智慧城市产业生态圈白皮书

SCIE/WP 1-2019

智慧城市网络安全白皮书

智慧城市产业生态圈发布

二零一九年十二月十七日

编制单位（排序不分先后）

西安电子科技大学

深圳市标准技术研究院

山东省电子信息产品检验院（中国赛宝（山东）实验室）

华为技术有限公司

深圳竹云科技有限公司

北京神州绿盟信息安全科技股份有限公司

深圳市华傲数据技术有限公司

北京超图软件股份有限公司

目 录

1 前言

城市是人类生活和社会发展最重要的承载体，其内涵随着时代发展、科技进步不断丰富和延伸，人们的生活方式也被源于信息技术的创新力量持续影响和改变。特别是随着数字技术深度融入到政府管理、百姓民生、公共安全和产业发展等城市活动中，城市已逐步成为物理世界和数字世界融合的综合体，并被赋予了前所未有的内涵，即智慧城市。

自 2010 年以来，以“发展更科学，管理更高效，社会更和谐，生活更美好”为目标，中国智慧城市建设取得了积极进展。2015 年底国家又提出了“新型智慧城市”概念。当前，我国的新型智慧城市建设以“无处不在的惠民服务、透明高效的在线政府、融合创新的数字经济、精准精细的城市治理、安全可靠的运行体系”为总体建设目标，已经成为推动我国经济改革、产业升级、提升城市综合竞争力的重要驱动。

智慧城市是现代城市发展的新模式，以大数据、物联网、云计算、人工智能、5G、区块链为代表的新一代信息通信技术不仅改变了人们的生产、生活和交往方式，而且正在从根本上变革城市的规划、建设、运行、管理、服务方式，使得城市更加智能化。数字孪生通过构建城市物理世界和网络虚拟空间的对应，在网络空间再造一个与之匹配、对应的孪生城市，形成物理维度上的实体世界和信息维度上的虚拟世界同生共存、虚实交融。

日新月异的信息通信技术在给城市带来便利、高效、智能的同时，也带来网络安全挑战。数字技术融合在城市物理世界的各个方面，网络空间的安全问题对现实世界带来的影响越来越大，各种安全事件层出不穷：

2016 年 10 月 21 日，美国东部遭遇史上最大规模的 DDoS 攻击，攻击流量超过 1Tbps，亚马逊、Twitter、Netflix、Airbnb、PayPal 等百余家知名网站出现数小时的瘫痪。

2017 年 5 月 12 日，勒索病毒“WannaCry”席卷全球，在全球感染了至少 150 个国家超过 30 万台计算机，影响到金融，能源，医疗等众多行业。

2018 年 9 月，万豪国际集团旗下喜达屋酒店客房预订数据库遭黑客入侵，最多约 5 亿名客人的信息可能被泄露。

新技术的应用往往也带来新的安全风险，数据集中共享、工业控制系统数字化、物联网终端大规模部署使用、人工智能的安全等，都给智慧城市的安全带来了全新的挑战。数据安全及隐私保护、物联网安全、供应链安全等都是智慧城市安全建设需要考虑的主要问题。

通过分析智慧城市建设面临的网络安全风险，提出构建智慧城市安全体系的技术、管理和运营措施，为智慧城市安全建设提供指导和参考，智慧城市生态圈安全技术组特发布此白皮书。

2 智慧城市技术特征及框架

2.1 智慧城市技术特征

2.1.1 5G 的商用为智慧城市发展提供新支撑

5G 技术与 4G 相比，具有更快的数据速度、更高的带宽、更大的容量和更低的时延。在 5G 环境下，不仅给智能手机用户带来更好体验，还可以支撑摄像头、路灯、红绿灯、垃圾桶、汽车、无人机、各种仪表和家用电器等各种“物”连接上互联网，这将大大提高一个城市的感知能力和互联互通能力。

2.1.2 物联网让城市实现实时感知和控制

物联网（IoT）通过感知芯片或模块，将城市中的各种要素连接上网，使得城市有了“神经末梢”，可以实现对城市更好的感知和控制。通过各种网络可以实现物与物、人与物的互联。通过物联网实现万物感知、万物互联，是实现城市智能的基础。

2.1.3 Wi-Fi 覆盖给城市居民和游客上网带来便利

为方便居民和游客上网，一些城市在人员聚集的商务圈、旅游景点部署了 Wi-Fi 热点，提供免费上网服务。IEEE 也推出了新的 Wi-Fi 6（IEEE 802.11ax）协议，将在 2019 年底逐渐推出商用。Wi-Fi 6 高并发、广覆盖、低时延的特性将与 5G 技术一起为智慧城市构建更强大的“神经网络”。

2.1.4 区块链技术应用于智慧城市正逐步兴起

区块链基于分布式数据存储、多中心的点对点传输、共识机制和加密算法等多种技术集成创新，实现了不可篡改、可追溯、透明可信、系统高可靠等特点，解决了多方信任与高效协同的问题。在智慧城市中涉及多参与方的应用场景中，区块链可以发挥很好的作用。例如，区块链的高度可溯源性，可帮助监管机构、交易方或消费者核查某种产品的真实来源。在全球化供应链中，区块链有助于提高交易的可靠性并提升监管效率。

2.1.5 云让城市的 IT 资源高效复用随需使用

云计算技术让人们像使用水和电一样使用 IT 资源，按需使用、按使用量付费。一个城市统一集中建设云数据中心，为城市的各个政府部门、企业和个人提供 IT 资源，既有利于 IT 资源的高效复用，降低了建设成本和维护成本，也便于数据共享和大数据分析。云数据中心为政府部门办公、社会服务、各种智慧城市应用提供了一个公共平台。

2.1.6 通过数字平台打造智慧城市 IT 基础设施的“中间件”

智慧城市建设中，上层应用种类多，下层物联网连接多，搭建一个中间平台，可以沉淀共性功能，提高智慧城市 IT 建设的标准化、组件化水平，从而可以降低智慧城市建设过程中数据集中与处理、视频数据收集与处理、各种 IoT 设备的兼容与连接的复杂度，同时提供公共地理信息服务（GIS）、融合通信平台等公共服务产品和大数据分析、人工智能（AI）能力支撑。

数字平台面向智慧城市的关键业务场景，实现了城市大数据、物联网、视频云、GIS 和融合通信等多个业务能力的融合，向下兼容各种终端，向上支撑各种应用，在复杂的城市场景下，打破了原有“烟囱林立”、相互隔离的“信息孤岛”状态，支撑智慧城市实现真正的数字化、智能化。

2.1.7 智慧大脑实现智慧城市可视可管可控

智慧城市需要一个智慧大脑，基于数据采集、大数据分析和人工智能的结果，通过一个智能运营中心（IOC）可以让各类数据，如经济数据、人口数据、城市公共信息、实时视频信息、告警信息等集中呈现，实现城市数据和趋势的可视。在此基础上，通过融合通信系统、GIS 系统的支撑，可以实现对城市各种突发事件、各类告警的处理，实现快速、统一的应急响应和指挥调度。

2.2 智慧城市技术框架

根据智慧城市产业生态圈技术架构组的前期研究，智慧城市技术框架可以分为四个维度五个层面，即云（包括数字平台层和应用服务层）、管（网络连接层）、边（边缘计算层）、端（终端感知层）。

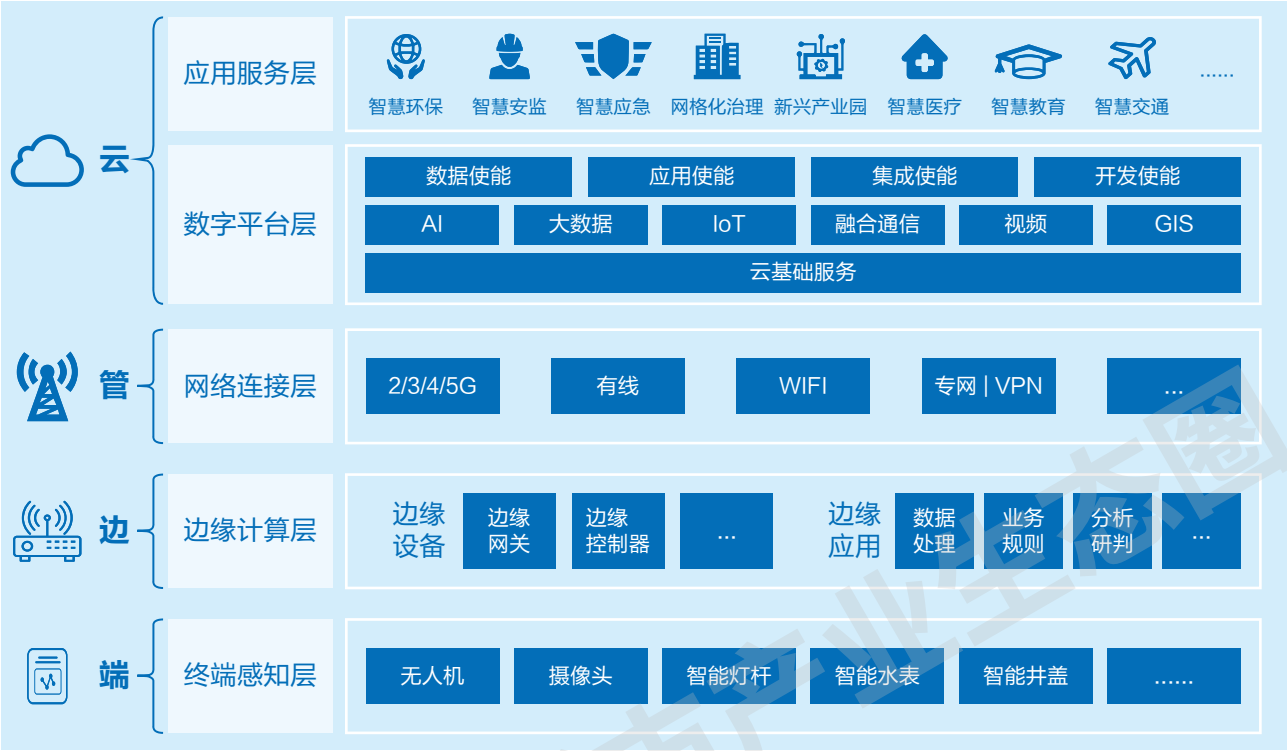

图 1 智慧城市技术框架

智慧城市技术框架中，各个层次的主要内容如下：

终端感知层：提供对物理环境的智能感知能力，通过感知设备及传感器网络实现对城市范围内基础设施、环境、安全等方面的识别、信息采集、监测和控制。

边缘计算层：在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的分布式开放能力，就近提供边缘智能服务，满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。

