是否在用户终止使用电信服务或者互联网信息服务后，业务系统能够停止收集和使用用户个人数据信息。 | 合格 | 用户终止使用相关服务后，能够及时停止收集和使用用户个人数据信息 |
| 业务运行安全保障 | 13-BZ-01 | 评估人员通过人员访谈、文件审查等方式，了解业务办理过程中是否实施用户二次确认授权机制。 | 合格 | 通过短信验证码二次确认授权 |
| 13-BZ-02 | 评估人员通过人员访谈、文件审查等方式，了解业务办理环节是否单一采用或组合采用短信验证码、图片验证码、语音验证码、智力测试验证码等验证码类型进行用户身份验证。 | 合格 | 主要通过短信验证码方式身份验证  业务系统用户登录采用短信验证码校验  运营管理系统用户登录采用密码+图形验证码+短信验证码方式登录 |
| 13-BZ-03 | 评估人员通过人员访谈、文件审查等方式，对端口类短信下发添加签名，防范不法分子伪造署名假冒企业进行短信下发。 | 合格 | 在短信中添加签名 |
| 13-BZ-04 | 评估人员通过人员访谈、演示查验等方式，了解业务是否合理设置登录密码策略，明确密码长度、强度、复杂度等。 | 合格 | 密码已具备复杂度，字母，数据加特殊字符 |
| 13-BZ-05 | 评估人员通过人员访谈、演示查验等方式，了解业务是否对频繁试错登录、异地登录等业务异常登录情况进行监测。 | 合格 | 对频繁试错登录等进行了监测，并采取限制措施 |
| 13-BZ-06 | 评估人员通过人员访谈、演示查验等方式，了解业务是否通过短信提示、下发验证码二次确认等方式，强化业务登录行为的实时告知。 | 合格 | 后台运营管理系统用户登录采用密码加图形验证码方式+短信验证码登录 |
| 13-BZ-07 | 评估人员通过人员访谈、演示查验等方式，了解业务使用过程中存在通讯信息诈骗高风险的关键环节，是否采用短信验证码、密保问题、图片验证码、语音验证码、智力测试验证码等方式进行用户身份验证。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-08 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严格申请主体资格管控，是否存在违规为个人用户办理语音专线、“400”、“商务总机”业务。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-09 | 评估人员通过人员访谈、文件审查等方式，了解业务是否制定业务管理文件，明确业务在申请主体资格管控、渠道管理、资质核验、码号申请数量管理、台账管理、落地号码管理、外呼管理、合同管理、业务使用复核监测、退出管理、定期检查、考核问责、工作规程管理等关键环节的管理要求。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-10 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严禁代理渠道或网络渠道代为办理。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-11 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严格落实用户实名信息核验登记。基础电信企业应建立用户真实有效身份信息核验登记留存机制，加强个人用户身份信息、单位用户证照信息核验，严格落实电信业务用户实名制。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-12 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严格落实申请数量要求，同一用户在同一基础电信企业全国范围内申请“400”、“一号通”、“商务总机”等重点业务号码，每类原则上不得超过5个。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-13 | 评估人员通过人员访谈、文件审查等方式，了解业务是否严格落实台账管理，“400”、“一号通”、“商务总机”业务台账信息应包括用户资质、使用用途、真实落地号码等。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-14 | 评估人员通过人员访谈、文件审查等方式，了解 “400”、“一号通”、“商务总机”等重点电信业务是否建立业务落地号码核验登记机制。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-15 | 评估人员通过人员访谈、文件审查等方式，了解业务在合同和协议中是否包含登记用户主体责任，细化责任条款。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-16 | 评估人员通过人员访谈、文件审查等方式，了解业务是否利用语音专线进行超频、超时段外呼，利用其他码号等电信资源外呼行为管理是否严格。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-17 | 评估人员通过人员访谈、文件审查等方式，了解业务是否有退出管理。当出现异常情况时，应根据实际情况对相关业务及时予以关停、注销。 | 合格 | 建立了相关业务退出管理机制。  待补充 |
| 13-BZ-18 | 评估人员通过人员访谈、文件审查等方式，了解基础电信企业应配套建立防范打击通讯信息诈骗相关重点电信业务的信息化管理手段。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-19 | 评估人员通过人员访谈、文件审查等方式，了解基础电信企业应配套建立用户终端侧安全提示服务相关技术手段 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-20 | 评估人员通过人员访谈、文件审查等方式，了解语音专线是否实施主叫鉴权。企业应全面落实语音专线主叫鉴权机制，对未按规范进行主叫鉴权的呼叫一律拦截。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-21 | 评估人员通过人员访谈、文件审查等方式，了解语音专线呼叫转移管理是否严格。开通语音专线呼叫转移业务功能，应由基础电信企业集团公司统一审核并建立台账。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-22 | 评估人员通过人员访谈、文件审查等方式，了解是否建立外呼白名单制度，允许外呼的业务号码必须为本网实际开通的、属本企业分配的号码或号段，并统一纳入白名单管理。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-23 | 评估人员通过人员访谈、文件审查等方式，了解企业是否在接入侧设备上禁止违规传送主叫号码为空号或设置主叫号码禁显的呼叫。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-24 | 评估人员通过人员访谈、演示查验等方式，了解企业在网间关口局对不符合号码管理、网间互联规定和标准的违规呼叫、违规号码是否进行拦截。 | 不涉及 | 该业务不包含相关功能属性 |
| 13-BZ-25 | 评估人员通过人员访谈、文件审查等方式，了解建立不良呼叫号码监测处置能力。 | 不涉及 | 该业务不包含相关功能属性 |

