备案号 XXXX—XXXX

四川省工程建设地方标准

P DBJ51/TXXX—XXXX

四川省数字家庭系统基础平台通用技术标准

Technical standard for digital home system basic platforms

in Sichuan Province

（征求意见稿）

XXXX-XX-XX发布 XXXX-XX-XX实施

四川省住房和城乡建设厅 发布

四川省工程建设地方标准

四川省数字家庭系统基础平台通用技术标准

Technical standard for digital home system basic platforms

in Sichuan Province

DBJ51/TXXX—XXXX

主 编 单 位： 四川通信科研规划设计有限责任公司

四川邮电职业技术学院

批准部门： 四川省住房和城乡建设厅

施 行 日 期 ： 2024年XX月XX日

XXX

2024-XX-XX 成 都

前 言

根据四川省住房和城乡建设厅《《关于下达2023年四川省工程建设地方标准制订计划（第二批）的通知》（川建标函〔2023〕4003 号）的要求，本标准由四川通信科研规划设计有限责任公司、四川邮电职业技术学院会同有关单位共同编制本标准。

编制组经广泛调查研究，认真总结实践经验，参考有关国内外标准，并在广泛征求意见基础上，编制本标准。

本标准共分为7章和1个附录，主要内容为：1 总则；2 术语和符号；3 基本规定；4 平台架构及功能；5 基础数据及要求；6 系统管理及运维；7 安全及保障；8 运行评价。

本标准由四川省住房和城乡建设厅负责管理，由四川通信科研规划设计有限责任公司负责具体技术内容的解释。执行过程中如有意见或建议，请反馈给四川通信科研规划设计有限责任公司（地址：中国（四川）自由贸易试验区成都高新区天韵路186号高新国际广场E座5、6楼，邮编：610041）。

主编单位： 四川通信科研规划设计有限责任公司、

四川邮电职业技术学院

参编单位： 中国电信股份有限公司四川分公司

四川省建设科技发展信息中心

四川省建筑设计研究院有限公司

中节能建设工程设计院有限公司

四川蜀天信息技术有限公司

中通服创立信息科技有限责任公司

成都同步新创科技股份有限公司

成都睿信天和科技有限公司

主要起草人：伍金明 尹久亮 黄春华 张 骥

张 华 胡 斌 黄志强 侯 通

才虹丽 覃仁超 杨 涛 周秀方

谭 东 何 杰 黄育成 王小彬

孟 胜 崔国龙 余思凡

主要审查人：

**目 次**

[1 总则 1](#_Toc14078)

[2 术语和符号 2](#_Toc17869)

[2.1 术 语 2](#_Toc753)

[2.2 符 号 3](#_Toc8833)

[3 基本规定 4](#_Toc17356)

[4 平台架构及功能 5](#_Toc4395)

[4.1 一般规定 5](#_Toc16829)

[4.2 平台架构 5](#_Toc8360)

[4.3 功能要求 8](#_Toc16879)

[4.4 硬件要求 8](#_Toc13366)

[5 基础数据及要求 10](#_Toc27257)

[5.1 一般规定 10](#_Toc12822)

[5.2 数据接口 11](#_Toc9982)

[5.3 数据互通 11](#_Toc1085)

[5.4 数据应用共享 12](#_Toc6925)

[6 系统管理及运维 14](#_Toc25507)

[6.1 一般规定 14](#_Toc22723)

[6.2 系统管理 14](#_Toc27373)

[6.3 系统运维 16](#_Toc1344)

[6.4 服务管理 18](#_Toc4998)

[7 安全及保障 19](#_Toc8676)

[7.1 一般规定 19](#_Toc6247)

[7.2 系统安全 19](#_Toc10365)

[7.3 网络安全 20](#_Toc21520)

[7.4 信息安全 20](#_Toc22978)

[7.5 数据安全 21](#_Toc7061)

[7.6 安全审计 22](#_Toc22742)

[7.7 安全运维 22](#_Toc26267)

[8 运行评价 24](#_Toc17314)

[附录A 数字家庭系统基础平台运行评价指标](#_Toc21693)[（参考性附录） 25](#_Toc14153)

[本标准用词说明 26](#_Toc25277)

[引用标准名录 27](#_Toc26891)

Contents

[1 General provisions 1](#_Toc18242)

[2 Terms and symbols 2](#_Toc3941)

[2.1 Terms 2](#_Toc24860)

[2.2 Symbols 3](#_Toc22722)

[3 Basic requirement 4](#_Toc10714)

[4 Platform architecture and functionality 5](#_Toc21285)

[4.1 General requirement 5](#_Toc29561)

[4.2 Platform architecture 5](#_Toc10256)

[4.3 Functional requirements 8](#_Toc19207)

[4.4 Hardware requirements 8](#_Toc23456)

[5 Basic data and requirements 10](#_Toc19016)

[5.1 General requirement 10](#_Toc13859)

[5.2 Data interface 11](#_Toc16267)

[5.3 Data exchange 11](#_Toc7962)

[5.4 Data application and sharing 12](#_Toc9485)

[6 System management and operations 14](#_Toc7556)

[6.1 General requirement 14](#_Toc27809)

[6.2 System management 14](#_Toc3952)

[6.3 System operation and maintenance 17](#_Toc2427)

[6.4 Service management 18](#_Toc31524)

[7 Safety and Security 19](#_Toc12609)

[7.1 General requirement 19](#_Toc11857)

[7.2 System safety 19](#_Toc22236)

[7.3 Network security 20](#_Toc17464)

[7.4 Information safety 21](#_Toc13471)

[7.5 Data security 21](#_Toc12714)

[7.6 Security audit 22](#_Toc10419)

[7.7 Safe operation and maintenance 23](#_Toc11846)

[8 8 Operational evaluation 24](#_Toc32245)

ppendix A Operational evaluation indicators for digital home system basic platform(Reference Appendix) [25](#_Toc19616)

[Explanation of wording in this code 26](#_Toc17459)

[List of quoted standards 27](#_Toc11951)

# 1 总则

**1.0.1** 为规范四川省数字家庭系统基础平台建设，满足用户对数字家庭智能业务的需求，制定本标准。

**1.0.2** 本标准适用于四川省数字家庭系统基础平台的设计、建设和运营。

**1.0.3** 基础平台应满足设备互联互通技术要求。

**1.0.4** 基础平台应满足数据开放共享技术要求。

**1.0.5** 基础平台应满足安全与隐私保护技术要求。

**1.0.6** 基础平台应同步规划、同步建设、同步使用网络安全技术。

**1.0.7** 基础平台的设计、建设和运营除应符合本标准的规定外，还应符合国家和行业现行有关标准的规定。

# 2 术语和符号

## **2.1 术 语**

**2.1.1** 数字家庭 digital home

数字家庭是以住宅为载体，利用物联网、云计算、大数据、移动通信、人工智能等新一代信息技术，实现系统平台、家居产品的互联互通，满足用户信息获取和使用的数字化家庭生活服务系统。