网络连接层：包括互联网、电信网、广播电视网以及三网之间的融合的公共网络，以及一些专用的网络（如：集群专网），为智慧城市提供大容量、高带宽、高可靠的光网络和全城覆盖的无线宽带网络所组成的网络通信基础设施。

数字平台层：聚合人工智能、云计算、大数据、地理信息、视频、指挥调度等多种资源，提供应用所需的数据和服务的融合服务，为构建上层各类智慧应用提供支撑。

应用服务层：在终端感知层、边缘计算层、网络连接层、数字平台层的基础之上建立的各种行业或领域的智慧应用集合，如智慧政务、智慧环保、智慧安监、智慧应急、智慧旅游等，为社会公众、企业用户、城市管理决策者等提供全面的信息化应用和服务。

3 智慧城市安全风险

3.1 主要安全风险

3.1.1 数据集中存储、边界模糊带来数据泄漏风险

智慧城市中涉及大量的城市公共数据及市民个人信息的共享使用。城市公共数据，比如地理信息、水文信息、房屋信息等。市民个人数据，例如大量市民户籍、医疗、社保、住房等各种个人隐私相关数据。

智慧城市运营中，会采集各个政府部门存储的一部分数据进行集中存储，在此基础上进行大数据分析和人工智能方面的运算，得出更有价值的结果进行存储和使用。这使得数据更加集中，数据聚集的价值更大，就更容易成为被攻击目标，数据被泄漏、窃密的风险也更大了。如果保护措施不到位，就有可能被外部恶意人员窃取，或者因工作人员无意疏忽而造成数据泄露。

另一方面，智慧城市场景覆盖区域大，对外连接多，需要与外界进行互联互通，如果防护和权限管理工作没有做到位，也会带来数据泄漏风险。

3.1.2 企业重要信息、个人隐私信息管理不严带来滥用风险

在智慧城市的运营中，除了城市公共信息和个人基本信息外，还会采集企业的信息，使用个人隐私数据，比如企业的经营数据、个人的人脸信息、行踪信息、车辆信息等，这些信息如果管理不严，被非授权的人滥用，将造成企业重要数据和个人隐私数据泄露，给企业带来损失，给个人的生活带来困扰，产生不良社会影响。

3.1.3 因关键信息基础设施失效带来服务不可用风险

随着城市信息化程度越来越高，各类应用越来越多，平台和系统越来越复杂。如果智慧城市关键信息基础设施因自身健壮性不够、高可靠性措施不到位，或者受外部入侵攻击等影响，可能会带来应用或服务的不可用。这将严重影响城市的管理和运行，带来负面的社会影响。

3.1.4 网络因被攻击或意外原因导致瘫痪风险

网络是智慧城市的“神经系统”。随着智慧城市应用越来越深入，网络触角也深入到城市的各个角落，这些网络将各政务办公点、对外服务点，以及各种物联网设备连接在一起，城市网络也会与各个外部的网络进行对接。如果网络遭受攻击，或因意外原因，如光纤被挖断等，可能造成网络瘫痪。

3.1.5 物联网设备被攻击风险

在智慧城市中，物联网设备众多，在将摄像头、路灯、红绿灯、各种仪表连接到互联网的同时，也建立了黑客反向攻击的通道，这些物联网设备理论上都有被攻击的风险。在电力、交通等关键基础设施中，其生产系统也会越来越多地使用智能设备，并与互联网直接或间接相连。这些设备的数据可能被非授权获取，或被非法篡改，也可能因攻击而失效或瘫痪。

3.2 各层面临的安全风险

总体安全风险与各层面临的安全风险是总与分、宏观与具体的关系。依据智慧城市技术架构，从各层的视角更具体地剖析智慧城市面临的安全风险。各层主要面临的风险如下表所示。

分层	主要安全风险
应用服务层	应用不可用风险 隐私泄露风险 网络欺诈风险
数字平台层	数据泄漏风险 平台被入侵风险
网络连接层	网络被攻击风险 网络失效不可用风险 无线网络被侵入风险
边缘计算层	设备被入侵风险 设备被攻击风险
终端感知层	终端设备被盗用风险 数据完整性被破坏风险 设备被仿冒风险 设备被干扰风险

表 1 各层面临的安全风险

3.2.1 终端感知层主要安全风险

· 终端设备被盗用风险

如果密码管理不善，使用弱密码或长期不修改密码，终端设备容易被非法访问。如摄像头被盗用，被非法获取视频信息。终端设备被获取使用权限后，也容易成为黑客攻击的跳板。

· 数据完整性被破坏风险

终端设备，如水质监测、空气质量监测的仪表，获取的是城市的各类基础信息，这对于准确了解城市运行状态很关键。如果这些设备的数据被篡改，或被破坏，将不能准确反映城市运行状态。

· 设备被仿冒风险

如有人仿冒合法身份在公共区域安装摄像头，非法获取数据。

· 设备被干扰风险

感知设备往往使用无线方式传输数据，恶意人员可能通过无线电波干扰感知设备的运行，导致不能正常工作或无法传输数据。

3.2.2 边缘计算层主要安全风险

· 设备被入侵风险

边缘计算层设备收集来自物联网设备的数据，并进行处理。如果设备因密码管理不善等原因被黑客入侵，将造成数据被非法获取，造成数据泄漏。

· 设备被攻击风险

边缘计算层设备可能会被攻击，导致设备失效，无法正常工作，使得底层设备收集的数据无法及时上传和处理。

3.2.3 网络连接层主要安全风险

· 网络被攻击风险

网络设备因存在漏洞、弱密码等问题被攻击或被控制，也可能被 DDoS 攻击，造成网络无法正常工作，甚至完全瘫痪。

· 网络失效不可用风险

除被攻击外，网络设备也可能因自身可靠性不够，以及一些意外原因如物理破坏造成失效而不可用。

· 无线网络被入侵风险

网络连接，往往采用无线连接方式，如物联网数据回传、Wi-Fi 网络覆盖等。由于无线网络的开放性，易被非法入侵，导致非法获取用户信息。

3.2.4 数字平台层主要安全风险

· 数据泄漏风险

数字平台层存储城市的各类数据，如城市运行信息、企业和居民信息等，以及大数据分析和人工智能运算的结果，数据机密性高。这些数据一旦泄露，将造成重大的社会影响。这些数据涉及面广，使用的人员多，也是黑客比较关注的点，容易造成数据泄漏。

· 平台被入侵风险

平台涉及网络设备、计算设备、存储设备，涉及各种对外接口，也涉及数据库等基础应用，容易被黑客入侵，造成设备无法正常工作。

3.2.5 应用服务层主要安全风险

· 应用不可用风险

智慧城市应用多，涉及到政务、医疗、交通、教育等多个方面，这些应用的用户涉及政府部门员工、企业及个人。

这些应用如果因自身健壮性原因或外来攻击导致不可用，将影响智慧城市正常运营，带来不良社会影响。

· 隐私泄露风险

应用服务层也会输入、存储和处理各种数据，如让用户输入各种信息，这些信息往往涉及到用户隐私，一旦泄露将造成恶劣影响。

· 网络欺诈风险

不法分子往往在网络上通过非法编制诈骗程序、发布虚假信息、篡改数据资料等违法手段，非法获取信息、实物或金钱。

3.3 风险应对分析

智慧城市建设覆盖区域广、涉及的人员多、对外连接多、系统种类多，因系统自身健壮性原因、意外原因或被恶意攻击，可能造成业务中断、应用不可访问、网络瘫痪等，造成业务不连续，因此系统、网络都应该具有较好的韧性，同时具备较好的防攻击措施。智慧城市存储和处理的数据多，既要考虑数据安全，还有考虑将政府数据对外共享，数据集中和大数据分析后数据泄漏风险加大，位于城市内的机场、银行、高铁等会与城市有信息的交互、应急指挥上的联动，这些都给保障数据的安全带来挑战。智慧城市系统中存储有企业、个人的大量信息，加强隐私保护，防止隐私数据被窃取或滥用非常必要。智慧城市建设中使用了大量的信息通信产品和方案,这些产品来自不同的厂家，这些产品的开发涉及到很多工程师，不同厂家之间的产品可能有集成关系，因此如何保障智慧城市方案中的整体生态安全及供应链安全，也是一个挑战。

面对这些风险和挑战，应该用体系化思维去思考安全问题，要主动防御、动态防御、整体防控、精准防护，应该进行统一规划、分步实施，不断改进和完善。要从国家网络安全法等法律、法规和标准中找要求、找依据、找方法，保证智慧城市网络安全建设是遵法的、合规的。网络安全建设和智慧城市建设要融为一体，两者同步规划、同步建设、同步使用，将安全内生于智慧城市之中，避免两张皮。通过识别关键资产和核心信息，做到重点防护。要采取适当的技术措施，部署必要的安全产品，并进行运维和管理。要加强智慧城市安全管理和安全运营工作，使智慧城市网络安全建设和管理常态化。

