

北京电信技术发展产业协会团体标准

T/TDIA 00010—2022

基于数字孪生的新型智慧城镇建设技术规范

第 2 部分：数字治理

(征求意见稿)

2022 - 12 - 20 发布

2022 - 12 - 20 实施

北京电信技术发展产业协会发布 发布

目 次

前言.....	III
引言.....	IV
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	2
4 党建引领建设.....	4
4.1 组织建设.....	4
4.2 党员学习.....	5
4.3 统计分析.....	7
4.4 用户管理.....	7
5 城镇治理.....	7
5.1 生态环境综合分析.....	8
5.2 垃圾分类全流程治理分析.....	8
5.3 地下管线综合分析.....	9
5.4 工地精细化管理分析.....	11
6 社会治理.....	11
6.1 创建文明城市.....	12
6.2 政务巡查.....	12
6.3 防疫.....	13
7 数字社区.....	13
7.1 综合治理.....	13
7.2 社区安防.....	14
7.3 应急指挥.....	14
8 农村数字化能力.....	15
8.1 农村公共服务.....	15
8.2 农村网业协同服务.....	15
9 系统安全保障建设.....	16
9.1 一般规定.....	16
9.2 前端安全.....	16
9.3 平台安全.....	16
10 支撑系统建设.....	17
10.1 一般规定.....	17
10.2 接口建设方案.....	17
10.3 安全系统方案.....	17
10.4 存储系统和备份系统建设方案.....	23
11 数据与数据接口标准.....	23

11.1 一般规定.....	23
11.2 接口标准规范.....	23
12 结束语.....	25

前 言

本文件按照GB/T1.1—2020《标准化工作导则第1部分：标准化文件的结构和起草规则》的规定起草。请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由北京电信技术发展产业协会提出并归口。

本文件起草单位：北京市怀柔区杨宋镇人民政府、北京电信技术发展产业协会、三六零视觉科技有限公司、中科云星（北京）科技有限公司、华夏无限科技有限公司、中国联合网络通信有限公司内蒙古自治区分公司、中关村泛联移动通信技术创新应用研究院、国兴网络有限公司、大唐安途（江苏）信息技术有限公司、广东省地理国情监测与综合分析工程技术研究中心、河北省高分辨率对地观测系统数据应用中心、北京建院装饰工程设计有限公司、北京智象信息技术有限公司。

本文件主要起草人：王磊、李文华、李永振、张伟、陈杰飞、孙遥、刘思、李炳华、樊敬尧、高金龙、王东、朱巍、白伟、张戈、马俊涛、杨明、孙照辉、刘曦镁、魏红哲。

引 言

伴随着大数据、人工智能等新兴资源和技术的应用推广，城镇治理正经历深刻的数字化转型。近年来，我国各地以习近平新时代中国特色社会主义思想为指导，践行以人民为中心的发展思想，坚持党建引领，深入推进治理体系和治理能力现代化建设。为切实提高政府的数字治理能力，充分发挥数字科技在政府工作中的优势和作用，探索基于政务、民生、防疫、舆情等丰富场景的数字化应用工具和平台，加快推进社会信息资源整合和应用共享，围绕“人、地、事、物、情、组织”等城镇公共服务和治理要素进行“一网统管”，实现城市运行“全域感知、智能响应、全局协同”，在数字孪生的新型智慧城镇建设的业务及相关规范的基础上制定《基于数字孪生的新型智慧城镇建设技术规范第2部分：数字治理》，推动镇域农村社会“治理”逐步向“智理”转变。

基于数字孪生的新型智慧城镇建设技术规范

第2部分：数字治理

1 范围

本文件规定了基于数字孪生的新型智慧城镇建设应用技术、应用范围、业务需求、场景建设规范等方面内容。

本文件适用于但不限于由城镇建设向城镇管理、智慧运行及城镇服务转变产生的新型智慧城市建设要求，运用大数据、物联网、云计算、人工智能、移动互联网等新一代信息技术，对城市运行进行全局监测和分析，以打好基础、做好服务、强化能力、加强开放为指导，构建智能、宜居、生态、可持续发展的智慧城市典范。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB 8566—2007 软件开发规范
- GB/T 8567—2006 计算机软件产品开发文件编制指南
- GB/T 9385—2008 计算机软件需求说明编制指南
- GB/T 9386—2008 计算机软件测试文件编制指南
- GB/T 13923—2006 基础地理信息要素分类与代码
- GB/T 7408—2005 数据元和交换格式 信息交换 日期和时间表示法
- GB/T 14394—2008 计算机软件可靠性和可维护性管理
- GB/T 16831—2013 基于坐标的地理点位置标准表示法
- GB/T 17798—2007 地理空间数据交换格式
- GB/T 17963—2000 信息技术 开放系统互连 网络层安全协议
- GB 21139—2007 基础地理信息标准数据基本规定
- GB/T 29854—2013 社区基础数据元
- GB/T 30320—2013 地理空间数据库访问接口
- GB/T 31490.1—2015 社区信息化 第1部分：总则
- GB/T 34680.4—2018 智慧城市评价模型及基础评价指标体系 第4部分：建设管理
- GB/T 36333—2018 智慧城市顶层设计指南
- GB/T 36620—2018 面向智慧城市的物联网技术应用指南

- GB/T 36621—2018 智慧城市信息技术运营指南
- GB/T 36625.2—2018 智慧城市数据融合 第2部分：数据编码规范
- GB/T 36625.3—2021 智慧城市数据融合 第3部分：数据采集规范
- GB/Z 38649—2020 信息安全技术 智慧城市建设信息安全保障指南
- GB/T 41150—2021 城市和社区可持续发展 可持续城市建立智慧城市运行模型指南
- GB 50348—2004 安全防范工程技术规范
- CJJ 100—2004 城市基础地理信息系统技术规范
- CJJ 103—2004 城市地理空间框架数据标准
- CH/Z 9001—2011 地理信息公共服务平台 电子地图数据规范
- GA/T 367—2001 视频安防监控系统技术要求
- HT 9015—2012 三维地理信息模型数据产品规范
- SJ/T 11608—2016 人脸识别设备通用规范
- DB33/T 552—2005 1:500、1:1000、1:2000基础数字地形图测绘规范
- DB31/T 294—2018 住宅小镇域智能安全技术防范系统要求
- T/SCSS 020—2017 智慧城市智慧社区规划导则

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧党建 SmartPartyBuilding

智慧党建是现代社会党建工作的一种新理念。它是运用互联网、大数据等新一代信息技术，实现党建信息资源融合共享，稳步提升新时代党建科学化水平。促使党的建设多维度全覆盖、党建措施智慧生成的实现，从而提升党的执政能力和治理能力。

3.2

城市治理 Urbangovernance

城市治理是指从广义的角度上是一种城市地域空间治理的概念，为了谋求城市经济、社会、生态等方面的可持续发展，对城市中的资本、土地、劳动力、技术、信息、知识等生产要素进行整合，实现整体地域的协调发展。狭义的城市治理是指城市范围内政府、私营部门、非营利组织作为三种主要的组织形态组成相互依赖的多主体治理网络，在平等的基础上按照参与、沟通、协商、合作的治理机制，在解决城市公共问题、提供城市公共服务、增进城市公共利益的过程中相互合作的利益整合过程。