**2.1.2** 智慧社区 smart community

利用物联网、云计算、大数据、人工智能等新一代信息技术，融合社区场景下的人、事、地、物、情、组织等多维数据资源提供面向政府、物业、居民和社区企业的社区管理与服务类应用，提升社区管理与服务的科学化、智能化、精细化水平，实现共建、共治、共享的一种社区模式。，

**2.1.3** 数字家庭平台digital home platform

提供设备控制、数据交互、服务共享等功能，实现家居智能化，满足用户在线获取社会化服务、政务服务等需求的软件、硬件系统。

**2.1.4** 家庭网络 home network

将家庭套内音视频设备、家用电器、信息设备、水电气暖计量表、照明系统、安防报警求助系统等连接在一起组成的一种局域网络。

将家庭内音视频设备、家用电器、信息设备、水电气暖计量表、照明系统、安防报警求助系统等连接在一起组成的一种局域网络。

**2.1.5** 家庭网关 home gateway

对家庭网络内部所有网关的统称，提供协议转换、设备管理和网络管理等功能。

**2.1.6** 物联网网关 internet of things gateway

连接家庭子网和家庭主网的主要设备， 通过以太网接口与家庭网络连接， 通过有线及无线方式与控制器、 传感器等设备连接， 并对家庭子网内的设备及业务进行统一协调控制。

注：主要功能是接口及协议转换， 在某些应用场景下， 可嵌入在家庭网关里，实现两个设备的融合。

**2.1.7** 控制器 controller

能够接收控制指令，并对家庭内电气设备或家居设施做出相应的操作。

**2.1.8** 云服务器cloud server

部署在家庭网络之外的互联网上，对家庭网络网关、控制终端等设备及业务进行统一控制、管理、协调的服务器系统。

**2.1.9** 家庭主网 home primary network

支撑家庭视频监控、多媒体影音娱乐、IPTV等数据业务的网络。

**2.1.10** 家庭子网 home low-speed sub-network

支撑家庭传感类、监测类及控制类等物联网业务的网络。

## **2.2 符 号**

AI：人工智能(Artificial Intelligence)

API：应用程序编程接口(Application Programming Interface)

APP：应用程序（Application）

CPU：中央处理器(Central Processing Unit)

DDoS：分布式拒绝服务(Distributed Denial of Service)

ID：身份标识号(Identity Document)

Java：一种面向对象的编程语言

QoS：服务质量（Quality of Service)

TCP：传输控制协议（Transmission Control Protocol）

UDP：用户数据报协议（User Datagram Protocol）

WiFi： 一种无线局域网技术（Wireless Fidelity）

Web：全球[广域网](https://baike.baidu.com/item/%E5%B9%BF%E5%9F%9F%E7%BD%91/422004?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/web/_blank)(World Wide Web)

# 3 基本规定

**3.0.1** 数字家庭系统基础平台应包括平台架构与功能、基础数据及要求、系统管理与运维、安全及保障等内容。

**3.0.2** 基础平台采用云平台的建设模式，宜包括家庭云平台和运营云平台。

【条文说明】家庭平台中无第三方运营服务时，根据家庭需求由家庭自由选择，可参照本标准中的要求按需进行建设、配置及管理。

**3.0.3** 基础平台通过云服务器实现家庭网关、物联网关、控制器等设备及系统的联动。

**3.0.4** 基础平台应提供智能家居服务、线上社会化服务和线上政务服务。

**3.0.5** 家庭云平台应实现家庭内各种智能家居设备的连接、控制和管理，提供智能家居服务。

**3.0.6** 运营云平台应实现对多个家庭云平台统一管理，提供社会化服务和政务服务。

**3.0.7** 基础平台应考虑建设的可行性和数据的便利度，具有可操作性、开放性、通用化和综合化。

# 4 平台架构及功能

## **4.1 一般规定**

**4.1.1** 基础平台应基于大数据、AI、云、物联网等技术，面向居民提供多种服务。

**4.1.2** 基础平台应支持对业务的接入、汇聚和管理运营，通过业务门户将业务推送到家庭用户。

**4.1.3** 基础平台应支持各种信息数据的汇聚和整合，分类存储数据资源，具备数据挖掘、数据分析等功能。

**4.1.4** 基础平台应与相关城市、社区、物业及社会化专业服务平台对接。

【条文说明】加强与相关平台对接。推进数字家庭系统基础平台与新型智慧城市“一网通办”“一网统管”等政务服务系统、智慧社区信息系统、智慧物业管理以及社会化专业服务等平台的对接，开放信息接口，在遵循信息安全与隐私保护的前提下，推动信息资源共享，保障居民更加安全便利地获得政务、社会和产品智能化服务。

**4.1.5**基础平台应充分利用社区和城市公共基础数据，以及各类商业数据，为居民提供智慧物业、智慧社区和智慧政务等信息化服务。

**4.1.6** 基础平台应支持不同智能设备间按照预设规则或用户自定义规则进行系统联动，构建数字家庭智能产品生态系统。

**4.1.7** 基础平台应具备对IPv6的支持能力。

**4.1.8** 基础平台宜结合人工智能发展，开发数字家庭领域模型，提升人工智能在家庭场景中的自然理解和交互能力。

## **4.2 平台架构**

**4.2.1** 数字家庭系统基础平台由家庭云平台和运营云平台组成,平台框架示意见图4.2.1。

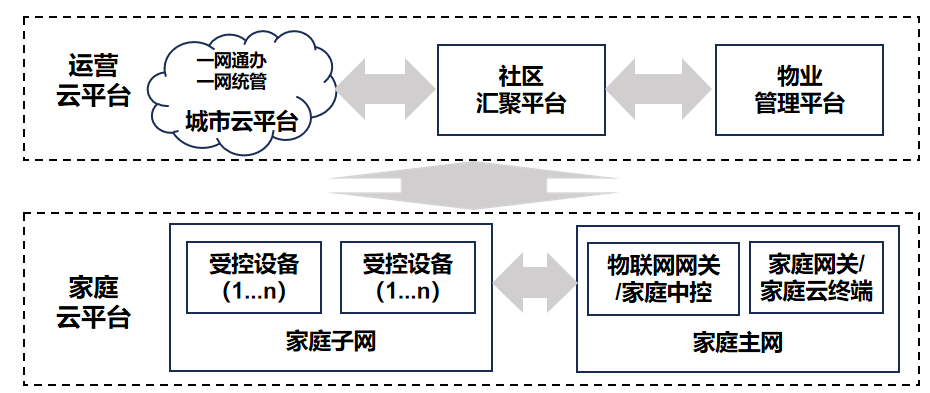


图4.2.1 数字家庭系统基础平台框架示意图

【条文说明】运营云平台可以通过授权，实现数字家庭的城市、社区和物业的服务，家庭云平台可以在对户内、户外（如手机、电脑等终端）实现对智能家居的控制管理服务，也可通过运营云平台实现。