## 日常安全管理介绍

联通在线公司主要制定了以下的网络与信息安全方面的管理制度：

《联通宽带在线有限公司客户信息安全保护管理办法》

《中国联通网络与信息安全管理办法》

《联通在线信息科技有限公司互联网新技术新业务信息安全评估管理办法（试行）》

《应急响应预案》

《信息分类与密级控制策略》

**（一）在信息安全组织机构方面**

**（二）在新技术新业务信息安全评估方面**

待补充

**（三）在信息安全责任管理方面**

待补充，定期对从业人员开展信息安全意识教育和安全技能考核，以及相关网络信息安全培训。

待补充

**（四）用户真实身份管理方面**

待补充

**（五）在违法信息监测处置方面**

联通家庭卫士•亲子守护业务建立了信息安全保障管理制度和机制，明确了信息安全事件报告处置流程以及信息安全责任要求，建立了联通家庭卫士•亲子守护业务黑名单管理机制。同时与百度等企业合作建立了违法不良信息样本库，能够依托在管道侧部署恶意内容过滤设备对指定上网流量进行安全过滤，对用户浏览的恶意网址进行拦截。

**（六）在日志留存方面**

系统日志记录业务系统中的系统安全事件、用户访问记录、系统运行日志、系统运行状态等各类信息；包含时间、操作内登陆IP等关键字段；支持查询、统计等关键操作。

## 应急管理措施介绍

**（一）总体的应急管理策略**

待补充，联通在线公司建立了安全事件应急管理办法，

**（二）联通家庭卫士•亲子守护业务的应急管理策略**

联通家庭卫士•亲子守护业务制定了系统应急预案，以应对业务系统突发事件和异常事件的处理，明确了应急预案的启动条件和执行原则，对常见的故障应急处理措施进行了说明，并包括了预防保障措施和业务测试方案，确定了业务应急联系人员。此外，在安全保障措施中明确了信息安全事件应急处置流程、信息安全教育培训演练、信息安全事件通报等内容。建议进一步补充完善对违法信息应急处置、信息内容安全方面的应急管理措施和处置流程，提高应急管理规范性和有效性。