3.3

社会治理 Socialgovernance

社会治理是指社会治理是政府、社会组织、企事业单位、社区以及个人等多种主体通过平等的合作、对话、协商、沟通等方式，依法对社会事务、社会组织和社会生活进行引导和规范，最终实现公共利益最大化的过程。

3.4

数字社区 DigitalCommunity

数字社区是通过数字化信息手段将管理、服务的提供者与居民实现有机连接的网络系统。这种数字化的网络系统，使社会化信息提供者、社区的管理者与住户之间可以实时地进行各种形式的信息交流互动。

3.5

农村数字化能力 Ruraldigitalcapability

农村数字化能力是伴随网络化、信息化和数字化在农业农村经济社会发展中的应用，以及农民现代信息技能的提高而内生的农业农村现代化发展和转型进程，既是乡村振兴的战略方向，也是建设数字中国的重要内容。

3.6

智慧城市 SmartCity

智慧城市是指利用各种信息技术或创新概念，将城市的系统和服务打通、集成，以提升资源运用的效率，优化城市管理和服务，以及改善市民生活质量。

3.7

物联感知 TheInternetofThings

通过射频识别（RFID）、红外感应器、全球定位系统、激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络。

3.8

元数据 Metadata

元数据，又称中介数据、中继数据，为描述数据的数据，主要是描述数据属性的信息，用来支持如指示存储位置、历史数据、资源查找、文件记录等功能。

3.9

数据库 Database

数据库是按照数据结构来组织、存储和管理数据的仓库。是一个长期存储在计算机内的、有组织的、可共享的、统一管理的大量数据的集合。

3.10

大数据 BigData

大数据指的是所涉及的资料量规模巨大到无法透过目前主流软件工具，在合理时间内达到撷取、管理、处理、并整理成为帮助企业经营决策更积极目的的资讯。

3.11

云计算 CloudComputing

云计算是分布式计算的一种，指的是通过网络“云”将巨大的数据计算处理程序分解成无数个小程序，然后，通过多部服务器组成的系统进行处理和分析这些小程序得到结果并返回给用户。

3.12

人工智能 ArtificialIntelligence

人工智能是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。它企图了解智能的实质，并生产出一种新的能以人类智能相似的方式做出反应的智能机器，该领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。

3.13

云环境 CloudEnvironment

云环境是指能够从动态虚拟化的资源池中向用户或者各种应用系统按需提供计算能力、存储能力或者虚拟机服务等互联网或者大数据环境。

3.14

地理信息系统 GISGeographicInformationSystem

地理信息系统是一种特定的十分重要的空间信息系统。它是在计算机硬、软件系统支持下，对整个或部分地球表层（包括大气层）空间中的有关地理分布数据进行采集、储存、管理、运算、分析、显示和描述的技术系统。

4 党建引领建设

党建引领重点为各级组织部门提供的基于PC端及手机应用的基层党建工作信息系统，通过该系统可对基层党员信息进行存储和管理，也可实现各级组织部门与基层党员之间的政策下达、意见反馈和信息互动。系统的建立是加强各级党组织与基层党员的沟通联系，实现信息快捷传递，实现基层党建工作的信息化的重要手段。

4.1 组织建设

4.1.1 党组建设

组织建设管理：通过组织管理模块将组织建设全流程信息化、组织化，包括党委换届、支部换届、新增党组、党组撤销、党组织排序、党组织的查询等全流程电子化办公；

组织荣誉管理：获奖组织在获奖之后，支部委员，党委委员进行组织获奖归档；经支部书记审核后
进行组织获奖的公开。

4.1.2 党员管理

党员管理包含以下内容：

- 党员档案管理：新增党员、党员变动、党员发展、党员调出时的全信息存档、跟新及删除；
- 党费管理：设置党费标准、党员交纳正常党费、党员交纳特殊党费、支部党员党费情况、党费支出、支部党费统计、党委党费情况等生成报表；
- 党员荣誉管理：确定表彰范围，制定评选标准，推荐评选，确定对象，考察审批，作出表彰决定，宣传先进事迹。党员获得相关荣誉后，组织委员，宣传委员对个人荣誉进行归档。

4.1.3 组织发展

组织发展模块应包含以下内容：

- 入党流程：完成入党全流程，如填写入党申请书、成为积极分子、发展对象、预备党员、正式党员全流程电子化审批；
- 民主评议：党委委员，通知开会，电子化进行评议，将每次会议评议结果公示、归档；
- 计划总结：支委、党委、党组分别制定年度计划书和年度工作计划、修改、存档。

4.1.4 党员建设

制定党员计划（本年度）、党员承诺、党员民主评议进行归档。

4.1.5 党组电子信息库管理

党组电子信息库管理应符合下列要求：

- 电子档案管理：对各级党员的人事档案进行分类、归档管理；
- 文件资料柜：为各级管理部门提供扫描纸质档案自动录入等文件资料管理服务，每条记录包括文档编号、文档名称、发布人、发布时间等信息；
- 数据导入：填写党员信息等相关内容后，将信息导入系统，系统自动生成主要组织架构及人员信息；
- 年度报表：将系统数据中党员信息按指定格式导出，自动生成上报组织的基础报表样式；
- 组织设置：设置党组织和行政部门基本信息；
- 人员设置：提供按党组织和按部门两种查询人员的方式，可以查看修改人员信息可以添加人员；
- 流失党员汇总：运用 LBS 通过基站定时轮训党员位置，对党员流动轨迹进行记录，最终提供数据以供统计分析，汇总党员流失情况；
- 电子通讯录：将所有党员的通讯地址信息统一录入，通过 PC、手机终端两种呈现形式便于党员之间相互沟通（将电子通讯录接入 PC/手机端）。

4.2 党员学习

4.2.1 在线学习

在线学习主要包含以下内容：

- 党建学习：通过手机客户端上网方式，访问智慧党建管理服务平台系统。查看党建的有关知识、基层党委近期工作，为广大党员了解党的时事政治，查看基层党组织各类活动提供便利；
- 统计党员学习情况：统计党员学习时间、登陆次数、在线考试成绩等信息；
- 在线练习：学员在线可以选择练习资料进行练习，可以实现自主练习、练习记录查询等功能；
- 在线考试：包含在线考试，在线提交阅卷，错题收藏等功能。

4.2.2 在线学习管理

在线学习模块应支持以下操作：

- 视频在线学习：视频在线学习由接入服务、视频播放服务、学习信息存储、播放客户端等四个部分组成；
- 文档在线学习：文档学习服务由接入服务、文档转换服务、文档存储服务、学习信息存储及播放客户端组成；
- 课程管理：课程管理由教师课程管理和学员课程管理两个部分组成；
- 教师课程管理：设置必修课课程、课程教学对象、授课起止日期、课程学时、课程学分；设置选修课课程、课程教学对象、授课起止日期、课程学时、课程学分；审核学员对选修课的选择；
- 学员课程管理：查询必修课的相关情况，查询选修课的相关情况，选择选修课程；
- 学习测评管理：党建平台学习人员通过 PC/手机端进行在线答题、学习小测、手机短信答题、综合测试等测评功能来考核学习情况。