**4.2.2** 家庭云平台应由家庭网关、１个或多个物联网网关、家庭中控(终端控制器)、云服务器等设备及系统，以及用于连接上述设备及系统的家庭网络构成。

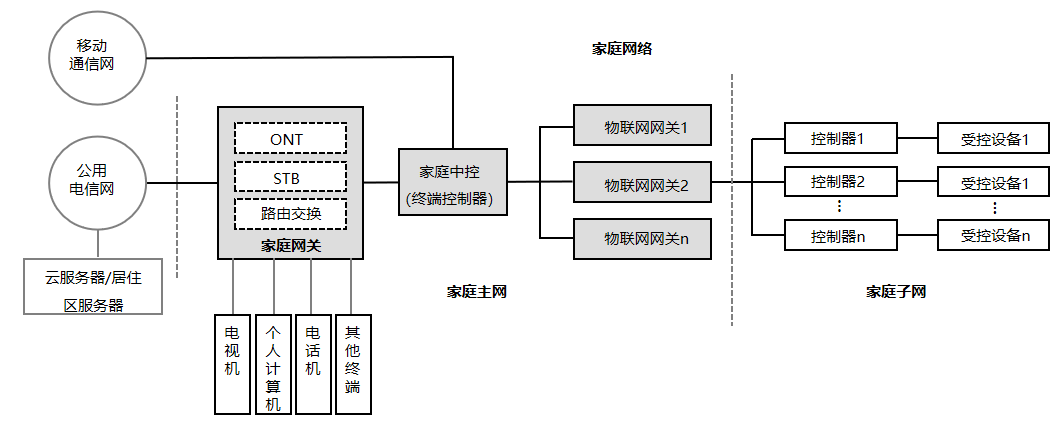
【条文说明】参考《建筑及居住区数字化技术应用家庭网络信息化平台》GB/T 38321，家庭云平台架构示意图见图4.2.2。数字家庭通过移动通信网络连接家庭中控实现远程控制。

图4.2.2 家庭云平台架构示意图

**4.2.3** 运营云平台架构组成宜满足以下要求：

1根据管理对象和服务范围以及层级不同，包括城市云平台（省、市、区县）、社区汇聚平台和物业管理平台；

【条文说明】为推动数字家庭的智慧应用发展及数字要素的流通，宜加快建设和应用省级、市级统一运营云平台。

2平台类型包括物联网类开放平台和应用类开放平台。

【条文说明】常见技术较成熟、运用较广泛的数字家庭类系统平台有以终端连接为主的物联网类开放平台和以视频服务为主的应用类开放平台。

**4.2.4** 基础平台的特性及主要要求如下表4.2.4：

表4.2.4 基础平台的特性及主要要求

|  |  |  |  |
| --- | --- | --- | --- |
| 特性 | 家庭云平台 | 运营云平台 | |
| 物业管理/社区/街道（镇乡）等平台 | 区县/地市/省平台 |
| 位置 | 居住区 | 物业/社区 | 城市 |
| 基础设施部署 | 家庭服务器/  家庭云 | 边缘数据中心/  社区云 | 云数据中心/  各级城市云平台 |
| 服务类型 | 智能家居服务 | 线上社会服务为主，部分政务服务 | 线上政务服务为主 |
| 关键技术 | 物联网、智能感知 | 云计算、安全、AI | 云计算、安全、AI |
| 平台功能 | 全屋智能家居控制 | 15分钟生活圈线上服务 | 对接智慧城市“一网通办”“一网统管” |
| 应用场景举例 | 居家养老、影音娱乐  节能等智能家居 | 智能安防、社区养老  线上社交等 | 公共健康、远程医疗  教育服务等 |
| 数据处理 | 数据采集、控制及反馈 | 权限内数据管理 | 数据交易、流通 |
| 数据 | 个人数据为主、公共数据 | 公共数据（区域受限） | 公共数据（城市授权流通） |

**4.2.5** 控制及数据流向应符合下列规定：

1家庭子网中的受控设备通过物联网网关与家庭主网进行数据交互；物联网网关负责将子网中的设备数据转换成主网可以处理的格式，发送到家庭主网；

2家庭中的数据通过家庭网关统一接入公用电信网络，也可经家庭云终端发送到家庭云平台进行处理和存储；

3家庭中的数据经过家庭云平台可发送到运营云平台；实现与城市云平台进行数据交互，并将数据汇聚到社区汇聚平台和物业管理平台，实现社区管理和物业管理的数字化；

4运营云平台可根据需要将数据发送回家庭云平台中的受控设备，实现远程控制和管理。

## **4.3 功能要求**

**4.3.1** 基础平台通过设备接口和服务应用接口，实现与数字家庭智能产品和服务应用进行连接、管理，并支持与外部平台对接。。

**4.3.2** 基础平台应具备互操作性，实现与不同厂商品牌应用系统兼容。

**4.3.3** 家庭云平台应实现住宅内智能终端互连互通与数据共享，家庭内部与外部进行信息交换。

**4.3.4** 家庭云平台应实现室内防盗、防劫、防火、防水浸、防燃气泄漏以及紧急救助等智能家居服务功能，实现相关数据的上传。

**4.3.5** 运营云平台应提供数字家庭运营业务管理、服务综合运营体系管理、数据资源配置、外部业务合作平台接入和数据支撑平台管理等功能。

**4.3.6** 运营云平台应实现对设备的数据采集、存储、交换、传输、管理、分析，并能对感知层设备进行控制，实现子系统的集成。

**4.3.7** 运营云平台应提供下列功能：

1提供安防、消防等管理功能；

2 对接物业服务、社区养老、家政服务、旅游服务、家庭教育、社区电商等社会专业化服务平台为家庭提供相关服务功能；

3对接政务云实现“一网通办”等政务服务功能。

**4.3.8** 家庭云平台应符合现行国家标准《智能家居自动控制设备通用技术要求》GB/T 35136 和[《物联网智能家居 数据和设备编码](https://www.biaozhun.org/guojia/36628.html" \o "" \t "_blank)》GB/T 35143中的有关规定。