4 智慧城市安全建设原则和合规遵从

4.1 智慧城市安全建设原则

4.1.1 遵法合规原则

智慧城市的建设和运营，要遵守国家网络安全法以及相关的合规要求，将这些要求体现到智慧城市安全架构和安全方案中。随着信息技术广泛应用和网络空间兴起发展，极大促进了经济社会繁荣进步，同时也带来了新的安全风险和挑战。世界多国都高度重视网络空间战略，以维护各自国家在网络空间的主权、安全、发展利益。我国也高度重视网络空间安全，出台了大量的法律法规及政策指导。作为智慧城市建设的各参与方，都应遵守相关的法律法规。

4.1.2 安全为业务服务原则

安全工作应该以智慧城市自身业务为中心，围绕业务展开，为业务服务。保护业务是所有信息安全方案的首要目标，智慧城市的安全负责人应当将安全方案与整体业务目标紧密联系起来，清楚了解安全可以为业务发展作出的贡献，将先进的安全技术和管理与智慧城市的运营相结合起来。这将有助城市集中精力，有效管控风险环境，战略性地保障智慧城市业务的健康运营。不能不重视安全，也不要将安全置于智慧城市业务发展之上。安全是相对的，不是绝对的，不必不计代价求安全。需要从风险管理的角度出发，考量城市所面临的信息安全风险发生时可能带来的后果和损失，风险发生的可能性，考虑安全、效率与成本之间的平衡，制定出适合各个智慧城市自身的安全策略。

4.1.3 安全内生原则

网络安全建设和智慧城市建设是一体的，要把安全内生于智慧城市中，不能把二者割裂开来，甚至对立起来。没有网络安全保障，就没有智慧城市建设的成功。智慧城市建设中的应用、设备都应该具备安全特性和安全机制，而不能仅依赖外部安全防护。各业务部门、信息化部门都要思考、参与、推动网络安全建设，而不能仅仅依赖于一个网络安全部门。应当把安全融入智慧城市的规划设计、建设实施、运营运维等全流程中。

4.1.4 体系化建设原则

网络安全只有作为一个体系，才能充分起到防护作用。在安全领域，木桶原理的短板效应明显，在某一个点的疏忽，就有可能造成整个系统被入侵。因此在进行智慧城市安全建设时，要有体系化思维，通盘考虑，统一规划，技术与管理并重，使得各种措施的考量比较完备而均衡，避免出现短板和缺失。尤其需要将智慧城市的安全作为一个整体来考虑，全天候全方位感知整体网络安全态势。加强网络安全检查，摸清家底，认清风险，找出漏洞，通过网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。

4.1.5 重点防护原则

智慧城市建设涉及面广，涵盖的数据多、应用多，但是防护力量和资源是有限的，不可能同时做到全面等同防御。应该开展关键信息、关键资产识别，通过风险分析，识别出重点信息、重点区域、重点人员，建立纵深分级的防御体系，对重点防护对象开展重点防护。特别是针对识别为关键信息基础设施的网络设施和业务系统，这类设施与系统一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，更应加强重点防护。

4.2 智慧城市安全建设相关的法律法规和标准

4.2.1 网络安全法

《中华人民共和国网络安全法》于 2017 年 6 月 1 日起正式实施，是我国实施网络空间管辖的第一部法律，属于国家基本法律，是网络安全法制体系的重要基础。《中华人民共和国网络安全法》以网络的运行安全为主，然后兼顾个人信息保护、网络信息内容管理，以及如何推动、促进网络安全产业发展，并明确提出了对应的法律责任。智慧城市建设的众多参与方，在智慧城市建设过程中应严格遵照《中华人民共和国网络安全法》要求，依法开展智慧城市建设工作。

4.2.2 密码法

《中华人民共和国密码法》于 2019 年 10 月通过人大表决，2020 年 1 月 1 日起施行。作为密码领域的综合性、基础性法律，密码法明确了三个原则：一是明确对核心密码、普通密码与商用密码实行分类管理的原则。二是把握职能转变和“放管服”需要与保障国家安全的平衡。三是处理好密

码法与网络安全法、保守国家秘密法等有关法律的关系。

密码法明确将密码分为核心密码、普通密码和商用密码，并对密码进行分类管理。核心密码、普通密码属于国家秘密，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。商用密码用于保护不属于国家秘密的信息。并提出了商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接。开展智慧城市建设时，应当分析所系统中信息的保密级别，对于不属于国家秘密的信息使用商用密码进行保护，依照密码相关规定使用密码进行保护，同步规划、同步建设、同步运行密码保障系统。

4.2.3 等级保护 2.0

“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务。”这是《中华人民共和国网络安全法》中第二十一条对等级保护制度有明确的法律要求。

《网络安全等级保护条例（征求意见稿）》于在2018 年 6 月公开征求意见，在该条例中，第六条明确规定了网络运营者应当依法开展网络定级备案、安全建设整改、等级测评和自查等工作，采取管理和技术措施，保障网络基础设施安全、网络运行安全、数据安全和信息安全，有效应对网络安全事件，防范网络违法犯罪活动。第七条中明确规定行业主管部门应当组织、指导本行业、本领域落实网络安全等级保护制度。在 2017 年 6 月 1 日《网络安全法》正式实施以后，已发生多起政府部门或企业由于未开展等级保护工作而被政府监管部门处罚的案例。

2019 年 5 月 10 日，等保 2.0 系列重要标准：GB/T 22239-2019《信息安全技术 信息系统安全等级保护基本要求》、GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》、GB/T 25070-2019《信息安全技术网络安全等级保护安全设计技术要求》正式发布。等级保护标准从 1.0 正式升级为 2.0，等保 2.0 从标准结构、防护理念、防护范围等角度与等保 1.0 都有了较大改动。

对于智慧城市的建设者来说，应按照等级保护制度，在规划设计阶段就应确定网络的安全保护等级。对拟定为第二级以上的网络，其应当组织专家评审；并在评审后报请主管部门核准。第二级以上网络运营者应当在网络的安全保护等级确定后 10 个工作日内，到县级以上公安机关备案。新建的第二级网络上线运行前应当按照网络安全等级保护有关标准规范，对网络的安全性进行测试。新建的第三级以上网络上线运行前应当委托网络安全等级测评机构按照网络安全等级保护有关标准规范进行等级测评，通过等级测评后方可投入运行。

4.2.4 关键信息基础设施安全保护

在《中华人民共和国网络安全法》第三十一条至第三十九条明确定义了关键信息基础设施运行安全的明确要求。《关键信息基础设施安全保护条例（征求意见稿）》也于 2017 年 7 月正式对外公开征求意见，第五条明确规定了关键信息基础设施的运营者（以下称运营者）对本单位关键信息基础设施安全负主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。

智慧城市建设主管部门按照关键信息基础设施识别指南，组织识别智慧城市中的关键信息基础设施，并按程序报送识别结果。关键信息基础设施识别认定过程中，应当充分发挥有关专家作用，提高关键信息基础设施识别认定的准确性、合理性和科学性。

此外，网信办于 2019 年发布了《网络安全审查办法（征求意见稿）》，其中明确提出“关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。”对于智慧城市中的关键信息基础设施，应采购通过网络安全审查的产品和服务。

目前，关键信息基础设施的相关标准和配套政策正在制定中，如正式发布后智慧城市运营者应及时关注并识别自己运营的信息基础设施是否属于国家关键信息基础设施范围内。如果属于，应遵照相关的标准、政策执行相应的保护措施。

4.2.5 云计算服务安全评估

为提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部于 2019 年 7 月联合发布《云计算服务安全评估办法》，自 2019 年 9 月 1 日起施行。云服务商可申请对面向党政机关、关键信息基础设施提供云计算服务的云平台进行安全评估，云计算服务安全评估工作协调机制办公室受理云服务商申请后，组织专业技术机构参照国家有关标准对云平台进行安全评价，并发布云计算服务安全评估结果。评估结果可作为党政机关、关键信息基础设施运营者采购云计算服务提供参考。云计算服务安全评估参照《云计算服务安全指南》《云计算服务安全能力要求》等国家标准，重点评估内容包括云平台技术、产品和服务供应链安全情况等。

在智慧城市的建设运营中，云计算服务是重要组成部分。智慧城市的建设运营者应考虑识别所建设运营的智慧

城市业务是否属于党政机关、关键信息基础设施范围，在采购云计算服务时重点参考云计算服务安全评估工作协调机制办公室提供的云计算服务安全评估结果。

4.2.6 数据安全管理

中央网信办于 2019 年 5 月发布《数据安全管理办法（征求意见稿）》对全社会公开征求意见。该管理办法以个人信息和重要数据为主要管理对象，针对在中国境内利用网络开展数据收集、存储、传输、处理、使用等数据活动，以及数据安全的保护和监督管理做出规定。该管理办法体现政府对数据安全的重视。

在该管理办法中，明确规定“重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等”。在智慧城市的建设场景中，有可能会涉及大量政府部门数据，应认真评估是否属于重要数据范畴，若属于，应遵照该管理办法。

另外，在该办法第二十八条中明确提出，“网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。”作为智慧城市的运营者，在识别重要数据后，将其发布、共享、交易或者向境外提供时应报送主管部门审批同意。