4.2.3 党员学习进度分析管理

学习进度分析管理应支持教师学习进度管理和学员学习进度管理，具体要求如下：

- 教师学习进度管理：按课程查看相关学员的学习情况；按学生查看相关课程的学习情况；根据设定的条件，自动生成学习情况、考核情况报表，进行综合的查询、统计分析；对进度拖后的学生进行短信群发提醒；
- 学员学习进度管理：查看自己的必修课学习进度；查看自己的选修课学习进度；查看自己已获得学分总数。查看学习情况、考核情况分析报表。

4.2.4 调查问卷及民主评定管理

调查问卷及民主评定管理内容如下：

- 问卷调查：由组织部相关工作人员发起和统计；党员干部学员及下级组织部门负责回答；问卷调查由首页、问卷内容管理、结束页组成；

——问卷内容管理包括：分类、题目、题型、答案等内容的管理；

——民主评定：由组织部相关工作人员发起对某项议题的评定；党员干部学员及下级组织部门通过 PC/手机进行表决、打分。

4.2.5 网上党校

开通网上党校，发布党建制度和各种基础知识，进行党员学习积分排名，通过互动的形式提升党员教育管理水平。可为支部以上各级党组织建立自己的栏目阵地，网站首页提供非常方便直观的导航手段，方便各级党员到自己组织的网页学习交流；

——栏目和积分设置：设置党员学习的栏目、积分、栏目级别。通过使用积分的手段将党员学习生活情况进行量化；

——党务公开：信息发布，面向系统的主管单位使用；信息由党员干部及下级组织部浏览；信息包括：通知公告、党建相关新闻的发布、精品课程推荐发布后的信息，浏览者可以通过 PC、手机、平板电脑进行浏览；

——党建制度：党员奖惩录入，记录党员的获奖及处分，记录党组织的荣誉；党员联系对象设置，设置党员的帮扶对象；党员调动管理，党员调动信息的修改和审批；满意度测评，查询、设置满意度测评项目；党费缴纳，设置人员岗位对应应缴党费金额。

4.3 统计分析

统计分析模块应支持以下操作：

——学习成绩数据分析与统计：系统可以根据具体业务提供多张报表以供查询与分析。党员学习情况进度分析报表，党员流动情况报表，党员基本情况汇总报表；

——满意率测评数据分析与统计：系统将定期开展满意率测评值根据群众占 60%，党员占 30%，领导占 10%等占比统计报表，以此反映群众对党员的满意率；

——绩效管理数据分析与统计：系统引入党员绩效管理制度，全面管理、分析党员的工作业绩情况，提高党员的战斗力和战斗力。

示例：党员考核报表、工单处置进度报表等。

4.4 用户管理

用户管理应支持以下操作：

——系统普通用户的功能：系统登录、个人信息维护、用户密码修改；

——系统管理员的功能：用户管理、角色及权限管理、组织结构及部门管理、帐号审核、系统日志管理。

5 城镇治理

基于数字孪生的新型智慧城镇建设数字基座创新政府公共服务模式，利用现实世界中的建筑、设施、人、物、事件等所有要素，实现数字化并在网络空间孪生再造与之对应的“虚拟城市”以基层管理要素中的“人、地、事、组织”为出发，随时随地、按需精准服务企业和个人，全面提升公共资源使用效率和社会满意度。

5.1 生态环境综合分析

为有效监测生态环境指标，构建智能化、精细化管理模式，通过多维度数据收集并联动分析。采用大数据融合分析方式，收集工地数据、渣土车数据、气象数据、环卫滴水作业、实时交通状态、园林绿化等数据，将数据集中进行分析。

5.1.1 大气异常分析

在环保态势页面，地图显示的大气站点如果出现污染情况。

示例：如PM10超标，就会触发预警，用户通过点击预警信息，即会进入大气站点页面，进入污染预判阶段。

5.1.2 月度环境空气质量累计情况

月度环境空气质量累计情况，包括月度优良天数以及相比去年同月的优良天数增长情况。年度空气天数分析，包括本年度优良轻污中污所占比例，以及相比去年优良天数增量。

5.1.3 AQI实时数据

AQI实时数据，以饼状图的形式呈现，包括AQI、各种监测指标的数值及优良情况，以及首要污染物。各社区、村实时AQI排名，以街道为单位按空气质量进行排名。

5.1.4 达标压力

达标压力，包括主要污染物的目标值，本年及近三年值。

5.1.5 扬尘分析

结合空气质量实时监测设备回传数据以及区域内视频监控，针对监测指标与收集的扬尘相关数据的空间关系进行分析，可分析监测设备与车流量较大路段之间的距离、监测设备周边的渣土车聚合数量、监测设备与大型工地之间的距离等。根据各项数据对扬尘指标的影响严重程度，可设置各项数据的指标分级阈值与指标权重，通过权重分值进行统计，分析出扬尘影响居民生活的区域范围以及展示扬尘影响热力图。

5.2 垃圾分类全流程治理分析

通过建立垃圾分类全流程精细化管控平台，对垃圾分类进行智能化、科技化和数据化管理，综合利用物联网、Ai、云计算、大数据分析等科技手段对垃圾的分类投放、分类清运、分类处理等相关数据进行综合分析，实时掌握垃圾分类工作的开展成效、全面提高我区垃圾分类的知晓率，参与率、和正确率，

为我区制定垃圾整体减量的考核依据提供数据支撑，并推动实现我区垃圾投放、清运和处理等相关成本的降本增效。

5.2.1 垃圾分类主体基础数据分析

垃圾分类主体基础数据分析应具备以下功能：

- 垃圾分类主体基础数据，统计、分析垃圾分类参与主体（居民、沿街商户、社会单位等），掌握垃圾分类主体的基础信息，并建立基础信息数据库；
- 统计分析各街道社区、机关单位、沿街商户等垃圾产生量和垃圾类别的区域分布数据；
- 统计分析社区居民垃圾分类的参与率、正确率数据以及变化趋势。

5.2.2 厨余垃圾分出率的数据预警

针对重点考核的湿垃圾（厨余垃圾）分出率，建立各街道社区干湿垃圾分类计量的预警数据，实时掌握湿垃圾和干垃圾的计量数据，设定预警数据指标。提升厨余垃圾的分出率。

5.2.3 垃圾分类指导员工作成效数据

建立垃圾分类指导员信息数据库、全面掌握垃圾分类指导员的工作成效数据（包括各街道垃圾分类指导员数量、区域分布、服务时长、服务成效等相关数据），促进垃圾分类公众参与的管理成效。