## **4.4 硬件要求**

**4.4.1** 基础平台采用分布式部署，硬件设施根据需求在以下不同位置部署：

1 家庭云平台可部署在家庭室内或互联网数据中心；

2 物业、社区、街道（镇乡）平台可部署在边缘数据中心（物业机房、社区机房、街道和镇乡机房））或互联网数据中心；

3 区县、市、省级宜部署在互联网数据中心。

**4.4.2** 基础平台所部署物理环境应确保安全可靠。

**4.4.3**基础平台性能应符合以下规定：

1 应满足多种设备的兼容接入；

2 应满足大规模设备的同时接入；

3 应满足大量并发访问性能要求。

**4.4.4** 基础平台宜根据数字家庭服务需要在边缘数据中心、互联网数据中心部署通用算力和智能算力。

【条文说明】平台宜根据数字家庭服务需要在边缘数据中心、互联网数据中心部署通用算力和智能算力，其中基础通用算力主要基于 CPU 芯片的服务器所提供的计算能力，智能算力主要是基于 GPU、FPGA、ASIC 等芯片的加速计算平台提供人工智能训练和推理的计算能力。

**4.4.5** 基础平台应在可信环境中运行，保障数据安全、执行流程可靠。

**4.4.6** 基础平台应建立网络及信息安全的硬件防范措施，防止非法访问，确保数据安全。

# 5 基础数据及要求

## **5.1 一般规定**

**5.1.1** 数字家庭的基础数据分为个人信息、组织数据和公共数据。

【条文说明】根据国家现行标准《数据安全技术 数据分类分级的规则》GB/T 43697中附录A的规定，从数据主体角度，可将数据分为公共数据、组织数据、个人信息三个类别，数据分类参考示例如下表5.1.1：

表 5.1.1 基于数据主体的数据分类参考示例

|  |  |  |
| --- | --- | --- |
| 数据分类 | 类别定义 | 示例 |
| 公共数据 | 各级政务部门、具有公共管理和服务职能的组织及其技术支撑单位，在依法履行公共事务管理职责或提供公共服务过程中收集、产生的数据 | 如政务数据，在供水、供电、供气等公共服务运营过程中收集和产生的数据等 |
| 组织数据 | 组织在自身生产经营活动中收集、产生的不涉及个人信息和公共利益的数据 | 如不涉及个人信息和公共利益的业务数据、经营管理数据、系统运维数据等 |
| 个人信息 | 以电子或者其他方式记录的与己识别或者可识别的自然人有关的各种信息 | 如个人身份信息、个人生物识别信息、个人财产信息、个人通信信息、个人位置信息、个人健康生理信息等 |

**5.1.2** 数字家庭中数据主要包括个人基础数据、家庭基础数据、家庭设备数据、用户行为数据、环境数据、场景数据、家庭成员社交数据等。

**5.1.3** 数字家庭智能家居设备需要支持统一或兼容的通信协议，确保不同品牌和类型的设备之间可以互相识别并进行数据交互。

**5.1.4** 接口与数据格式标准化，设备应遵循统一的数据模型和API接口标准，以便不同厂商的智能产品可以共享控制指令、状态信息和其他数据，从而无缝集成到数字家庭的控制系统中。

**5.1.5** 数字家庭智能家居设备终端可连接到云端，通过互联网和云端服务器，实现远程数据获取和传输。

**5.1.6** 数字家庭服务通过建立家庭网关与服务平台连接，实现家庭设备和人之间的沟通与联系。

**5.1.7** 数字家庭基础数据的应用应符合现行国家标准《数字家庭服务资源分类与代码》GB/T 36528的有关规定。

## **5.2 数据接口**

**5.2.1** 数字家庭各个控制系统之间的接口以及采用的协议，应符合现行国家标准《建筑及居住区数字化技术应用家庭网络信息化平台》GB/T 38321的有关规定。

**5.2.2** 接口采用云数据中心接口和家庭数据采集传输接口，分为用户接口、设备接口、产品测试接口、第三方服务接口四大类。

**5.2.3** 基础平台接口应符合下列规定：

1提供服务详单接口和采集接口；

2提供服务应用接口；

3提供用户数据接口。

**5.2.4** 数字家庭智能家居设备终端接口可分为移动智能终端、智能控制屏、智能机顶盒和宽带光纤等网络接口。

**5.2.5** 接口可采用设备直连模式、平台互联模式，宜使用TCP/IP方式。

**5.2.6** 基础平台和家庭网关接口设置设备ID应具有唯一性，用于区分不同设备，并应符合下列规定：

1全屋智能设备应使用唯一的设备ID进行标识与解析认证。

2在特定场景，如需对设备进行标识保护（标识匿名化），可采用分布式数字身份技术设置设备ID。

## **5.3 数据互通**

**5.3.1** 基础平台应与政务、社区、物业、社会化专业服务平台进行系统连接和数据交换，实现数据互联互通。

【条文说明】建设开放的数字家庭基础平台，推进与新型智慧城市“一网通办”“一网统管”、智慧物业管理、智慧社区信息系统及社会化专业服务平台的对接，实现数据的互联互通，提升便民性，扩大服务范围，结合数字家庭推动国家“数据要素x”行动。

**5.3.2** 基础平台数据的互联互通应坚持公平公正原则，确保各方的平等义务和权利。

**5.3.3** 基础平台应支持使用运营商手机号作为互联互通体系的统一账号，实现多平台多服务的相互认证。

【条文说明】运营商手机号作为互联互通体系的统一账号，为同一账号下的各生态的智能家居设备的互联互通提供基础条件。且运营商手机账号具有通用、安全、高效、便于统一管理的优点。