4.2.7 个人隐私保护

我国尚未出台单独的个人信息保护法律，但是近年来逐步加强公民个人信息保护方面的顶层立法工作，陆续在《网络安全法》、《刑法》和《民法》等基本法中加入个人信息保护的内容，不断完善个人信息保护法律体系。

《网络安全法》第四十条至第四十五条，对个人信息保护做出有关规定，明确了我国个人信息保护的基本原则和框架。第四十条是对网络运营者保护用户信息义务的原则规定，要求网络运营者对其收集的用户信息严格保密，建立健全用户信息保护制度。第四十一条对网络运营者收集、使用个人信息应遵守的规则进行了规定，这些规定与国际通行规则是一致的。第四十二条是关于个人信息安全原则、个人信息匿名化处理和个人信息泄露报告义务的规定，首次明确提出建立数据泄露通知报告机制。第四十三条是关于个人信息删除权和更正权的规定，信息主体在具备法定理由的情形下，拥有请求删除其个人信息的权利；在个人信息不完整或不准确时，拥有要求及时改正、补充的权利。第四十四条是关于禁止非法获取、非法出售、非法提供个人信息的规定。第四十五条是关于负有网络安全监督管理职责的部门及其工作人员的保密义务的规定。

《刑法修正案（七）》是我国第一次将个人信息保护写入刑法，规定了国家机关与金融、电信等领域工作人员出售或非法提供个人信息的法律后果。2015 年的《刑法修正案（九）》，将“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”整合为“侵犯公民个人信息罪”。从三个方面完善了对公民个人信息保护的规定：一是扩大犯罪主体的范围，规定任何单位、组织、个人违反有关规定，出售或向他人提供公民个人信息，情节严重的，都将构成犯罪；二是严打“内部人”犯罪，明确规定任何单位、组织、个人违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，从重处罚；三是提高量刑标准，规定侵犯公民信息罪情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。为了保障法律正确、统一适用，2017 年最高人民法院会同最高人民检察院联合发布《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（《刑九解释》）。《刑九解释》在《刑法修正案（九）》基础上列出了十三条具体的司法解释，明确了“公民个人信息的范围”包括身份识别信息和活动情况信息，细化了非法获取、提供公民个人信息的认定标准，对侵犯公民个人信息犯罪的定罪量刑标准和有关法律适用问题作了全面、系统的规定。

2017 年发布的《民法总则》规定自然人的个人信息受法律保护，任何组织和个人需要获取他人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。个人信息权被纳入《民法总则》具有重大意义，表明个人信息权利拥有了基本民事权利的地位。今后除了严重侵犯公民人身权利、财产权利的重大违法犯罪行为应当依照《刑法》承担刑事责任（可以附带提起民事诉讼）外，对于一般的侵害个人信息权的侵权行为，任何自然人或组织均可以从侵权法的角度进行维权，以个人信息权被侵犯为由提起民事诉讼。

《信息安全技术 个人信息安全规范》（GB/T 35273—2017）于 2018 年 5 月 1 日起正式实施，该标准将《网络安全法》中的个人信息保护原则性规定从技术和管理角度进行了落地，该标准规定了个人信息安全基本原则，个人信息收集、保存、使用和处理等流转环节以及个人信息安全事件处置和组织管理要求等。

《儿童个人信息网络保护规定》由国家网信办正式发布，自 2019 年 10 月 1 日起施行。该规定要求应设置儿童专门用户协议、设置专人负责、征得儿童监护人明确同意、

加密存储和最小授权访问等儿童个人信息保护要求，相较于 14 周岁以上的未成年人和成年人，其各项要求均更加严格。

在智慧城市的建设过程中不可避免的会涉及市民的大量个人隐私信息，对此应严格识别个人隐私信息，并遵照相关法律法规、标准采取技术和管理手段进行保护。

4.2.8 智慧城市建设产业政策

在国家主管部门出台产业政策引导智慧城市建设的过程中，一直把安全放在重要位置。

2014 年八部委联合发布的《关于印发促进智慧城市健康发展的指导意见的通知》中，提出了“可管可控、确保安全”的原则，并提出了网络安全长效化的目标，达到城市网络安全保障体系和管理制度基本建立，基础网络和要害信息系统安全可控，重要信息资源安全得到切实保障，居民、企业和政府的信息得到有效保护。

2015 年，有网信办、公安部、发改委、工信部四部委针对智慧城市安全问题，专门印发《关于加强智慧城市网络安全管理工作的若干意见》。该意见中突出强调加强智慧城市网络安全的顶层设计和统筹协调，坚持信息系统建设与网络安全建设“同步规划、同步设计、同步实施”的三同步原则，实现网络安全与智慧城市建设的深度融合。并要解决云计算、大数据、物联网、移动互联网、智能位置服务等新技术新应用带来的网络安全风险与隐患，有效提高抵御和防范风险能力。

国家发改委分别于 2016 年、2018 年发布《关于组织开展新型智慧城市评价工作务实推动新型智慧城市健康快速发展的通知》和《关于继续开展新型智慧城市建设评价工作深入推动新型智慧城市健康快速发展的通知》，在智慧城市的总体评价指标中加入了网络安全方面考核评价内容，通过对智慧城市的网络安全组织机制、预警与通报机制、系统与数据安全等的评价，以提升智慧城市的安全防护水平。

4.2.9 智慧城市安全标准规范

作为对智慧城市安全产业政策的支撑，全国信息安全标准化技术委员会（TC260）也制定了一些相关国家推荐标准供参考。

《信息安全技术 智慧城市安全体系框架》（GB/T 37971-2019）给出了智慧城市安全体系框架，提出了智慧城市的安全保护对象、安全要素、安全角色及其相互关系。该标准是智慧城市安全方面的顶层设计标准，包括智慧城市安全体系框架、智慧城市安全战略、智慧城市安全管理、智慧城市安全技术、智慧城市安全建设与运营、智慧城市安全基础支撑等主要内容。

《信息安全技术 智慧城市建设信息安全保障指南》（报批阶段）以智慧城市建设安全需求为导向，围绕智慧城市所面临和需要应对的安全问题总结安全需求和安全角色，提炼出智慧城市安全保障机制和管理、技术要求。该标准明确了智慧城市建设全过程的信息安全保障规范，在基于已有信息安全标准规范的基础上，针对智慧城市建设中的新技术新应用，提出智慧城市建设信息安全保障管理和技术指南。

对于智慧城市中涉及的专业技术领域，如云计算、大数据、物联网、移动互联网等方面的安全，均有相对应的国家标准、行业标准可供参考。

5 智慧城市安全架构

基于第 2.2 节智慧城市技术架构，第 3 章对安全风险的分析，以及第 4 章的安全合规要求，提出如下智慧城市安全架构。

图 2 智慧城市安全架构

基于智慧城市分层技术架构，在终端感知层、边缘计算层、网络连接层、数字平台层、应用服务层逐层分析对应安全技术，并叠加贯穿各层的安全管理、安全运营，构成了智慧城市安全架构。

· 智慧城市安全技术

智慧城市安全技术架构主要从技术层面采取各种安全措施以降低来自各个层次的安全风险，从身份管理、防泄漏、防入侵、可用性、防抵赖等多个维度展开。

· 智慧城市安全管理

智慧城市安全管理是贯穿于组织内部全流程的管理过程，主要从安全管理组织、制度、人员管理、建设流程、供应链安全、应急演练与响应、安全测评等管理角度展开。

· 智慧城市安全运营

智慧城市的安全运营通过安全运营中心、安全防护手段和专业的安全运营团队，体系化地运用安全技术、安全运维和安全管理手段持续保障城市长期安全运营。

6 智慧城市主要安全技术措施

6.1 安全技术措施分类

智慧城市所涉及的安全技术措施，参考《信息安全技术 智慧城市建设信息安全保障指南》（报批阶段）中提到的智慧城市安全需求：“智慧城市建设信息安全保障应实现攻击者进不去，非授权者重要信息拿不到，窃取保密信息看不懂，系统和信息篡改不了，系统工作瘫不成，攻击行为赖不掉”。按照安全防护目的，可分为以下几种类型：

分类	定义及说明
身份管理	对智慧城市中的人员，包括使用智慧城市应用系统的用户、IT 系统和设备的管理员等进行身份鉴别，对设备进行接入认证，保证只有身份合法、具有权限的人员才能进行访问和管理，只有合法的设备才能接入智慧城市系统。
防泄漏	防止智慧城市系统中的数据、敏感信息、个人隐私信息等被恶意窃取、恶意滥用或无意泄漏。
防入侵	防范各类入侵、攻击对智慧城市系统的威胁，避免信息或文件被恶意篡改、数据被窃取、IT 基础设施瘫痪而不可用。
可用性	采取必要的安全措施，保证智慧城市系统能够持续对外提供服务，保障业务连续性。
防抵赖	通过数据溯源、数字签名、安全审计、攻击溯源等手段，提供足够证据，保证系统的使用者或入侵者不能否认他们的行为。

表 2 安全技术措施分类表

6.2 身份管理措施

6.2.1 身份鉴别

应对各种人员的身份进行鉴别，包括应用使用人员、数据访问人员、各类管理人员、IT 运维人员等，确保只有被授权的人才能进行操作或访问。对于重要系统和数据库的访问，应考虑采用多因素认证手段。

身份管理系统定义和管理了每个用户的身份角色及其所需资源的访问权限，并根据用户身份角色生命周期，对其所需资源访问权限进行动态管理，实现统一身份管理、统一身份认证、统一访问控制和权限合规管理等功能。在智慧城市建设中，可以集中部署身份管理与访问控制系统，既可以使身份认证和管理工作统一、高效，也可以提升用户体验，实现“一个身份、全网通行”。