5.2.4 垃圾分类问题的协同监管

融合接诉即办、网格巡检、物联网监控、视频监控等多类数据资源，对垃圾分类投放、垃圾混装、混运、垃圾生产量异常、居民参与率、正确率下降、垃圾处理成本异常等情况进行监管分析，并分析不同问题的要素关联、问题可能成因，为垃圾分类的管理工作提供科学完善的数据依据。

5.3 地下管线综合分析

地下管线综合分析，坚持问题导向、重在预防、综合管控、着力在防风险、以统筹计划监管、健全巡查机制、加强信息共享为主要措施，强化安全生产责任落实，统筹地下管线监管、最大限度预防和减少安全风险，通过信息化手段初步实现对地下管线安全运行的地上、地下全面管控，变被动为主动。

5.3.1 地下管线基础展示

实现热力、燃气、排污水数据为试点建设地下管线基础展示功能。

5.3.2 地下管线监督管理

地下管线监督管理应具备以下功能：

- 系统管理基础：提供用户管理、日志管理、权限管理、角色管理、层级管理等基础功能。相关管线类别、主管单位等角色权限可扩展，支持未来运营管理单位扩充；
- 接口管理：与微信小程序、城管委数据平台、城指平台问题上报等接口对接；

- 通知公告：提供系统通知及根据系统规则触发的自动通知；
- 统计分析：提供备案信息统计、施工信息统计、日常巡查统计、在施工巡查信息统计、上报问题统计分析等功能；
- 任务管理：根据人员和道路进行管网巡查任务设定和分配；
- 施工信息管理：涉及挖掘的施工信息、备案信息、管线信息增删改查，批量导入，临时施工点审核等；
- 上报问题管理：通过小程序上报的问题汇总及管理；
- 文件存储管理：对施工信息及上报问题的视频、图片、附件等文件的存储管理；
- 地图管理：提供二三维地图基本操作、地上地下空间基本操作、三维地理数据图层控制、三维空间量算、三维管线图例、地图接口、三维管线标注等功能；
- 基于地图的查询管理：基于地图的通用查询、快速查询、基本信息查询、符合条件查询等。
- 管线统计：实现管径分段统计、埋深分段统计、类型统计、管点管径分类汇总、材质分类汇总等；
- 管线分析：实现断面分析、净距分析、区域分析、拓扑分析等基础分析功能；实现上下游分析、流向分析、控制分析、爆管分析等功能；
- 监测控制管理：包括预警服务、控制服务、与巡检业务的地图交互服务；
- 管线编辑：包括地形开挖、编辑管线、编辑隧道等功能；
- 数据共享：根据城市大脑及相关信息系统需求，定制数据共享目录及共享机制。

5.3.3 巡查及问题上报移动端

巡查及问题上报移动端应符合以下要求：

- 道路巡查：实现巡查打卡，查看巡查记录（调用 GIS，生成轨迹）；根据任务系统发布的任务进行巡查，并查看历史任务；
- 问题上报：获取附近的施工点信息，自主上报案件；在巡查任务中上报案件，包括能查到备案信息的和未查到备案信息的问题上报；
- 我的任务：根据权限查看当前部门及个人的任务信息。包括待办任务、已完成任务等。并进行任务处理；
- 通知公告：接收、查看后台系统通知，并记录已读未读状态；
- 个人中心：个人基础信息维护。

5.3.4 地下管线信息共享系统

地下管线信息共享系统应符合以下功能：

- 通知公告：接收、查看监督管理系统发布的通知，并记录已读未读状态；

- 统计分析：各行业主管部门可根据自身权限查看相应备案信息统计、施工信息统计、日常巡查统计、在施工巡查信息统计、上报问题统计分析等功能；
- 任务管理：各行业主管部门接收共享任务，对上报问题等进行任务处理，处理完成后反馈处理结果；
- 上报问题管理：各行业主管部门针对本主管部门负责的上报的问题汇总及管理；
- 施工信息管理：涉及本行业主管部门的挖掘的施工信息、备案信息、管线信息增删改查，批量导入，临时施工点审核等；
- 管线信息共享服务：根据不同行业主管部门，对不同管线统计、管线分析、监测控制进行信息共享。

5.4 工地精细化管理分析

城市管理建设其中重要的一环是对重大项目的建设关怀以及建设监管,通过对重大项目现场安装物联网感知设备,实时获取相关感知数据反馈到城市管理平台。领导可以实时掌控各大项目的工期进展情况以及下场工作环境、施工人员的文明施工情况。

5.4.1 工地文明施工与环境监管

通过政府部门在工地现场部署的摄像头等物联网检测设备获取数据,根据基础设施建设数据标准,通过统一的接口收集政府建设设备数据。

环境监测方面包括扬尘监测、噪声监测、空气指数监测、风力监测。

5.4.2 施工现场视频监管

通过施工现场部署并全覆盖的红外线、昼夜网络高清监控设备获取数据,可随时随地监控现场作业情况,掌握工程实时动态,抓拍违章作业行为,加强安全生产管理,了解安全生产状况。

5.4.3 工地运输车辆监管

政府对施工机械运输作业车辆的监控,通过对运输设备工作期间的运行参数、状态信息等数据以及道路视频数据采集,运用智能算法自动识别运输物品遗洒、车轮带土等违规情况,根据车辆轨迹视频图像计算出所属工地范围。

工程运输及作业车辆监管主要包括对装载机、推土机、沥青摊铺机、叉车、渣土车等各类车辆的司机信息、车辆轨迹、运输物品、运输时间、运输线路等进行监管。

通过数据分析技术实时进行预警预测,提高政府的监管能力,有效控制工程建设中各类材料与垃圾的运输所产生的城市管理问题。

6 社会治理

通过数据中台和智能中台的数据共享交换，实现政府部门间的业务协同，以“接诉即办”为抓手，倒逼政府组织机构改革，提升政府数字治理效能。推进“互联网+政务服务”改革，以“在接诉即办工作中抓创城、抓城市管理，在创城、城市管理中抓接诉即办”创新服务模式、优化办事流程、减免办事材料的工作要求，扎实推动接诉即办与创城、城市管理工作中紧密结合、相互促进，聚焦共性问题，建设“互联网+创城，互联网+政务巡检”，有效的聚焦镇领导、干部和党员；发动企业、群众，将治理软件终端向社会、群众延伸，实现“随手报、闭环治理”的社会治理服务。从“创城—政务巡检—防疫”三个角度出发，实现多种场景的交互。

6.1 创建文明城市

创建文明城市应包含以下内容：

- 移动端实现对创城城市巡检情况进行登记和统计分析，登记信息包括责任人、时间、路段名称、测评标准、状态、操作等；
- 管理端实现对创建文明城市进行指标任务的管理，管理内容包括测评结果/全部、测评结果/今天、复审核结果、指标任务、测评标准、考核区域等。

6.2 政务巡查

6.2.1 城管巡查

城管巡查应包含以下内容：

- 移动端实现对经营单位进行城管巡查，对巡检责任人进行时间+定位，巡检情况进行登记，房屋属性进行编辑，所登记信息包括经营单位名称、最后调整时间、经营状况、公司类型、法人代表等；
- 服务端实现对经营单位进行城管巡查管理，安全巡检对象包括道路交通和市容环境，管理内容包括测评结果/全部、测评结果/今天、指标任务、测评标准、经营单位、自建房、小类管理等。