**5.3.4** 基础平台应支持智能家居控制终端和智能家居设备终端直接或间接连接到云平台，通过云平台完成设备间的交互。

**5.3.5** 基础平台应支持与不同厂商云平台之间进行互联，以便分别连接到不同云平台的家庭设备实现互联互通。

## **5.4 数据应用共享**

**5.4.1** 基础平台应通过对家庭内数据的采集、控制和反馈实现居家养老、影音娱乐和节能等智能家居应用服务。

**5.4.2** 基础平台应通过对区域公共数据的授权管理应用，实现社区养老、家政服务和社区电商等社区应用服务。

**5.4.3** 基础平台应通过对授权的公共数据交易、流通，实现就业、社保、健康、卫生、医疗、救助、养老、助残和托育等政务应用服务。

【条文说明】通过对公共数据的授权共享与流通，推动公共服务普惠化，实现政务服务“指尖办”“网上办”“就近办”。

**5.4.4** 基础平台应设定严格的数据共享、审核与鉴权机制，确保数据共享的安全性，并符合下列规定：

1宜采用分级共享机制，数据的共享依据分级实行授权访问，各分级具备各自独立的访问接口；

2支持对数据共享交换API接口的异常状态进行监测；

3提供对外共享交换的数据目录管理功能。

**5.4.5** 数据共享流通应符合主管部门的数据开放目录，应当遵循依法、规范、公平、优质、便民的原则。

**5.4.6** 公共数据按照共享属性分为无条件共享、受限共享和不共享数据。

**5.4.7** 数字家庭的不同数据共享流通应符合下列规定：

1在依法安全合规前提下，进行金融信用数据和公共信用数据、商业信用数据共享共用和高效流通；

2涉及公共卫生、交通管理、公共安全、生态环境、基层治理等公共数据按政府要求依法共享，实现态势实时感知、风险智能研判及时协同处置；

3社区、家庭的智慧医疗、智能健康管理等数据，可经个人允许后，依法依规与医疗机构进行数据共享和流通；

4个人信息需在保护个人隐私前提下合理利用。

【条文说明】为提升数字家庭服务的质量和便利性，在遵循相关法律法规，确保数据的安全、合法使用和有效保护个人隐私的前提下，推进公共数据开放与共享。

# 6 系统管理及运维

## **6.1 一般规定**

**6.1.1** 基础平台系统管理可由以下方式实现：

1运行在家庭内计算机终端上独立的网络管理系统软件实现；

2嵌入到家庭网关终端里的功能模块实现；

3云服务器上的管理系统联动家庭网关终端功能模块实现。

**6.1.2** 基础平台应具备系统管理、系统运维和服务管理等功能。

**6.1.3** 基础平台应提供后台管理系统，具备账户管理、设备管理、状态管理、消息发送、数据同步、日志管理、升级维护及其他等后台管理能力。

**6.1.4** 基础平台应提供统一的管控界面，包括自助服务/运营/运维服务等模块。

**6.1.5** 基础平台应实现设备和服务资源的有效管理。

**6.1.6** 家庭云平台实现对家庭网关、物联网网关、终端控制器等设备及系统的统一协调管理，并按需将其连接到运营云平台。

**6.1.7** 运营云平台应能对多个家庭云平台设备进行管理，并对连接到运营云平台的家庭智能终端设备实现自动发现、注册、配置及管理等控制。

**6.1.8** 基础平台应加强数据加密、身份验证、访问控制等安全管理，在满足互联互通的同时，保障用户信息安全及隐私不被侵犯。

**6.1.9** 基础平台应建立统一的认证体系，确保符合标准的设备能够通过认证。

## **6.2 系统管理**

**6.2.1** 基础平台系统管理应包括系统功能配置、权限管理、资源管理、数据管理。

**6.2.2** 系统配置功能应符合下列规定：

1支持系统图形化和分类、分角色等多方式配置项管理；

2支持配置项的批量修改、保存、导入、导出以及配置文件上传、下载、恢复、更新；

3云服务器支持采用滚动重启方式生效不中断业务，并能手动或自动推送配置更新至相关节点；

4支持通用型和个性化的参数配置，并能进行历史版本管理和过期管理，更新后与管理终端和管理系统同步。

**6.2.3** 系统应根据角色管理实现角色定义和权限控制, 确保不同角色的用户只能访问其授权范围内的信息和功能。

**6.2.4** 系统的权限管理应符合下列规定：

1系统对用户的管理至少支持普通用户和管理员用户的两级权限管理；

2 平台应对所接入的终端设备和用户身份建立认证机制，以验证合法接入和使用权限，用户提供合法的账号和密码才可以使用该业务；

3设备的认证信息应包括设备认证密钥、设备认证证书、设备唯一标识符；

4具备账号、密码的安全策略，如定期更换、复杂度要求等，应保证用户账号唯一性；

【条文说明】密码安全策略中要加强密码的复杂性，复杂口令设置应包括强制密码长度、必需包含大小写字母的复杂度设定,有效降低用户账号应对端口扫描、密码暴力破解、DDoS 攻击能力被破解的风险。

5家庭云平台的每个账户只能管理自己家庭的家庭网关、受控终端、终端控制器等设备。

**6.2.5** 设备设施管理方面，平台运营者应对服务器、网络设备、存储设备等基础设施进行有效管理，包括采购、配置、维护和报废等全生命周期管理。

**6.2.6** 软件资产管理方面，应对平台上的应用程序、中间件、数据库等软件资源进行管理，跟踪版本变更、许可证合规性等。

**6.2.7** 家庭网络管理应符合下列规定：

1 应支持对家庭网关进行远程管理，包括以下管理功能：

1) 对数据、语音、QoS 等功能进行部署、管理和控制；

2) 进行远程状态查询、故障管理、设备配置和软件升级；

3) 对智能应用进行加载、配置及生命周期管理。

2宜支持家庭网关软件和网关插件管理，包括远程安装、升级和卸载；

3宜支持软探针功能,并对家庭网络质量进行采集、存储、评估和调整优化的能力；

4 应能提供报表分析和管理能力,包括:家庭网关报表、WiFi性能报表和 WiFi覆盖报表；

5应提供对单个家庭的一键检测功能,并且能够诊断常见的家庭网络故障。

**6.2.8** 物联网网关、终端控制器的相关功能及管理维护应符合现行国家标准《建筑及居住区数字化技术应用 家庭网络信息化平台》GB/T 38321的有关规定。

**6.2.9** 基础平台应对存储的数据进行管理，数据的使用与安全总体上应符合现行国家标准《信息安全技术大数据安全管理指南》GB/T 37973的有关规定。

【条文说明】家庭内的个人信息宜以个人管理和对外授权管理为主，运营云平台的数据的管理，应根据授权情况分类管理，并符合相关数据法律法规和国家现行相关标准要求。

**6.2.10** 数据管理应确保用户数据、用户信息等存储于中国境内，具备数据备份、数据恢复机制。

**6.2.11** 数据管理应符合下列规定

1应确保只有在用户授权下，平台运营者或第三方才具有云服务用户数据的管理权限；

2 应采用校验技术或密码技术保证通信和存储过程中的数据完整性、保密性和可用性；

3用户转移和删除业务应用数据时，平台运营者应将对应的应用数据完全删除；

4数据的备份、存储及信息共享应符合国家相关法律法规以及国家现行标准[《信息技术 云数据存储和管理 第1部分：总则](https://www.biaozhun.org/guojia/12400.html" \o "" \t "_blank)》GB/T 31916.1、[《信息技术 备份存储 备份技术应用要求》](https://www.biaozhun.org/guojia/39867.html" \o "" \t "_blank)GB/T 36092、[《信息安全技术 云存储系统安全技术要求》](https://www.biaozhun.org/hangye/82829.html" \o "" \t "_blank)GA/T 1347的有关规定；