对于身份鉴别可以包括但不限于以下功能：

1) 确保用户身份整个全生命周期内用户标识的唯一性。

2) 对应用层建立统一身份管理体系，实现用户身份全生命周期闭环管理，统一身份数据贯穿整个应用域，确保身份体系协同一致，彻底杜绝孤儿账号、僵尸账号、私建账号等安全风险。

3) 满足不同维度的身份管理体系集中统一管理，并建立相对应身份管理规范，包括但不限于政府单位、管辖企业、合作单位、供应商、承建商、公众、法人等，针对不同的用户体系提供完整账号有效期管理机制。

4) 建立敏捷的身份生命周期管理机制，满足对内部、外部等不同身份的管理，并提供对多种用户库的支持，提供企业级目录服务，提供各机构之间用户身份数据隔离机制，保障不同的机构之间的数据互不可见。

5) 支持用户身份鉴权信息进行实名制等级划分，并对用户提供完整的自助实名认证等级服务，用户可自助完善实名认证等级（如绑定手机号、注册人脸信息、绑定企业信息等），并根据实名制等级开通相应系统的访问权限。

6) 打通线下与线上（云端）用户体系，实现一套身份体系即可安全访问线下及线上应用。

7) 可对应用系统的进行风险安全级别的划分，可根据不同安全级别配置不同的身份鉴别方式。

8) 基于融合认证框架，对应用进行认证赋能；基于策略进行认证链组合，增强认证安全系数，提高安全级别；提供包括账号密码、数字证书、手势、指纹、人脸、声纹等具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别。

6.2.2 权限管理

应对应用的访问权限进行限定，进行权限分类、分级，按业务相关性、最小授权原则配置权限，只有得到授权的用户才能登录或访问。

对于权限管理可以包括但不限于以下功能：

1) 对于用户权限可进行分类、分层、分级管理，可按部门、岗位、职责等维度自动设置权限；根据最小权限原则为用户分配权限，确保用户仅能访问被授权的信息。

2) 对用户访问行为进行自动收集与识别，对威胁进行分析；根据统一访问控制策略，实时对不同风险级别采用对应的加强认证方式与阻断措施。

3) 可查看所有用户的访问会话状态以及登陆设备，管理员可注销有风险告警用户的会话，支持对单个账户的多重并发会话进行限制。

4) 可设置权限合规及权限互斥策略，保障用户权限设置遵从相应规范。

5) 基于风险的访问控制机制，对用户访问控制进行风险计算，对用户访问元数据（时间、位置、习惯、账号、关系、行为等）进行控制，并基于该计算模型主动收集用户行为相关数据进行建模。

6) 建立基于角色的访问控制模型和基于属性的访问控制模型相结合的方式，通过对等组分析、权限合规分析等模型，持续对权限策略进行优化和风险评估，并触发工作流引擎对策略进行调整，形成身份和权限的智能闭环管理。

7) 应针对用户身份及权限进行全面风险评估管理，通过风险评估和分析，对角色和权限进行过滤，实现访问控制场景和风险感知的动态授权。

8) 入职 / 离职 / 调岗等，应用账号自动创建回收，工作状态切换时，应修改应用系统权限，使用户密码策略和有效期等统一管理。

6.2.3 口令管理

口令是在多种应用及产品中常用的身份鉴别手段之一，但是由于口令的使用不当，往往成为黑客攻击的一个突破口，因此应当加强对口令的管理。

对于口令管理可以包括但不限于以下功能：

1) 应对各类设备、数据库、应用的口令进行有效管理，避免使用弱口令，应定期更换密码。

2) 口令存储应进行加密。如使用非电子方式存放口令，应放置于安全的环境中，如放置于保密柜内。

3) 相关的产品应支持口令管理的相关策略，如口令的复杂度策略、多次尝试失败锁定、验证码机制、多因素认证机制等。

4) 针对用户及应用提供统一密码服务，支持可视化密码策略配置界面，包括不限于密码加密存储方式、密码生存周期、密码长度限制、密码组成规则、弱密码字典定义等。

5) 应支持密码修改、密码重置、密码找回等操作，从而将各类密码操作进行统一管控，对外提供服务。

6) 支持用户首次登录，应强制修改初始密码，同时支持定期强制修改密码策略。

7) 具有登录失败处理功能，包括多次登录失败锁定账户、登录连接超时自动退出、主动退出一键注销会话等功能。

6.2.4 设备接入认证

智慧城市的各类应用场景中将会有大量设备接入，应对接入智慧城市系统中的各类设备进行接入认证，包括物联网设备、网络设备等，保证设备是合法的、可信的，确保只有合法设备可以接入到系统中，避免设备被仿冒，造成未授权设备也混入系统中，非法接收和发送信息。

6.2.5 远程访问管理

对于远程接入智慧城市网络进行办公或访问的人员，应通过远程接入设备，如 VPN 设备，进行受控接入，并对接入的传输过程进行加密。对于运维人员的远程接入，应使用运维审计堡垒机作为运维的唯一入口，主机连接都必须经过堡垒机的统一身份管理，并基于 IP 地址、账号、命令进行控制，防止越权操作，整个操作过程支持实现全程的审计记录。

6.3 防泄漏措施

6.3.1 数据分级

数据的分级是数据能被广泛应用的基础。如果没有明确数据的安全分级，就无法对数据进行分级别的权限控制，容易造成数据使用管理的“一刀切”现象。“一刀切”的都开放，容易造成数据泄露，数据所有权不清晰等安全问题。“一刀切”的不开放，则容易造成数据的固化，无法充分发挥数据的价值，阻碍业务的发展。

数据的安全分级是一个安全和管理需要配合使用的问题，以数据的价值、内容敏感程度、影响和分发范围进行安全级别划分。对于数据划分几个安全级别，对于每个级别数据设计什么样的访问权限，属于管理机制问题，是要做数据化转型规划的时候应优先考虑的问题。而数据分级如何在数据平台中实现，权限访问控制如何实现则属于技术问题。权限控制可以采用基于角色的访问控制，对于数据访问者划分不同的角色，给予不同角色不同安全级别的访问权限。

在《数据安全管理办法（征求意见稿）》中，明确了重要数据的定义，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。除了重要数据以为，智慧城市中还包括非重要数据但不适合公开的数据、公开信息、个人信息、内部管理信息等多种形式的数据。在实际的应用过程中，这个安全分级可能还太粗粒度，无法很好的满足细粒度的权限访问控制要求，因此还需要根据实际情况，进一步根据智慧城市实际应用场景细化数据安全分级。

6.3.2 数据加密

对于智慧城市涉及的重要信息及敏感信息，应进行加密处理，加密后进行存储和传输。对数据的加密有多种不同层次，比如存储设备的加密、传输通道的加密、应用层对数据的加密，应根据实际场景分析需要在其中某个或多个层次进行加密。数据加密需严格按照城市数据分级分类标准规范，对相关数据进行加密 / 解密管理，防止重要数据被泄露。对于数据加密使用的密码算法和密码保障措施，应符合国家的密码管理相关制度和规定。

对于数据加密可以包括但不限于以下功能：

1) 对存储在数据库中的数据进行精细到列级的加密 / 解密处理；

2) 对服务器中的文件、图片、视频等数据进行加密 / 解密处理；

4) 实现加密数据的完整性保护，防止对密文的篡改，校验出密文的合法性；

5) 数据平台通过采用密钥管理系统以及加密机实现数据存储加密的功能，保障数据的机密性、完整性。

6.3.3 数据销毁

数据销毁，是指用户敏感数据（系统管理数据、用户鉴权数据、重要业务数据等敏感数据）所使用存储空间在被重新分配给其他用户使用前要被彻底擦除，使得信息被彻底销毁，不可恢复，以确保用户信息安全性。

数据销毁一般可在存储设备中得到全面实现。让使用者无需担心自己的敏感数据信息会因存储资源的重分配而遭泄漏。存储设备可将存储空间划分成多个小粒度的数据块，基于数据块来构建组，使得数据均匀地分布到存储的所有硬盘上，然后以数据块为单元来进行资源管理，大小范围是动态可调。数据删除时，系统进行资源回收时，小数据块链表将被释放。存储资源重新利用时，再重新组织小数据块，保证数据的销毁。

对于保密性要求更高的数据，可采用更加彻底的数据销毁方式，比如对存储空间的多次重写覆盖，存储介质的物理粉碎等方式。

6.3.4 数据脱敏

数据脱敏是数据利用处理前的关键一步准备工作，不仅要确保敏感信息被去除，还需要尽可能的平衡脱敏所花费的代价、使用方的业务需求等多个因素。确保数据脱敏的过程、代价可控，得到的结果正确且满足业务需要。

智慧城市主管部门应制定敏感信息规则，可从个人隐私数据、城市业务运营重要数据等方面，根据敏感数据的重要性程度明确对哪些数据需要脱敏处理。然后根据原始数据的特点和应用场景，选择合适的脱敏方法。常见的数据脱敏方法有：泛化、抑制、扰乱、假名化、随机、统计、合成等。由于脱敏后的数据需要在相关业务系统、测试系统等非原始环境中继续使用，因此需保证脱敏后的数据仍能真实体现原始数据的特征，且应尽可能多的保留原始数据中的有意义信息（比如原数据格式、原数据类型等），以减小对使用该数据的系统的影响。

对于数据脱敏可以包括但不限于以下功能：

1) 支持对所需脱敏的目标数据库系统的配置，包括目标数据库的用户名、口令、端口、IP 地址等。

2) 支持对脱敏系统的脱敏策略的配置，需完成基础策略配置管理（设置基础脱敏策略，包括对数字、字母、中文、身份证号、银行卡号、通讯地址、家庭住址、电话号码、网址、邮编等进行缺省脱敏策略设置）和用户定制化策略配置管理（设置自定义脱敏策略，读取目标数据库中的某些数据库字段属性进行提取和判断，并提供相应的策略配置界面进行个性化的修改）。