6.2.2 安全巡查

安全巡查应实现以下功能：

- 移动端实现对经营单位进行安全巡查，对巡检情况进行登记，所登记信息包括经营单位名称、企业证照名称、经营场所地址、最后调整时间、经营状况、公司类型、法人代表、电话、企业类型、登记注册类型、规模生产经营单位、生产经营方式、行政隶属关系、企业规模、营业执照、营业状况、备注等内容，提交确认电子签字；
- 服务端对经营单位进行安全巡查管理，安全巡检对象包括村民自建房安全检查、道具库现场检查、工业企业安全检查、敬老院老年驿站安全检查、酒店安全检查、旅游景区安全检查、拍摄园区安全检查、七小门店安全检查、医疗机构检查、中小学幼儿园安全检查、居住自建

房重大火灾安全检查，管理内容包括测评结果/全部、测评结果/今天、指标任务、测评标准、经营单位、自建房、小类管理等。

6.3 防疫

防疫应至少包含以下内容：

——移动端实现对人员进行登记，可以进行人员信息新增和修改，人员信息包括身份证号、姓名、居住地址、针次、机构、到镇日期、核酸证明、机构地址、负责人、法人等；

——服务端实现对“核酸检测、疫苗、人员摸排”三个角度进行管理，实现多种场景的交互，具体要求如下：

- **核酸检测：**对各类人员核酸检测情况进行管理，管理信息包括企业（单位）名称、进货名称、地址、所属镇街、行业监管部门、所属行业、七小分类、姓名、身份证号、联系电话、详细地址、核酸检测频次、当次检测时间、下次检测时间、共同居住人员等，可以核酸检测信息进行查询、二维码查询、导出逾期和全部信息，可对所需信息字段进行配置；
- **疫苗：**对疫苗接种情况进行管理，对第一二针区考核底库、第三针区考核底库、第三针重点人群底库、第一二针台账外数据、第三针台账外数据进行统计和汇总，可对各底库信息进行统计、查询及导出；
- **摸排管理：**对境内人员排查口径统计、境外人员排查口径统计、相关人员排查台账关联排查统计、相关人员总台账表排查统计，可对各统计表进行导出。

7 数字社区

7.1 综合治理

数字社区在综合治理方面，结合5G+AIOT、大数据等技术，打通社区内智慧场景，从“人一房一事”三个角度出发，实现多种场景的交互。

——对接“人”的角度，以地名地址管理为基础，以人口和房屋管理为主要内容，以网格管理为主要思路，以部门信息共享交换为主要支撑，实现对社区各类人口信息的动态采集、更新和维护，并通过对居民各类诉求的采集上报，保证数据录入的准确性，实现市民与政府的良性互动，形成实时、敏捷、长效管理机制，真正做到社区“底数清、情况明”。主要从居民人口资料管理，居民信息反馈，流动人口、孪生社区四个维度实现。居民资料管理以网格化的方式建立居民人口数据库，实现分域分管，并通过大数据交互，实现人口数据基座，匹配居民不同情况，实现合理化服务。同时对接安防、应急系统，进行不同级别的应急资料管理；居民信息反馈通过社区统一平台，畅通民情民意表达渠道，鼓励社区居民积极参与社区治理；流动人口服务通过信息技术手段，为流动人口提供信息采集、登记、居住证明办理服务，流动人口中重点人员和安全隐患、流动人口案(事)件、违法活动线索、出租房屋内案(事)件等业

务管控，提升社区内流动人口社会保障、基本公共服务水平；将社区、小区、网格、楼栋等信息直观的展现在社区孪生体中，方便工作人员快速定位楼栋房间，实现对场所、家庭、人口的精细化管理；

- 对接“房”的角度，通过“以房管人”的管理理念，结合GIS、智能AI技术，收集社区内建筑、公共设施等基础数据，并通过大数据实时交互共享给社区管理端。同时，依靠遥感与AI技术的结合，针对特殊人群或水电管道、智慧充电站等重要设施进行数字化管理，并增加相应标签，有效监管社区内违章建设，如私搭房屋，私改管道，私接线缆等行为，保障社区安全；
- 对接“事”的角度，通过业务和数据层面，实现社区协同治理。在网格化管理的基础上，结合GIS、物联网等技术，建立社区事件处置机制，通过数字孪生技术将日常业务信息展现在统一的平台上，包括社区人口数据，社区事件数量、类型分布等信息，进行家庭、商铺安全隐患分析，事件多发区域的预警和展示，以便做出针对性处理，为公安、监管局等管理部门有效赋能。

7.2 社区安防

数字社区将GIS+边缘服务融入物联网、大数据、人工智能分析等技术，精确把握社区内人、地、物的信息，将住户、租户、商户实现数据化标签，把流动人口纳入安防管控体系，并依据孪生社区基底数据与视频安防监控设备相结合，实现行为轨迹信息的分析，对可能存在的安全威胁，进行提前感知和实时探知。社区安防体系自动对进入社区的人员进行人像抓拍，并与留存的白名单进行比对分析，预警可能风险，并提醒社区工作人员上门核实，验证真实信息；

严格社区小区出入门禁管理，规范住户门禁卡实名办理，访客实名登记，小区门禁出入视频监控、人脸识别、公安联网比对等安防措施，建立城市建筑消防安全数字化系统，把每个建筑物的消防系统联网，实现网络化的监控管理；

在防疫场景中，利用视频安防监控，结合孪生社区基底数据与AI相结合，可以有效避免与疑似或确诊人员接触。对于社区孤寡老人、小孩、残疾人等重点看护人员，系统可以根据进出门记录和时间，智能分析及判断，提醒工作人员远程呼叫或上门查看。

7.3 应急指挥

目前社区的应急指挥对于应急分析、救援和处置方面尚不完善，对于重点场所的应急指挥存在遗漏问题。数字社区的应急管理从应急管理、组织结构和环境关系三个维度实现有机融合；

- 应急管理方面，数字社区将实现协同模式，将吸收社区居民、志愿团体等人员参与到应急管理过程中，结合GIS、AIOT等技术建立统一平台，在社区住宅、绿地等区域，提供基于物联网的消防设施、视频安防监控等设施，在紧急情况发生时实现智能预警，远程交互，安全引导等功能；

- 组织结构方面，数字社区呈现“扁平化”“智能化”特征，实现社区、执法机关、医疗机构三方联动。依靠 GIS+视频安防监控体系，统一协调应急管理工作，同时基于大数据和 IOC 平台，根据应急管理等级要求，提供智能化评估决策，并发挥协同治理作用；应急指挥上依托网格化管理，建立面向社区居民、网格长、网格员和治安管理人员，以电话、网络等方式为主的治安问题反馈机制，与出入口门禁系统、道闸系统、消防报警等系统实现有效联动，通过应急指挥系统进行调度指挥，及时快速地处理问题；
- 环境关系方面，实现应急管理系统与外部环境的良性互动。通过“社区数字孪生”场景演示，加强应急管理宣传工作和培训工作，提高社区居民应急反应能力。并对重点场景进行长效的场景监测，实现广播推送和重点推送，如对于孤寡老人、儿童家庭的火灾预警等。