5平台具备系统安全防护，防止数据损失、篡改和泄露；

6应对敏感信息进行加密处理，具备隐私申明，个人信息保护应符合国家相关法律法规和现行国家标准《信息安全技术公共及商用服务信息系统个人信息保护指南》GB/Z 28828、[《信息安全技术 个人信息安全规范》](https://www.biaozhun.org/guojia/59173.html" \o "" \t "_blank)GB/T 35273的有关规定。

## **6.3 系统运维**

**6.3.1** 基础平台系统运维一般包括日常运维和应急管理，其中日常运维应包括日志管理、性能监测和故障管理。

**6.3.2** 日志管理应符合下列规定：

1应具有日志记录、查询、过滤设置、导出等功能，记录信息包括但不限于登录、退出、注册、注销、操作、更改、创建删除等；

2 日志应能呈现查询报表，宜提供图形化页面检索运行日志；

3 应提供日志目录的管理功能,如更改日志存储空间、更改日志存储目录等，支持日志级别的设置；

4 应支持按照关键字段检索,如指定关键字、日志级别、服务、主机等；

5应设置操作日志存储机制，如至少保存6个月以上，并采取技术手段进行保护；

6实施日志审计，应对审计进程进行保护，防止未授权的中断；

7 应提供安全管理中心功能，对异常登录、日志篡改等事件进行预警。

**6.3.3** 性能监测应保障基础平台的稳定性和健康检查。

**6.3.4** 稳定性应符合下列规定：

1平台运营者应维护系统正常运行，通过监控系统性能、资源使用情况，及时发现并解决潜在故障，确保服务连续性；

2平台应提供7x24小时服务；

3平台服务可用性不低于99.99%。

**6.3.5** 健康检查应符合下列规定：

1 应定期进行自动检查和手工检查，能够输出检查报告；

2 平台宜提供界面化的系统运行环境自动检查服务，支持按照场景进行检查,如升级前检查；

3 执行定期的系统巡检、更新升级、补丁管理和硬件设施的维护保养工作。

**6.3.6** 基础平台运营者应建立故障处理流程和应急预案，确保在系统出现问题时能迅速恢复正常。

**6.3.7** 障管理应符合下列规定：

1平台应支持网元管理，包括故障诊断、网络应用服务、设备认证、状态监视、参数配置、软件升级、告警、设备信息、版本/配置文件信息、业务代码的管理,设备分组管理等功能；