## 低安全保障能力说明

通过梳理联通家庭卫士•亲子守护业务的业务应用安全保障、业务平台安全保障、Web应用安全保障、客户端安全保障、业务逻辑安全保障、非授权采集保障、数据存储保障、数据管理保障、数据传输保障、数据加工保障、数据转移保障、数据删除保障、业务运行安全保障等方面的安全保障能力，存在低保障能力环节主要包括：

（1）01-BZ-01/01-BZ-02：本次评估未见到联通家庭卫士•亲子守护业务试运营前安全评估报告。

（2）01-BZ-20/01-BZ-21：联通家庭卫士•亲子守护业务尚未建立第三方引入的新闻推荐信息的审核机制，包括人工或技术方式。

（3）02-BZ-08：联通家庭卫士•亲子守护业务尚未建立针对合作方信息安全保障能力（管理制度和技术手段）评估机制，未形成相关评估记录文档。

（4）03-BZ-06:存在网络安全高危漏洞，详见附件二。

# 评估结果及整改建议

联通家庭卫士•亲子守护业务涉及多个业务风险点，针对这些风险点，联通在线公司主要依赖其配套安全管理措施进行风险管控，通过这些保障措施主要风险点基本处于可管可控的水平，但部分风险点仍缺乏匹配的保障能力（01-FX-05、01-FX-09 02-FX-05、13-FX-02）。同时也发现部分保障能力措施呈现低水平状态（01-BZ-10、01-BZ-20/01-BZ-21、02-BZ-08、03-BZ-06）。详细情况及整改建议如下：

## 信息安全管理风险评估结果

联通在线公司建立了一些列网络与信息安全方面的管理制度，包括XXXX、XXXX、XXXX等制度，管理制度体系较为完善，基本满足信息安全管理要求。同时，建议联通在线公司进一步完善信息安全事件应急处置管理制度和机制，提升对违法不良信息和信息安全事件应急处置保障能力，同时进一步加强对第三方合作企业安全管理，强化合作企业信息安全责任意识，确保合作企业建立相关配套安全保障措施，满足信息安全保障能力要求。