8 农村数字化能力

农村数字化能力让乡村治理更为便捷有效，通过镇域感知体系与数字孪生城镇数字基座的数据和能力支撑，实现村规上图入库、在线查询、实时跟踪，有效地利用政府综合办公平台，实现农村数字化“信息发布、民情收集、议事协商、公共服务等村级事务”能力的场景化建设，通过网格将农村分解成一个个小块，专人解决对应区域的问题，农村社区网格化管理，将社区防控数据与公安、卫生健康、交通运输等部门数据汇总比对，形成分析能力的可视化中枢，实现了社区防控智能化、数字化、精准化。

8.1 农村公共服务

- 农村网格化管理：以村庄“一张图”为基础，“四级管理（镇、村、网格长、网格员）+户+房”组成网格信息，农村网格化管理从户籍与房屋两个维度实现精准集合，户籍方面，选择网格信息后，平台会根据实际情况将“常住户”、“流动户”、“空壳户”等户籍性质进行筛选，点选不同的户籍性质，在农村数字孪生体中可视化，房屋方面根据选择村庄名称信息，自动将村庄范围高亮显示，并自动定位，居中显示该村庄二三维地图，展示包含该村庄所的街巷、商业、楼栋和居民房，属性信息将该街巷、商业、楼栋和居民房的房屋资产和人员信息显示，同时人员信息会弹出住户信息卡，在农村数字孪生体中可视化，实现了精细、直观的人房信息管理模式。
- 农村安防管理：实现“视频安防监控”和“电子哨兵”有效结合，对居民小区、网吧/酒店/娱乐场所、沿街商铺/小街小巷、电动车停车场、乡镇院落等场景全高密闭环覆盖，实现视频监控、人员管理、车辆管理、疫情防控、智能分析、群众共治和综合治理等应用服务可视化；
- 农村环境数字化管理：通过视频监控+物联网传感设备强化垃圾分类、农村饮用水水源水质监测与保护，对农村污染物、污染源全时全程监测，实现农村环境综合监测系统。利用综合办公平台的村村版服务加强公众积极参与农村环境网络监督，共同维护绿色生活环境。

8.2 农村网业协同服务

运用5G+数字孪生技术，实现了农业指挥决策、治理决策、精准种植、科学预警、产品溯源、智慧营销等系统结构，推动传统农业向智慧化农业进行转型，助力乡村振兴发展。从“农业大数据决策、农产品种植精准化、数据普查智能化和园区管理数字化”四个角度出发，实现多种场景的交互。

- 农业大数据决策化。结合先进的信息化技术及深入的农业研究成果，通过物联网技术采集全域农业数据，通过农业数据治理在海量农业数据基础上构建农业资源信息库和农业修复方案库两大底层数据库；通过大数据分析、AI 计算、仿真技术提供六大前端服务模块：农业产业数字呈现、安全指数评估、高危区域分析、农业生态修复沙盘、方案推演仿真、综合效益追踪；
- 农产品种植精准化。利用 5G 组网与物联网传感器进行种植环境的采集，通过大数据分析决策，实现精准控制、科学预警；
- 数据普查智能化。利用 5G+AI+无人机应用，对农产品的种植规模进行数据普查，做到心中有数；
- 园区管理数字化。运用 5G 高清视频技术，实现农业产业园种植全景实时监控，打造放心农业产业园。五是农产品销售智慧化。运用 5G+区块链技术，消费者通过二维码实现“从农业产业园到消费者”的全程可追溯，有效保障了食品安全。

9 系统安全保障建设

9.1 一般规定

系统平台开发依据《信息安全等级保护管理办法》的有关规定，已通过信息安全等级保护三级测评及ITSS云服务能力标准三级认证，严格遵循国家在信息系统安全建设方面的技术保障和安全管理要求。

9.2 前端安全

平台的前端安全保障通过使用主动注册、双网口隔离、身份校验、数据加密等手段，确保数据传输私密可控。

9.3 平台安全

9.3.1 系统承载与 IDC 合作，采用多种手段确保平台的网络安全，以防范各类网络攻击及未授权访问，杜绝网络安全隐患。

9.3.2 系统通过一系列安全技术和安全管理措施，建立完整的主机操作系统及数据库的安全保护环境。安全手段包含“异常检测、漏洞扫描、主机账户规范管理、主机加固”。

9.3.3 系统从软件设计、开源服务部署、自研服务部署三个方面，确保平台应用安全。

9.3.4 通过数据加密传输、存储，双向加密通讯进一步保障平台的数据安全。

9.3.5 客户端访问支持校验用户名、密码的合法性，支持对用户所划分的数据、功能等权限进行验证，

验证通过后才能查看数据及功能使用。支持对客户端访问的日志审计功能，客户端实现账户管理、密码管理、日志记录。

10 支撑系统建设

10.1 一般规定

系统建设应满足信息系统基础规范、数据规范、应用规范等规范的要求。其中管理规范包括项目管理规范、系统运行维护管理规范等规范。

10.2 接口建设方案

10.2.1 城镇级共性平台要求

平台应具备数据收集、数据处理、数据共享、算法共享、统一认证登录等功能。平台使用的云计算资源均应源自城镇电子政务云平台。

10.2.2 城镇各部门业务系统

城镇数据共享交换平台应与其他业务系统进行数据交换共享，并通过与以综合应用支撑平台及系统对接，实现与相应系统及平台数据共享。

10.3 安全系统方案

10.3.1 安全计算环境

10.3.1.1 系统安全计算环境

10.3.1.1.1 主机身份鉴别与访问控制要求

主机身份鉴别与访问控制应符合下列要求：

- 系统应对登录用户进行身份标识和鉴别，保证用户名的唯一性；
- 登录口令必须具备采用 3 种以上字符、长度不少于 8 位，并且定期更换；
- 登陆失败应采取结束会话、限制非法登录次数和自动退出等措施；
- 远程管理时应启用 SSH 等管理方式，加密管理数据，防止被网络窃听；
- 自主访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级；
- 自主访问操作应包括对客体的创建、读、写、修改和删除等；
- 系统应制定严格的访问控制安全策略，根据策略控制用户对应用系统的访问，特别是文件操作、数据库访问等，控制粒度主体为用户级、客体为文件或数据库表级；
- 系统应严格限制默认账户的访问权限，重命名默认账户，修改默认口令；及时删除多余的、过期的账户，避免共享账户的存在。