2设备信息包括设备类型、设备业务能力等通用信息，以及设备 MAC 地址、IP 地址、最近连接信息等个性化信息；

3故障管理应能通过管理平台对家庭网关、下挂设备进行故障定位；

4平台应提供友好的故障诊断人机交互界面；

5若出现故障能及时告警，告警信息在日志中均能被记录。

**6.3.8** 应急预案应包括综合应急预案、专项应急预案和现场应急处置方案，并定期评估和更新预案，演练频次应符合下列规定：

1 综合应急预案，至少每年进行一次演练；

2 专项应急预案，每半年进行一次演练；

3 现场应急处置方案，每半年进行一次演练；

4 根据平台安全等级和所面临的风险程度，尤其遇重大变更或发生重大事件后，应及时补充应急预案，增加演练频次。

## **6.4 服务管理**

**6.4.1** 基础平台服务管理应支持智能家居服务、线上社会化服务和政务服务的管理。

**6.4.2** 基础平台应提供用户注册登录、设备管理、历史信息管理等功能界面。

**6.4.3** 基础平台应提供家居安全防范、家用电器控制、环境监测、家庭娱乐等智能家居应用服务人机交互操作界面。

**6.4.4** 基础平台应可对设备的状态进行直观显示，当设备状态发生改变时，应可实时更新。

**6.4.5** 系统界面应对用户的操作提供清晰明确的信息反馈。

# 7 安全及保障

## **7.1 一般规定**

**7.1.1** 基础平台安全应包括系统安全、网络安全、信息安全和数据安全等。

**7.1.2** 基础平台应进行安全审计和安全运维。

**7.1.3** 系统安全应进行系统接入身份鉴别、权限识别控制，保障系统物理环境安全和平台可靠，并具备容灾备份和容错升级机制。

**7.1.4** 网络安全应进行多层防御、白名单访问控制和定期安全扫描。

**7.1.5** 信息安全应保障信息的真实性、完整性、保密性、可用性、可控制性和可审查性，并具备平台自主可控。

**7.1.6** 数据安全应保障数据的访问控制、传输、存储和使用安全，并加强隐私及个人信息保护。

## **7.2 系统安全**

**7.2.1**系统安全应满足现行国家标准《信息安全技术网络安全等级保护基本要求》GB/T 22239、《信息技术安全技术信息安全管理体系审核指南》GB/T 28450等相关规定。

**7.2.2** 应有效管理系统的物理环境安全、通信与运营、访问控制、系统开发与维护、业务连续性等。

**7.2.3** 基础平台的云平台环境安全应符合现行国家标准《[信息安全技术 云计算服务安全能力要求](https://www.biaozhun.org/guojia/277706.html)》GB/T 31168的有关规定。

**7.2.4**设备物理安全应符合下列规定：

1 应保证运营云平台的基础设施和数据中心位于中国境内；

2 系统设备具备相应的静电放电、电磁辐射、电快速瞬变脉冲抗扰度和抗电强度；

3系统设备所处的环境和场地应具备防火、防潮、防雷电等相关能力；

4系统设备所在的环境和场地应具备人员和物品进出的管控能力，确保安全性和可控性。

**7.2.5**系统平台应进行身份鉴别和权限识别，确保权责一致性，并应符合下列规定：

1应提供对用户系统和服务账号进行统一认证、集中授权和综合审计管理；

2支持用户对智能模块所使用的各项资源访问权限进行管理；

3支持对用户的操作活动、系统运行情况等安全日志管理和审计管理。

**7.2.6**平台应提供开放的数据接入接口，对不同应用类型数据接口进行认证、监测及安全管理，对接口的调用应经过鉴权。

**7.2.7**系统应保障可靠性，提供容灾备份和系统恢复的能力，以应对意外事件和系统故障。

**7.2.8**平台应支持在不中断服务的情况下容错升级中央处理器（CPU）、内存和磁盘硬件性能功能。

## **7.3 网络安全**

**7.3.1**基础平台应采用多重防御，通过防火墙等安全措施对集群内流量进行严格管控，保护平台主机免受来自内（外）部的网络攻击。

**7.3.2**基础平台应采用白名单形式设置访问控制列表，可信主机才可访问集群内主机。

**7.3.3** 基础平台支持在云虚拟层面针对特定IP端口进行访问控制。

**7.3.4** 基础平台应定期进行安全扫描，及时发现安全漏洞，快速对漏洞进行修补或者防护。

【条文说明】基础平台支持对各种网络主机、操作系统、网络设备、常用软件以及应用系统的识别和漏洞扫描，支持Web动态安全漏洞检测，特别针对基于Java语言构建的Web漏洞检测，支持对网页Java类别进行恶意代码检测。