3) 支持基于用户身份进行脱敏权限控制。即针对不同用户身份按照不同的脱敏策略进行数据处理。

4) 支持脱敏审计，对系统全生命周期内的操作过程进行审计追踪，以快速发现违规操作和快速定位相应的攻击行为。

5) 在执行数据脱敏过程时，应规划制定数据脱敏工作具体流程，脱敏工作应结合具体的业务场景及工作流程开展，比如数据脱敏申请、申请审批、数据下发、脱敏数据使用等工作的流程化。

6) 数据应尽量在数据源环境（例如生产环境、备份库等）进行脱敏处理后，再将脱敏后数据传输到新环境（测试环境、其它业务系统环境）进行进一步使用。

6.3.5 API 安全

在智慧城市的业务系统中存在的各种 API 直接的互相调用访问，应防止被攻击或被非授权地访问。

对于 API 安全可以包括但不限于以下功能：

1) 在调用 API 时提供认证机制对接入开放 API 的用户进行身份标识和鉴别，并对访问权限进行管理。

2) 对于 API 的访问尽量使用基于安全协议的访问，如 HTTPS、SSL/TLS、SFTP 等安全协议；

3) 对 API 访问采用速率限制并设置访问配额；

4) 对 API 调用使用输入和输出校验组件，对接口不安全输入参数进行限制或过滤能力，为接口提供异常处理能力，防止注入攻击。

5) 对于上线后运行的 API，应对 API 接口的调用行为进行监控，并对数据异常情况进行告警（例如，调用 API 接口的数量突然异常增加），发现问题及时告警，并快速处置。

6) 对 API 的调用访问都有日志记录，能提供日志可供事后进行审计。

6.3.6 边界防护

应对内外网边界、不同等级的安全域之间的边界进行隔离和防护，特别是智慧城市系统与外部进行网络连接、互联网访问、数据交换的边界，避免内部网络、高等级的安全域受到攻击。同时，在各个边界之间进行的数据交换行为，也应该满足业务要求，简单而高效。当智慧城市业务部署在政务外网时，应根据业务特点考虑部署在政务外网的合适网络区域，某项业务的不同模块有可能需要同时部署在政务外网的互联网区、部门业务区和公共业务区。应符合政务外网对各个区域之间的网络隔离与接入要求。

6.4 防入侵措施

6.4.1 入侵防范

入侵攻击可能针对每个层面，因此防攻击也要考虑各个层面。总体上，应建立一个纵深防御体系，而不是仅依赖几个孤立的产品。在网络连接层，应考虑防范 DDoS 攻击。在终端感知层和边缘计算层，应重点考虑针对工业控制系统、生产系统的攻击。在数字平台层，应重点考虑对云平台的攻击防范。在应用服务层，应重点考虑对 Web 网站的防护。系统中应部署入侵防御系统等安全设备，检测并防御外来入侵、攻击行为。

应在物联网设备、边缘计算设备、网络设备及云端系统采取必要的安全措施，如最小化安装、关闭不必要端口、升级补丁等措施，提高自身的防入侵能力。

6.4.2 完整性检查

应对应用系统及物联网设备进行完整性检查，避免系统或设备遭到入侵。如对外服务的网站，应避免被黑客注入木马或恶意代码。重要数据或视频信息，应采取技术手段，避免被恶意篡改。

6.4.3 恶意代码防范

恶意代码是对网络空间中各种病毒的广义称呼，包括普通病毒、木马等。恶意代码是以设备、应用系统、数据库为感染对象，以移动网络和计算机网络为平台，通过有线或无线通信等方式，进行攻击，从而造成网络异常的各种不良代码。应防范病毒、木马等恶意代码，避免其对应用系统、数据库等造成破坏。可在网络上通过异常流量检测、病毒特征分析等方式进行恶意代码防范，也可通过主机端安装杀病毒软件的方式进行恶意代码防范。

6.4.4 源码安全检测

智慧城市系统中，往往有安全能力参差不齐的多家厂商的应用系统，源代码检测对安全能力要求比较高，一般仅对于重要系统，在系统上线前应对其源码进行安全检测，避免这些应用系统存在严重的安全漏洞。

6.4.5 数据库防护

数据库系统作为数据的主要承载体，是最具有战略性的资产，数据库系统的安全稳定运行直接决定着一个单位业务系统能否正常使用，因此数据库安全尤为重要。数据库的安全威胁主要有两个方面 黑客入侵和内部数据泄露。应做到可以实时监控数据库的所有操作，及时发现数据库的恶意破坏、误操作等。协助用户在第一时间发现可疑行为，及时整改，有效保护数据库的安全性和可用性。同时，有效发现数据库的账号权限滥用，发现网络系统中存在撞库、拖库等行为，实时上报告警，防护数据库安全。提供基于角色的审计，能够有效区分不同等级的维护人员，便于事后追查原因与界定责任。

6.5 可用性措施

6.5.1 物理环境安全

智慧城市覆盖区域广，包括各种物理边界、卡口、园区等。应对重要的场所和物理环境，采取物理访问控制措施，如采用门禁系统、视频监控、人脸识别、车牌识别、黑白名单管理等。如非法人员进入到非授权的区域，可以及时发现并制止。各类终端设备，如摄像头、物联网设备等，应采取措施，防止被恶意毁坏或干扰。

6.5.2 终端隔离

随着物联网、云计算技术的快速发展，各类物联网终端或云终端数量激增，当一些终端受到攻击或被劫持时，可以主动发现并上报异常终端，告警至管理员进行操作，严重情况下可以将其自动隔离至安全区或进行断网处理，避免影响其它终端运行而造成大面积瘫痪，从而提升终端排障速率，降低终端运维成本，为海量终端提供安全保障。

6.5.3 网络隔离

应根据不同的安全需求和安全级别对网络进行划分，成为不同的安全域，并通过配置网络设备，使得不同的子

网络之间进行逻辑隔离。必要时，需采取物理隔离措施。网络隔离技术的目标是确保隔离有害的攻击，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成不同网络之间数据的安全交换。

6.5.4 网络冗余

网络层应采用网络冗余措施，如双链路、网络设备冗余、接口板冗余等措施，加强网络的可靠性。如果网络中的主链接产生断线等问题，那么网络中的数据会通过备链接进行传递，保证网络的通讯正常。

6.5.5 机房安全

应对机房采取防火、防水、防静电、防雷击等安全措施，保障电力供应的连续性。机房内部的设计应根据数据的不同保密级别，进行合理分区。机房出入口应有物理访问控制手段。

6.5.6 资源隔离

应对系统中的计算、存储和网络资源进行物理隔离或逻辑隔离，使得当一些资源失效或受到入侵而不可用时，其它资源不受影响，仍能对外提供服务。这对于云计算平台、大数据平台等共享模式特别重要，平台上往往包含各业务相关的组件，共享、抢占系统资源，任一组件问题都有可能影响其他组件服务。应做好资源隔离，使得部分资源的受损，不会扩散到其它资源，而影响整体业务运作。

6.5.7 应用容灾

为提高应用系统的可用性，对安全级别高的关键系统应采取应用容灾措施。在本地数据中心或异地备份中心建立一套完整的与本地生产系统一致的备份应用系统，互相之间可以进行健康状态监视和功能切换。在本地生产系统出现灾难时，备份中心可以立即接管本地生产系统的业务，保障了业务的连续性。并在本地生产系统正常使用后，恢复完整的数据，并保证恢复数据可用。这样可以保证关键应用在允许的时间范围内恢复运行，尽可能减少灾难带来的损失，让用户基本感受不到灾难的发生，使系统所提供的服务是完整的、可靠的和安全的。

6.5.8 垃圾邮件防范

垃圾邮件不仅占用大量系统资源，影响网络传输、运算速度和正常的邮件服务，还需要用户浪费时间来处理，浪费了大量人力物力，同时垃圾邮件可能携带病毒、木马或者其他恶意程序，引发安全事件，近年来，病毒邮件越来越具有欺骗性，对于普通用户来说，很难做出正确的判断。对于提供的邮件服务，应部署防垃圾邮件措施。

6.5.9 数据备份

为防止系统出现操作失误或系统故障导致数据丢失，将全部或部分数据集合从应用主机的硬盘或阵列复制到备份存储介质中。传统采用内置或外置的磁带机进行冷备份。随着技术的不断发展和安全要求的提供，数据的海量增加，异地备份中心的远程备份措施被广泛采用。远程备份一般需要通过专业的数据存储管理软件结合相应的硬件和存储设备来实现。对于所有数据，应考虑本地数据备份措施。对于重要数据，还应考虑远程备份措施。

6.6 防抵赖措施

6.6.1 数据溯源

由于数据应用场景的日益复杂，数据融合、共享的需求广泛存在，因此使得数据的流通途径变得错综复杂，除了在政府内部流动以外，数据还有可能合法流通到其它机构或企业，流通到其它机构的数据，将不可控制。由于数据本身的可复制性，导致数据源头的数据所有者将对数据使用不可控制。因此数据所有者对于数据分发后，有追溯数据被谁使用的需求。另一个角度，智慧城市运营单位内部人员有可能对自己能访问到的内部重要信息数据，通过拷贝、外发、截屏、录屏等各种方式，将内部信息泄露出去。