10.3.1.1.2 一体化终端安全防护

系统应建设恶意代码防范体系、落实终端安全管理技术措施、启用统一终端运维、开启安全审计功能，建设终端合规一体化体系。

10.3.1.1.3 漏洞扫描系统功能要求

部署漏洞扫描系统，可以帮助用户快速建立针对自己网络的安全风险评估体系。

——系统应帮助用户快速发现内部风险，实现内部 IT 数据的标识和分类管理，方便安全扫描策略的部署和风险评估的进行；

——系统应利用漏洞知识库以及漏洞扫描策略，针对网络设备、系统主机、应用程序等存在的漏洞和风险进行有效评估，完善评估报告，帮助用户建立起高效的安全漏洞管理解决方案；

——系统应定期扫描漏洞，帮助用户形成规范的全网漏洞管理体系，并辅以风险报表以及解决方案建议，为用户提供了完整的从漏洞发现、验证、修复建议的流程。

10.3.1.1.4 虚拟机安全防护

系统应采用虚拟化安全管理类系统对虚拟主机进行统一的安全防护，并且应具备恶意软件防护、进程管控、防火墙、应用控制、入侵防护、DDoS防护等功能。

10.3.1.1.5 应用身份鉴别要求

应用身份鉴别应符合下列要求：

——标准化 CA 接口：数字证书认证中心检查证书持有者身份的合法性，并签发证书以防止被伪造或篡改，对证书和密钥进行安全管理；。

——登录密码加密：用户在客户端输入的密码采用 SHA—1 加密算法；平台对重要信息支持 MD5 不可逆算法，传输支持 HTTPS 协议；

——用户名+动态口令：安全登录除了需要用户名和密码外，还需要与用户相匹配的动态口令输入，以便于保障账户信息的安全性；

——登录验证码：用户登录需要输入随机验证码，以防止恶意爬虫程序等入侵，保证信息安全；

——身份验证狗：身份验证狗作为验证用户身份的 USB 可插拔式硬件，可提供保密性极高的登陆验证。

10.3.1.1.6 访问控制要求

访问控制应符合下列要求：

——权限控制总表：采用基于角色的访问控制权限体系，使权限控制更加严格；

——流程、公文、文档等详细内容的访问控制：在权限控制总表的基础上，设置不同用户权限的具体参数以及业务的逻辑顺序，从而实现全程零代码操作；

- 公告、调查等业务表单与附件下载、关联：系统用户在平台上只能查看自己身份权限范围内的公告、调查等业务员表单；
- 表单统计查询页面访问控制：业务逻辑体系应根据登陆用户角色所对应的权限，输出用户权限可查询的页面范畴，从而保证用户只能接触到权限内的信息；
- 文档的授权与日志：文档的相关操作，包括授权、只读、浏览、下载和打印等都采用 urlDigset 机制，用户在进行登录操作时，每次均会生成不同的动态参数，从而准确识别用户信息。

10.3.1.1.7 WEB 应用安全防护功能

WEB应用安全防护应符合下列要求：

- 漏洞防护：Web 应用类防火墙能够对 SQL 注入、跨站脚本、代码执行、目录遍历、脚本源代码泄露、CRLF 注入、COOKIE 篡改、URL 重定向等多种漏洞攻击进行有效防护；
- 攻击防护：针对 Flood 攻击、SQL 注入、跨站脚本、目录遍历等主要攻击手段，系统应提供有效识别、阻断并告警；
- 网页代码检查：Web 应用防火墙能够对用 ASP、ASPX、JSP、PHP、CGI 等语言编写的页面，对用 SQL Server、MySQL、Oracle 等数据构建的网站进行检查，能够在客户网站被“挂马”之前发现网站的脆弱点，避免“挂马事件”的发生；
- 访问加速：Web 应用防火墙应增加一层新的网络架构，以此来避免由于网络带宽小、用户访问量大、网点分布不均等原因造成的用户访问网站响应速度慢的问题；
- 网页防篡改：系统应对网页防篡改客户端进行实时监控。

10.3.1.1.8 应用安全系统功能要求

应用安全系统功能应符合下列要求：

- 身份鉴别：
 - 对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
 - 提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
 - 强制用户首次登录时修改初始口令；
 - 用户身份鉴别信息丢失或失效时，采用技术措施确保鉴别信息重置过程的安全；
 - 采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。
- 访问控制：
 - 提供访问控制功能，对登录的用户分配账号和权限；
 - 重命名或删除默认账户，修改默认账户的默认口令；
 - 及时删除或停用多余的、过期的账户，避免共享账户的存在；

- 授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
- 由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
- 访问控制的粒度达到主体为用户级，客体为文件、数据库表级、记录或字段级；
- 对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。

——安全审计：

- 提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- 审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- 对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- 确保审计记录的留存时间符合法律法规要求；对审计进程进行保护，防止未经授权的中断。

——入侵防范：

提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

——数据完整性：

采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

——数据保密性：

采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

——剩余信息保护：

保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

——个人信息保护：

仅采集和保存业务必需的用户个人信息；禁止未经授权访问和非法使用用户个人信息。

——开发代码安全：

第三方软件开发商应具备相应的开发资质，在应用开发过程中采用安全开发过程管理，并在开发过程中进行代码安全检测与审计，并要求第三方开发厂商提供系统源代码。

10.3.1.1.9 数据加密与保护要求

数据加密与保护应符合下列要求：

- 加强对于数据的分级分类管理：对关键敏感数据须设置标记，对于重要的数据应对其本身设置相应的认证机制；

- 加强对于数据的授权管理：对文件系统的访问权限进行一定的限制；对网络共享文件夹进行必要的认证和授权。除非特别必要，禁止在个人的计算机上设置网络文件夹共享；
- 数据和文档加密：网络设备、操作系统、数据库系统和应用程序的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性和存储保密性；当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息。

10.3.1.1.10 数据访问安全审计功能

数据访问安全审计应符合下列要求：

- 数据访问审计：记录所有对保护数据的访问信息，包括文件操作、数据库执行 SQL 语句或存储过程等。系统审计所有用户对关键数据的访问行为，防止外部黑客入侵访问和内部人员非法获取敏感信息；
- 数据变更审计：统计和查询所有被保护数据的变更记录，包括核心业务数据库表结构、关键数据文件的修改操作等等，防止外部和内部人员非法篡改重要的业务数据；
- 用户操作审计：统计和查询所有用户的登录成功和失败尝试记录，记录所有用户的访问操作和用户配置信息及其权限变更情况，以便用于事故和故障的追踪和诊断；
- 违规访问行为审计：记录和发现用户违规访问。支持设定用户黑白名单，以及定义复杂的合规规则，支持告警。

10.3.1.1.11 数据备份与恢复功能

数据备份与恢复应符合下列要求：

- 应提供重要数据的本地数据备份与恢复功能；
- 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
- 应提供重要数据处理系统的热冗余，保证系统的高可用性。