## 信息内容安全风险评估结果

1.违法不良信息传播风险

风险类型：违法不良信息传播风险

风险描述：联通家庭卫士•亲子守护业务引入第三方新闻推荐内容，尚未建立审核机制，存在违法不良信息传播风险。

整改建议：建议对引入的第三方新闻推荐内容建立先审后发机制，并建立完善违法信息监测处置工作机制和技术手段，降低违法不良信息传播风险。



## 业务平台安全风险评估结果

1. 合作风险

风险类型：合作风险

风险描述：尚未建立对第三方合作单位安全保障能力评估机制，但通过访谈以及核查相关文档，未发现联通家庭卫士•亲子守护业务对合作方开展信息安全保障能力评估

**整改建议:** 建议联通在线公司建立对合作单位信息安全保障能力评估机制，评估合作企业的信息安全管理工作及保障措施能否满足相关法律法规要求、能否保障业务的信息安全。

## 业务运行安全风险评估结果

3.业务规则风险

风险类型：业务规则风险

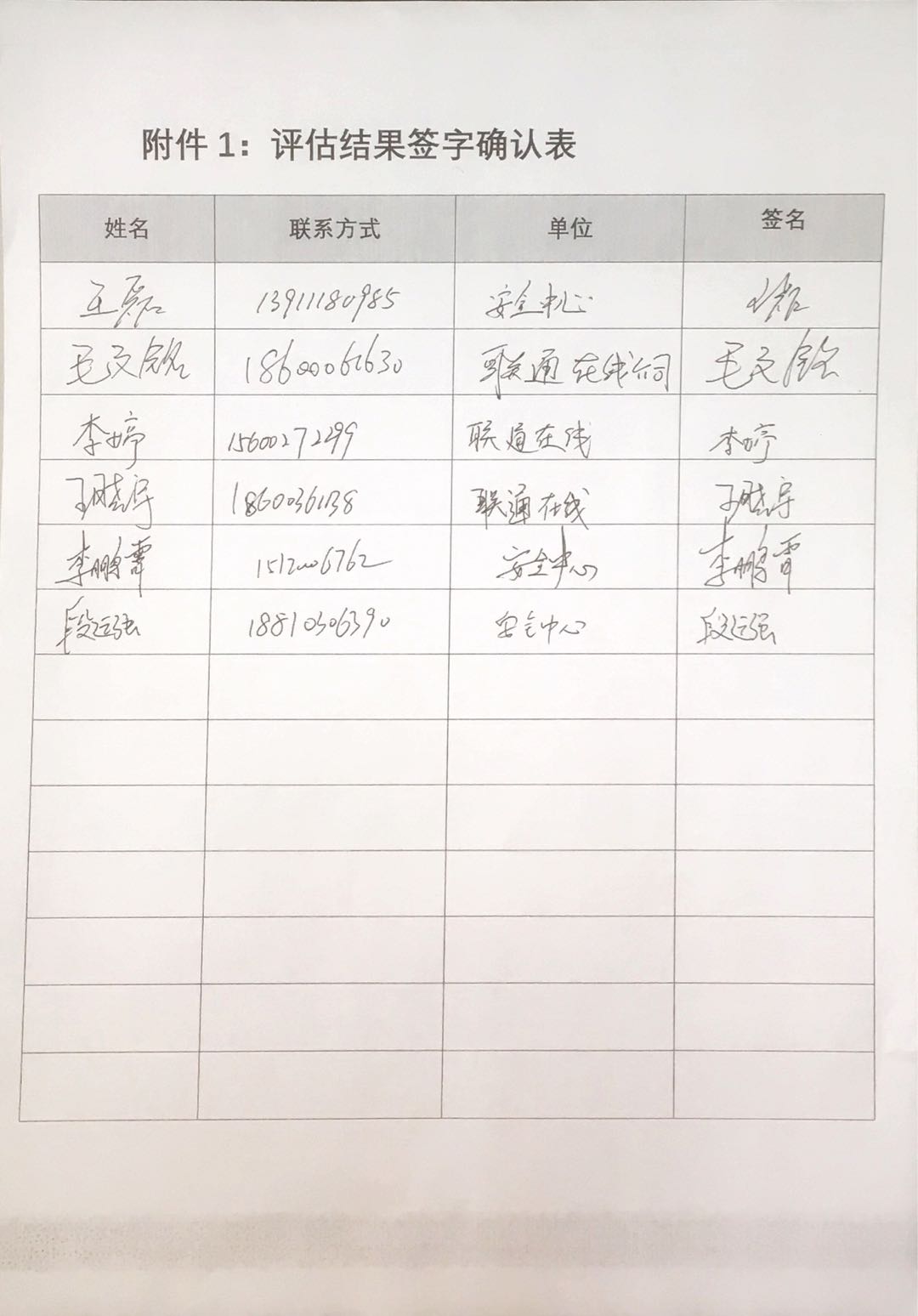
风险描述：联通家庭卫士•亲子守护业务不同手机号之间可以相互添加为守护号码，能够相互监看手机上网行为，与业务规则要求存在一定差别；同时，由于因涉及用户上网行为分析、上网管理、位置定位等用户个人隐私信息（用户为孩子家长），存在用户隐私信息泄露风险。

**整改建议：**进一步完善业务规则，明确家长手机号码、孩子手机号码之间守护关系，防止出现可相互守护监看手机上网行为情况发生；同时建议应明确该业务添加守护号码注册在同一用户身份证号下，以避免产生用户隐私信息泄露风险。

# 安全评估结论意见

联通家庭卫士•亲子守护业务涉及多个业务风险点，联通在线公司通过配套的安全管理措施，主要的风险点基本处于可管可控的水平，但仍存在部分风险点缺乏匹配的保障能力，部分保障能力措施呈现低水平状态，建议根据整改建议加强相关的安全保障能力建设。

# 附件一：评估结果签字确认表



# 

# 附件三：安全风险整改落实情况

**１.风险描述：**

**２.整改情况：**