以上两种场景都需要有数据溯源技术和管理手段的支撑，在数据泄露事件发生后，“事后”的源头追查是及时发现问题、查缺补漏的关键，同时对安全管理制度的执行也会形成一定的威慑作用。应能追查到数据的真实来源，包括数据的生成者，以及来自于什么地域等。通过对数据平台上的敏感数据打上标签，相关属性无缝地嵌入到现有数据之上，并且不改变现有数据的任何结构，处理完成后的数据提交给具体的数据使用者，这种数据不会影响数据使用者的使用，但是如果数据使用者将该数据泄露给其他机构或个人，数据溯源分析处理系统则可以进行审计和跟踪，从而实现数据的非授权扩散监管。

6.6.2 数字签名

数字签名是利用密码学技术对信息的发送者发送信息真实性的一个有效证明，在网络环境中代替传统的手工签字与印章，解决伪造、抵赖、冒充和篡改问题。《中华人民共和国电子签名法》规范了电子签名行为，确立了电子签名的法律效力。在智慧城市的应用中，应对重要的文件、数据进行数字签名，防止抵赖。

7 智慧城市安全管理

7.1 安全管理组织

安全管理组织是信息安全体系的重要组成部分，建立符合监管要求、符合智慧城市信息安全建设目标的安全管理组织是安全体系建设的主要内容之一。安全管理组织应的建立应符合以下原则：

a) 应具备安全领导协调机构；

b) 应设置信息安全专门管理机构；

c) 相关部门应设立信息安全管理岗位；

d) 应对于信息安全职责要清晰定义。

例如，信息安全管理组织的安全职责可参考如下设置：

组织	安全职责描述
智慧城市安全领导委员会	(一) 制定智慧城市安全工作总体目标、总体方针和总体安全策略 (二) 确定安全组织架构和安全角色和职责 (三) 提供足够资源，以建立、实施、运行、监督、评审、保持和改进智慧城市安全管理体系 (四) 授权相关部门对智慧城市安全工作进行考核，审批考核结果并做决策。
智慧城市安全管理部门	(一) 作为智慧城市安全工作的归口管理部门，负责智慧城市安全工作管理、监督和指导 (二) 制定并协调发布智慧城市安全管理办法 (三) 制定智慧城市安全工作的流程、预案并加以落实 (四) 制定并执行智慧城市安全管理计划，指导相关单位 / 部门开展有效的信息安全工作 (五) 负责管理、监督相关单位 / 部门开展自有业务、合作业务的内容监测工作，并对疑似违规信息进行核查处理 (六) 对每年的智慧城市安全工作开展情况进行总结，并发布年度智慧城市安全工作报告
智慧城市安全执行部门	(一) 负责制定具体的信息安全管理策略和规章制度，组织实施信息安全管理措施 (二) 负责每年对安全制度进行修订，以确保其适用性 (三) 负责网络内用户的设置及用户的开户、撤销、权限等管理，负责网络终端重要数据的安全性并定期进行备份 (四) 负责系统健康检查，及时反馈系统缺陷和系统负荷，确保信息系统正常运行 (五) 开展员工信息安全培训，并为员工提供信息安全咨询服务 (六) 保持与监管机构日常的工作联系，跟踪和评估监管意见和监管要求的落实情况 (七) 系统上线时，对应用进行安全配置检查 (八) 负责组织信息安全事件的应急演练和处置工作，以及信息安全教育、培训工作 (九) 负责组织开展等级保护等合规性测评工作 (十) 负责建立信息安全投诉举报受理渠道，承接和处理有关举报线索并反馈处理结果

7.2 安全管理制度

应根据业务的实际需求，制订安全管理制度和策略，并在实际实施过程中进行优化更新。避免制订不能实际执行的制度。制订策略要和安全技术支撑能力相结合，相匹配。

可以制定分层级的安全管理制度体系，可包含但是不限于安全策略、制度与流程、细则与指南等多个层次的管理制度，其中:

· 安全策略类主要确定信息安全总体目标、方针等

· 制度与流程则覆盖了信息安全建设与管理的各个方面

· 细则与指南规范了操作的具体方法和环境

7.2.1 安全策略类

安全策略类管理制度主要目的是统一对安全建设目标、范围、基本原则等基本问题的认识，让智慧城市建设相关各类角色明确智慧城市安全建设方向。

具体的设计和内容可参考如下设置:

类别	管理制度名称	主要内容简介
安全策略	智慧城市安全管理办法	指导智慧城市安全保障的方向，包含智慧城市安全的建设目标、智慧城市安全管理的范围、智慧城市安全管理的基本原则等重要内容。

表 3 安全策略类管理制度举例

7.2.2 制度流程类

制度流程类安全管理制度主要用于明确安全管理的流程，将安全管理的动作行为固化为流程，成为制度可以例行执行起来。

相关设计和内容可参考如下设置:

类别	管理制度名称	主要内容简介
制度流程类	信息安全事件管理规定	建立信息安全事件等级划分、报告、响应、处置机制，明确各类信息安全事件的负责部门和管理流程，确保信息安全事件发生后能得到快速反应和处置，减少后续影响。
	信息系统变更管理规定	对信息系统运维过程中所发生的所有变更进行规范和管理，确保所有变更的统一、有效及可追踪，使变更对信息系统正常运行造成的风险和影响减小到最小程度。
	技术脆弱性管理规定	定期对业务系统实施安全基线检查、漏洞扫描等安全检测，跟踪相关厂商的补丁公告，及时发现系统漏洞并采取适当的处理措施进行修补，减少信息系统自身的脆弱性。
	信息备份管理规定	规范智慧城市各类信息数据的备份机制、备份策略及其管理流程，避免数据的丢损，确保经营和管理等工作的安全稳定运行和历史数据的保存。

制度流程类	日志安全管理规定	通过建立日志安全管理机制，部署日志审计和备份策略，为信息系统监控、审计以及事后追溯提供了重要信息和证据，为信息安全事件管理提供了基础条件。
	终端用户安全管理规定	保障员工使用的终端设备安全、正常、有序运行，规范员工终端设备的使用和职责，并对防病毒、准入、账号密码的用户终端侧的管理进行了明确规定。
	办公区安全管理规定	为办公室、房间和设施设计并采取物理安全管理措施，确保关键设施应坐落在可避免公众进行访问的场地，规定包含敏感信息的文档和介质应妥善保存，不能轻易被公众得到。
	人员安全管理规定	通过制定人员安全管理规定，进一步明确员工的信息安全职责和义务，加强全员的信息安全意识，提升员工的信息安全基础防护技能，减少违规以及误操作的风险。岗位和职责划分应明确，工作人员须签订工作协议，涉及重要信息及隐私信息的人员应签署保密协议。
	信息资产管理规定	规定智慧城市所有信心资产应是可核查的，并且有指定的责任人，赋予保持相应控制措施的职责，应清晰的识别所有信息资产，编制并维护所有重要信息资产的清单。
	设备安全管理规定	通过设备安全管理，防止设备资产的丢失、损坏、失窃或危及设备安全，减少未授权访问信息的风险和防止信息丢失或损坏，避免智慧城市业务活动的中断。
	机房安全管理规定	建立机房安全管理制度，对机房的出入、服务器的开机或关机等工作进行管理，并对有关机房物理访问、物品带进、带出机房和机房环境安全等方面的管理做出规定。
	数据分类管理规定	规定对智慧城市信息数据进行全面识别和逐步梳理，明确定义数据的分类和分级，明确数据在生成、存储、传输、使用和销毁过程中的管理责任，确保数据资产得到适当的保护。
	安全培训管理规定	制定智慧城市信息安全培训管理规定，将信息安全培训与意识教育固化下来，逐步将安全培训和安全遵从纳入到绩效中，以逐步建立和形成信息安全文化。对不同工作人员每年进行不少于一次的安全培训，培训其安全意识、安全技能等。
	第三方管理规定	对涉及访问、处理或管理智慧城市信息或信息处理设施以及与之通信的第三方组织或人员的行为进行明确规定，以减少因恶意或误操作导致的风险，确保符合智慧城市的信息安全要求。
	信息交换管理规定	通过建立信息交换安全管理机制，并根据城市信息数据的分类与分级规定，制定和发布针对合作伙伴、客户、供应商等外部的信息交换管理规定和操作指南。
	系统上线安全管理规定	明确新业务系统上线安全测试和验收工作流程，实现新业务系统上线的规范管理，减少业务系统上线后的安全风险和后期被入侵的可能，保证业务系统的安全稳定运行。

表 4 流程类管理制度举例

7.2.3 操作指南类

操作指南类安全管理制度主要用于指导具体操作或运维人员安全地开展具体的运维操作。

相关设计和内容可参考但不限于如下设置：

类别	管理制度名称	主要内容简介
操作指南类	信息系统配置管理规定	指导系统管理人员进行正确配置管理和操作，实现将各类主要信息系统的配置信息统一备份到配置库，并实施版本控制、配置信息备份和权限管理。
	系统服务与端口管理规定	规范系统管理人员对于信息系统提供的通用服务或专用服务以及系统端口的维护和操作，未授权情况下禁止启用和开放相关服务或端口。
	信息安全监控管理规定	规范和指导系统维护人员对信息系统运行状态、网络流量、各类安全事件等进行实时监控，掌握网络安全态势，规定相关的操作流程，定期提交监控分析报告。
	防病毒管理规定	对防病毒体系进行统一管理规定，包括主机防病毒、网络防病毒、防病毒日常检查与操作管理、病毒库升级与更新等。
	账号口令安全管理规定	明确信息系统账号和口令管理的相关职责、管理流程，确保智慧城市所有计算终端和移动终端、网络设备和服务器、应用系统和数据库等必须设置符合安全要求的账号和密码。