10.3.1.2 物联网系统安全计算环境

10.3.1.2.1 感知层设备身份鉴别

采用常规鉴别机制对感知设备身份进行鉴别，确保数据来源于正确的感知设备；对感知设备和感知层网关进行统一入网标识管理和维护，并确保在整个生存周期设备标识的唯一性。

10.3.1.2.2 感知层设备访问控制

通过制定安全策略如访问控制列表，实现对感知设备的访问控制；感知设备和其他设备（感知层网关、其他感知设备）通信时，根据安全策略对其他设备进行权限检查。

10.3.2 安全镇域边界

10.3.2.1 边界访问控制

10.3.2.1.1 系统应利用硬件防火墙和虚拟防火墙实现基于网络 IP 地址、协议、端口的强访问控制，并支持针对用户的访问控制。

10.3.2.1.2 系统防火墙安全策略可以控制内网访问外网的权限、控制内网不同安全级别的子网间的访问权限等。

10.3.2.2 边界入侵防范

边界处部署入侵防御类系统，主机层面部署主机安全防护类系统。主动阻断针对系统的各种攻击，如病毒、木马、间谍软件、可疑代码、端口扫描、DoS/DDoS等，实现对网络层以及系统的安全防护，保护核心信息资产免受攻击危害。

10.3.2.3 边界完整性检测

系统应部署终端安全类系统实现非法接入控制，提供非法外联监控功能，解决发现和管理用户非法自行建立通路连接非授权网络得行为。

10.3.2.4 边界恶意代码检测

在互联网边界处部署防病毒网关，在边界处进行病毒清除及拦截，防止病毒在网络内蔓延；在主机层面部署主机安全防护系统，主机层面进行病毒查杀防护。采用不同的病毒库，实现病毒防护能力的互补。

10.3.2.5 安全审计

部署网络安全审计系统，日志审计系统并开启网络设备、安全设备的日志功能，实现对网络设备的运行状况日志审计、流量审计等，应实现对日志信息的集中记录。利用集中日志系统收集网络设备日志。

10.3.3 安全通信网络

10.3.3.1 安全体系架构

安全体系构架应参照等级保护的要求对系统安全镇域域进行划分设计，从而实现内部办公、数据共享交换与外部接入镇域域之间的安全隔离，并对核心镇域域进行冗余建设，用以保障关键业务系统的可用性与连续性。

10.3.3.2 网络通信安全

网络通信安全应符合下列要求：

——密码技术：远程传输加密的设备或组件除了需要支持 AES、DES、3DES、RSA 等多种国际商用加密算法之外，还需要支持国密算法，包括 SM1、SM2、SM3、SM4 等。

——数据远程传输加密保护：远程办公终端连接 VPN 以后，远程终端与网关之间采用加密传输协议进行数据传输，以便于实现数据的保密。

——数据远程传输完整性保护：远程办公终端在传输数据的过程中，通过采用校验码技术或密码技术对传输数据的完整性进行验证和保护。

——多因素认证：能够采用用户名密码、数字证书认证、指纹认证、Radius 动态口令等多种身份认证方式进行认证。

10.3.4 安全管理中心

安全管理中心应负责设备安全运维与审计、集中安全运营与管理、策略集中管理与分析等工作。

10.4 存储系统和备份系统建设方案

10.4.1 主系统云环境

10.4.1.1 政务云平台对虚拟主机的备份采用每周全量备份，每天增量备份。

10.4.1.2 政务云平台对数据库归档日志备份采用每周全量备份，每小时增量备份。

10.4.1.3 备份服务器的备份任务对数据库数据文件每4个小时全库备份一次到备份服务器。

10.4.1.4 备份服务器的备份任务对数据库数据文件每4个小时全库备份一次到360云平台备份服务器。

10.4.2 备份系统云环境

10.4.2.1 政务云平台对数据存储采用每周全量备份，每小时增量备份。

10.4.2.2 政务云平台对虚拟主机的备份采用每周全量备份。

11 数据与数据接口标准

11.1 一般规定

11.1.1 建库规范应囊括每类数据的处理规则、更新规则、融合方法等内容。

11.1.2 规范的建设应结合国家、测绘行业及地方等相关规范的要求进行编制。

11.1.3 规范内容应涵盖范围、规范性引用文件、术语和定义时空基准、矢量数据处理、数据组织与命名规则等。

11.1.4 规范应重点规定矢量数据的处理流程、数据处理规则、时间标识添加原则。

11.1.5 规范应规定不同数据的组织方式和命名规则。

11.2 接口标准规范

11.2.1 数据共享接口标准

11.2.1.1 服务元数据模型

服务元数据模型应在《DGCWeb服务通用规范》、《ISO19119地理信息服务》的基础上，结合现行国家标准《地理信息元数据》以及最新的《ISO19115地理信息元数据》的内容，根据系统中对各类网络服务的应用需求按照Web服务的要求，规定描述各类信息服务的信息模型。

11.2.1.2 目录数据服务接口规范

11.2.1.2.1 包括描述获取系统目录及相关元数据描述接口方法及返回结果信息。

11.2.1.2.2 主要内容应包括前言、范围、规范性引用文件、术语定义、目录服务接口、云数据服务接口等。

11.2.1.2.3 目录服务接口以及数据服务接口均应详细描述获取系统目录的相关操作简介、使用协议、参数说明、调用方式、返回结果等。

11.2.1.3 数据服务接口规范要求

11.2.1.3.1 数据服务接口规范主要内容应包括前言、范围、规范性引用文件、术语定义以及各类 Web Service 服务接口等。

11.2.1.3.2 服务接口应包括 WMS、WFS、WMTS 等标准 OGC 服务，还应包括 REST 地图、矢量地图、三维地图、专题地图等服务。

11.2.1.3.3 服务规范应详细描述服务的操作简介、使用协议、参数说明、调用方式、返回结果等。

11.2.1.4 应用服务 API 规范

11.2.1.4.1 API（应用程序开发接），是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节。

11.2.1.4.2 应用 API 可以为应用层提供标准、灵活的云服务。应用框架则基于 ESB 进行扩展，提供一系列满足地理信息应用的 API，应用组件将通过这些标准的 API 进行数据交换、通信等工作，并通过应用框架把自身提供的 API 发布出去，供其他功能分区来调用。

11.2.1.4.3 规范应规定系统中主要服务类参考及常用服务示例。

11.2.1.4.4 应用 API 规范主要内容应包括前言、范围、规范性引用文件、术语定义以及 Javascript API、Flash API、Silver light API、Web 三维 API、桌面端开发 API、移动端开发 API 等的主要服务类参考及常用服务示例等。

11.2.2 仿真模拟规范

仿真模拟规范应包括模拟仿真的内容、模拟仿真的功能的使用、模拟结果的更新等。

11.2.3 系统集成接口规范

在项目建设过程中，不仅需要对接管理系统，还需集成各相关部门的业务系统。

12 结束语

本规范从端、管、云的维度规定了数字孪生的新型智慧城镇建设系统各部分的技术要求，为新型智慧城镇建设应用技术、应用范围、业务需求、中台建设规范、数据平台建设规范、数据系统标准等方面内容提供了更加先进实用、丰富可靠的手段。随着人工智能和物联网技术的进一步成熟和本规范的逐步推广应用，相关规范将有效支撑各区域等级规模的新型智慧城镇建设，在未来的城镇建设开发中对城镇运行进行全局监测和分析，为构建智能、宜居、生态、可持续发展的智慧城镇等方面发挥越来越大的作用。