**7.3.5** 基础平台应提供云边界、虚拟化及主机安全防护措施，实现恶意程序检测、威胁攻击、病毒检测、主机入侵检测和漏洞扫描等。

**7.3.6** 基础平台应具备抵抗大容量DDoS攻击的能力，支持实时检测、实时告警、自动清洗的能力。

## **7.4 信息安全**

**7.4.1**基础平台的信息安全应符合现行国家标准《信息安全技术公共及商用服务信息系统个人信息保护指南》GB/Z 28828和《信息安全技术个人信息安全规范》GB/T 35273的有关规定。

**7.4.2**基础平台应保障信息的真实性，对信息的来源进行判断和鉴别，对不明来源的请求予以终止。

**7.4.3**基础平台应保障信息的完整性，支持对用户信息的数据类型进行自动校验和认证，确保信息数据的准确一致。

**7.4.4** 基础平台应保障信息的保密性，对用户登录账号和密码等个人信息应进行加密传输。

**7.4.5**基础平台应保障信息的可用性。保证合法用户对信息的使用不会被不正当拒绝；对允许用户设置的信息应具备容错性，确保各智能模块的应用与服务不会因用户的错误操作而中断。

**7.4.6**基础平台应保障信息可控制性，支持对用户相关信息数据的实时传播、信息内容的及时发布等具有适度控制能力。

**7.4.7**基础平台应保障信息的可审查性，持对云平台上的操作提供或保留事后审查的依据和手段。

**7.4.8**基础平台的云平台应自主可控。

**7.4.9**基础平台的城市云平台宜使用“国资云”及国产化设备。

【条文说明】云平台宜使用国产化设备，考虑到运营云平台提供服务的居民范围和数据量，为保障数据完全，在城市云平台（省、市、区、县）宜使用“国资云”。

## **7.5 数据安全**

**7.5.1** 基础平台在数据访问控制方面应具备权限控制功能。对数据库设置不同访问策略，对关键安全信息文件、数据的上传下载操作等进行权限控制。

**7.5.2**基础平台在数据传输安全方面应具备数据传输机密性和数据完整性保护机制，防止未授权的第三方对数据进行修改、破坏和消息重放等。

**7.5.3**基础平台在数据存储安全方面应符合下列规定：

1 应具备密钥安全存储功能，保证密钥不被泄露；

2 应具备数据完整性保护功能,确保关键安全信息在损坏和丢失时能够及时发现；

3 应具备完备的数据备份和恢复功能；

4 应具备对各类数据和文件进行归档和对临时数据及文件进行定期自动清理的功能；

5 当数据删除后系统内的文件、目录和数据库等资源所在存储空间被释放或重新分配时,应具备数据的完全清除和不可恢复的功能。

**7.5.4**基础平台应支持对数据进行权限分级使用、加密保护和隔离。

**7.5.5** 基础平台应建立隐私和个人信息保护机制。

**7.5.6** 隐私和个人信息应依法合规收集，在得到个人授权后存储和使用，不得越权、越级、变向使用。

**7.5.7**隐私数据需脱敏处理，按国标安全加密存储和传输。

## **7.6 安全审计**

**7.6.1**基础平台的物理机应全部启用安全相关的日志记录功能，日志重定向到独立的服务器。

**7.6.2**基础平台应对整个安全基础设施包括虚拟环境提供统一的日志安全审计系统。

**7.6.3**基础平台应针对账户管理、登录事件、系统事件、策略更改，账户登录事件的成功/失败开启审计。

**7.6.4**基础平台应对家庭内各智能模块设备的操作配备安全审计日志，并及时保护，杜绝信息记录丢失或数据篡改情况发生。

**7.6.5** 基础平台应提供云上数据库访问行为、数据流向等安全审计。

**7.6.6** 基础平台提供的服务应用上线前应做代码审计，防止带病入云。

**7.6.7** 基础平台应具备数据库审计能力，并符合下列规定：

1支持主流数据库、非关系型数据库、主流业务协议的审计能力；

2支持通过部署代理实现web环境准确关联；

3支持审计记录中敏感数据的模糊化处理。

## **7.7 安全运维**

**7.7.1**基础平台的角色管理系统实现定义和权限，运维工程师应具有唯一身份。

**7.7.2** 通过加密信道进行管理，具备身份鉴别和认证。

**7.7.3** 登录、操作过程均被实时审计。

**7.7.4** 应建立内部流量汇聚点，监控网络动态和流量。

**7.7.5** 对物理机主机进行实时的中央处理器（CPU）、带宽、磁盘监控，发现异常情况应立即通过短信、邮件告警。

**7.7.6** 应对数据开展分类分级保护。

**7.7.7**用户独立管理家庭云平台，非授权用户不能访问。

**7.7.8** 家庭云平台的各用户彼此独立，应隔离防护和限制彼此访问。

**7.7.9** 运营云平台能够动态实时监测平台安全运营态势。

**7.7.10** 运营云平台应具备独立云安全管理平台，并符合下列规定：

1支持使用云平台提供的虚拟化资源部署云安全能力，并以组件形式支持多租户共享架构；

2云安全管理平台支持以授权许可的方式激活虚拟安全组件。

# 8 运行评价

**8.0.1**基础平台的运行评价指标分为二级，包括6个一级指标、20个二级指标。详见附录A《数字家庭系统基础平台运行评价指标》。

**8.0.2** 每个一级指标下设多个二级指标，基本内容对二级指标进行进一步展开，对其应具备的功能或要求进行描述。

**8.0.3** 一级指标包括平台基本功能、平台互联互通、数据应用共享、平台安全、服务内容和服务质量。

**8.0.4** 基础平台基本功能下的二级指标包括硬件设施、数据接口、系统管理、系统运维。

**8.0.5** 基础平台互联互通下的二级指标包括系统平台对接、手机号统一账号、多种终端连接交互。

**8.0.6** 数据应用共享下的二级指标包括数据分级共享、数据审核与鉴权。

**8.0.7** 基础平台安全下的二级指标包括系统安全、网络安全、信息安全、数据安全。

**8.0.8** 服务内容下的二级指标包括智能家居服务、线上社会服务、线上政务服务。

**8.0.9** 服务质量下的二级指标包括服务管理、服务响应、服务效率、服务便捷。

**8.9.10** 平台运行服务质量应符合下列规定：

1 服务应有人员保障。平台运行应具备专业化运维服务力量，保障业务服务人员稳定性，服务工作规范性，有良好的服务支持配合度；

2 服务应响应及时。保障平台维护作业、各类资源故障申告、重要安全事件的通告及时准确，并保障故障响应与解决的时效性；

3 服务应确保效率。及时响应平台资源及服务的相关问题，并快速配合解决；

4 服务应保证便捷。提供平台资源运行优化和动态调整建议，提供便利的新建业务、现有业务迁移平台的服务对接。

# 附录A 数字家庭系统基础平台运行评价指标

# （参考性附录）

A.0.1数字家庭系统基础平台运行评价应符合表A的规定。

表A数字家庭系统基础平台运行评价指标表

|  |  |  |
| --- | --- | --- |
| 一级指标 | 二级指标 | 基本内容 |
| 平台基本功能 | 硬件设施 | 物理环境应确保安全可靠，平台硬件性能满足多种设备的兼容接入、大规模设备的同时接入、大量并发访问性能要求 |
| 数据接口 | 支持统一或兼容的通信协议，遵循统一的数据模型和API接口标准，以便不同厂商的智能产品可以共享控制指令 |
| 系统管理 | 包括系统功能配置、权限管理、资源管理、数据管理。 |
| 系统运维 | 包括日常运维和应急管理，其中日常运维应包括日志管理、性能监测和故障管理。 |
| 平台互联互通 | 系统平台对接 | 支持与新型智慧城市政务云“一网通办”“一网统管”对接，支持与智慧物业管理平台、智慧社区信息系统、社会化专业服务平台进行对接 |
| 手机号统一账号 | 支持使用运营商手机号作为互联互通体系的统一账号，实现多平台多服务的相互认证 |
| 多种终端连接交互 | 支持智能家居控制终端和设备终端直接或间接连接到云平台，通过云平台完成设备间的交互 |
| 数据应用共享 | 数据分级共享 | 采用分级共享机制，数据的共享依据分级实行授权访问 |
| 数据审核与鉴权 | 数据按共享属性分为无条件共享、受限共享和不共享数据，应进行相应的审核与鉴权 |
| 平台安全 | 系统安全 | 进行系统接入身份鉴别、权限识别控制，保障系统物理环境安全和平台可靠，并具备容灾备份和容错升级机制 |
| 网络安全 | 进行多层防御、白名单访问控制和定期安全扫描 |
| 信息安全 | 应保障信息的真实性、完整性、保密性、可用性、可控制性和可审查性，并具备平台自主可控 |
| 数据安全 | 应保障数据的访问控制、传输、存储和使用安全，并加强隐私及个人信息保护 |
| 服务内容 | 智能家居服务 | 支持室内防盗、防火、防燃气泄漏、紧急救助、居家养老、影音娱乐、节能等应用 |
| 线上社会服务 | 支持线上获得物业服务、社区养老、家政服务、旅游服务、家庭教育、社区电商等社会专业化服务 |
| 线上政务服务 | 支持政务服务“指尖办”“网上办”“就近办” |
| 服务质量 | 服务人员 | 具备专业化运维服务力量，保障业务服务人员稳定性，服务工作规范性，有良好的服务支持配合度 |
| 服务响应 | 保障平台维护作业、各类资源故障申告、重要安全事件的通告及时准确，并保障故障响应与解决的时效性 |
| 服务效率 | 及时响应平台资源及服务的相关问题，并快速配合解决 |
| 服务便捷 | 提供平台资源运行优化和动态调整建议，提供便利的新建业务、现有业务迁移平台的服务对接 |

# 本标准用词说明

1 为便于在执行本标准条文时区别对待，对要求严格程度不同的用词说明如下：

1）表示很严格，非这样做不可的：

正面词采用“必须”，反面词采用“严禁”；

2）表示严格，在正常情况下均应这样做的：

正面词采用“应”，反面词采用“不应”或“不得”；

3）表示允许稍有选择，在条件许可时首先应这样做的：

正面词采用“宜”，反面词采用“不宜”；

4）表示有选择，在一定条件下可以这样做的，采用“可”。

2 条文中指明应按其他有关标准执行的写法为：“应符合……的规定”或“应按……执行”。

# 引用标准名录

1 《信息安全技术 云存储系统安全技术要求》GA/T 1347

2 《信息安全技术网络安全等级保护基本要求》GB/T 22239

3 《信息技术安全技术信息安全管理体系审核指南》GB/T 28450

4 《信息技术 云数据存储和管理 第1部分：总则》GB/T 31916.1

5 《信息安全技术 云计算服务安全能力要求》GB/T 31168

6 《智能家居自动控制设备通用技术要求》GB/T 35136

7 《物联网智能家居 数据和设备编码》 GB/T 35143

8 《信息安全技术 个人信息安全规范》GB/T 35273

9 《信息技术 备份存储 备份技术应用要求》GB/T 36092

10 《数字家庭服务资源分类与代码》GB/T 36528

11 《信息安全技术 Web应用安全检测系统安全技术要求和测试评价方法》GB/T 37931

12 《信息安全技术大数据安全管理指南》GB/T 37973

13 《智慧城市 建筑及居住区综合服务平台通用技术要求》GB/T 38237-2019

14 《建筑及居住区数字化技术应用 家庭网络信息化平台》GB/T 38321

15 《信息技术 大数据 系统运维和管理功能要求》GB/T 38633

16 《公众电信网 智能家居应用技术要求》GB/T 39579

17 《信息安全技术 智能家居通用安全规范》GB/T 41387

18 《数据安全技术 数据分类分级的规则》GB/T 43697

19 《信息安全技术公共及商用服务信息系统个人信息保护指南》GB/Z 28828