表 5 操作指南类管理制度举例

7.3 人员安全管理

人员管理是安全管理的重要组成部分，智慧城市的建设、运维人员是否能合格的履行自己职责对智慧城市的安全运行至关重要。对人员录用、离岗都应有相应的安全管理流程，对于重要岗位应与员工签署保密协议。应对不同岗位的人员制定相应的培训计划，定期对安全基础知识、岗位操作规程等进行培训，并适当开展技能考核。对内部员工塑造正向的安全文化与意识，牵引员工树立财富要靠劳动创造的价值导向。对员工发现风险、制止风险，给出建设性意见的行为进行表彰，对员工违反安全管理规定的行为进行处罚。对安全管理到位的部门进行表彰，对安全管理混乱且出现重大违规行为部门主管进行管理问责。

对于外部人员的到访，应有完整的陪同、登记备案流程。

7.4 建设安全管理

在智慧城市的建设过程中，应当遵从“三同步”的原则，同步规划设计、同步实施、同步投入运行。将安全管理纳入方案设计、产品采购和使用、软件开发、工程实施、方案测试验收、系统交付等建设过程的全流程。

重点在于以下三个阶段：一是项目设计阶段，坚决按要求进行同步规划设计，建议并要求所有工程项目建议书、可行性研究报告、工程设计文件都要把网络信息安全作为单独章节进行详细说明和介绍，并根据本期工程的建设内容编制网络信息安全技术方案，确保新建、扩容系统本身的安全无漏洞。同时，在投资中计列出网络与信息安全评估的相关费用，真正做到“早规划、早防护”。二是建设环节。对涉及网络信息安全的工程项目，严格按照设计以及相关规范要求同步建设所需的网络与信息安全配套系统进行同步建设。三是验收环节。建议项目中所有交付资料、监理资料中都必须附“网络信息安全专项验收报告”或者相应的章节，并根据实际实施情况将验收内容填写完成。

7.5 供应链安全

随着信息通信技术的普及应用，加强 ICT 供应链的安全可控保障变得至关重要。业界已普遍认识到，ICT 供应链存在安全风险，需要加强 ICT 供应链安全管理。ICT 供应链具有许多不同的特点，ICT 产品由全球分布的供应商开发、集成或交付，ICT 供应链的全球分布性使得使用者对供应链的理解能力和安全风险控制能力在下降。ICT 供应链安全更关注是否会将额外功能注入产品或服务，交付的产品或服务是否一致等。

智慧城市建设涉及到多个阶段多个供应商的多种产品，因此在供应链安全管理应重点考虑以下几个方面：

- 确保供应商提供产品的完整性，保证产品是真正的“干净的”未篡改的产品；
- 确保产品可追溯性，从合同签订到产品到货、部署上线、事后维修等供应链全流程可追溯。
- 对各供应商方案、产品提出安全基线要求，优先选择通过安全测试认证产品，有条件的情况下宜开展安全测试。
- 对于关键信息基础设施等重要的业务系统，优先考虑安全可控的产品，遵从国家的相关规定。

7.6 应急响应

为了在面对安全事故时，能正确的响应、报告和处置，防止业务活动异常中断，减轻安全事故和紧急情况可能造成的损失和后果，安全事件的响应和恢复很重要。

据信息安全事件与故障的反应过程建立事件处理组织，能够有效收集并分析安全事件，并进行相应处理和响应，为安全运维提供工具、工作流以及报告，可减少攻击识别和补救之间的时间，具体工作应包括：事件识别和分类、取证分析、报告与跟踪等。

应建立信息安全应急响应机制，制定应急预案，分类分级处置信息安全突发事件，并定期（不少于 1 年）开展应急演练，依据应急演练的情况，重新评估和完善应急响应机制。进行过程中需要充分听取业务部门的意见，在进行应急演练之前需要与业务部门充分沟通。

应建立风险上报机制。对新发现的风险应及时上报并有效应对。

7.7 安全测评

智慧城市安全建设过程应根据国家相关法律和规定，进行安全规划和设计，依照安全规划设计开展安全建设，建设完成后开展安全测评或评估，并依据测评意见进行整改。具体应遵从安全法规参见 4.2 章。对于智慧城市建设过程中采用的产品也应符合国家对相关产品的检测要求。

8 智慧城市安全运营

8.1 安全运营原则

智慧城市的安全运营是以城市安全运营中心为主要载体，通过安全运营中心、安全防护手段和专业的安全运营团队，体系化地运用安全技术、安全运维和安全管理手段持续降低城市面临的安全风险。

智慧城市的安全运营应遵循以下原则：

- 城市安全运营建设应遵从统一规划、分步实施、不断完善原则；
- 安全运营数据应遵从数据安全法规要求，安全运营过程应遵从安全法规要求；
- 安全运营数据在严格安全保护的前提下应具备最小权限的共享能力；
- 通过安全运营在管理和数据上应具备与其他重要大数据平台或安全管理平台的协同互动能力；
- 应加强包括数据、过程和结果的管理协同和技术合作；
- 应加强隐私、保密和开放的平衡关系；
- 应充分利用已有投资技术设备的融合；
- 应加强政府和企业、企业和企业之间协同，达到更好的社会效应；
- 应注重与第三方安全管理机构、安全测评组织等加强合作，补齐能力短板，借鉴业界先进经验。

8.2 安全运营能力

城市安全运营中心一般由政府牵头组建，由专业安全运营公司负责平台建设、人才输出、培养和运营，可以为智慧城市中的各个信息系统提供从安全咨询、安全防御、安全告警、安全处置、安全应急服务等一揽子的信息安全服务，从事前、事中、事后全面解决信息安全问题。在解决城市中企事业单位安全问题的同时，产生一定的经济价值和社会价值。

城市级安全运营可包括以下能力：

- 7*24 小时全天候城市安全监控中心；
- 快速响应的网络安全应急响应中心；
- 以提升安全治理水准的安全服务中心；
- 支撑可持续性安全能力建设的人才培训教育基地；
- 创新为主的产学研用为一体的安全联合实验室。

8.3 安全运营团队

由于安全运营要求运营团队的专业安全能力，安全运营团队应符合以下要求：

- 安全运营团队应覆盖监测、预警、防护、响应和恢复五大场景的运营；
- 安全运营团队应由“运营交付人员”、“安全分析师”、“研究建模人员”和“安全专家”等多种类专业人员组成。
- 安全运营团队应在人员管理、流程管理、业务管理等方面具有一定先进性。

安全运营团队的建立模式应根据城市的安全人才储备、智慧城市运营模式等多方面实际情况，可采用独立运营、合作运营和自建自营等方式。

8.4 安全态势感知

对于智慧城市安全运营人员应能够了解和把握当前整体的安全态势和未来趋势，通过日志收集和关联分析、可视化等手段，基于大数据分析和安全事件处理结果，对全系统的安全态势进行展现，可以及时将城市的安全运营情况呈现给城市的管理者。

安全态势感知主要涉及以下几点关键技术：

- 基于大数据的智能安全威胁检测

大数据技术已经成为新的一波浪潮，在各个领域被广泛应用。在网络安全领域也可以被有效的用于安全威胁的分析和预判。比如，通过聚类（域名特征、返回特征）和分类（域名语法分析、统计分析）等机器学习算法发现利用动态生成域名绕过防火墙域名黑名单策略的行为。更进一步，基于深度神经网络技术，将威胁判断从一条直线扩展到类似人脑神经网络的多维立体空间，在高维度多拐点的样本空间里，可以实现对“黑白”样本的更精细判断。

此外，利用上百万的黑白恶意 C&C 样本、对上百种报文行为特征（如报文长度分布、时间分布）进行有监督机器学习发现混淆加密来绕过入侵检测系统和情报检测的行为；利用多种行为特征来发现利用 Ping/DNS 协议弱点来外发数据绕过数据防泄漏系统等内容安全系统的行为；采集现网 NetFlow 日志进行自适应滚动基线学习来发现内部侦查、恶意软件扩散、数据窃取、非法端口开放等绕过 IDS 的内部异常行为。

· 多维度事件关联

攻击者的整个攻击行为往往会涉及多个维度，仅从一个维度看可能是正常的，但是把多个维度利用起来综合分析，往往就能发现异常。利用多维度综合分析能力，可以在关键步骤上识别和还原攻击链。通过恶意文件检测分析、WEB 异常检测分析、邮件异常检测分析以及相关关联学习，可以识别是否存在钓鱼邮件、水坑攻击等外部渗透行为，准确识别可以帮助安全管理员将恶意攻击行为拦截在外；大多数攻击者是以数据窃取为入侵目的，通常会将 DNS 协议和 ICMP 协议作为数据外发的承载协议，因此这两种协议是网络服务中最常用、最普通的协议，因此通过对 DNS 流量、Ping 流量的异常检测及关联分析能力，可以精准识别是否存在数据外发行为。通过流量基线异常检测分析、服务器日志检测分析及关联分析能力，可以识别攻击者在内网横向扩散的行为，保护其他核心资产。

· 未知威胁检测

业界通常采用基于已知签名的特征库匹配技术，来检测文件或软件中是否存在恶意代码。这种方式通过匹配样本，可以快速识别已知威胁。而弊端也显而易见，一方面是受限于安全产品的硬件能力，加载的特征库仅用于识别和应对当前主流的已知恶意代码，无法做到未知威胁的有效覆盖。另一方面是新恶意代码的产生速度远远高于安全厂商的特征库更新能力，越来越多的新恶意代码被用于 APT 攻击。因此，进行未知威胁检测是更深入的一种检测方式。

最常用的是利用沙箱技术来进行未知威胁检测，沙箱为程序提供了模拟运行环境，含有恶意代码的未知程序进入到模拟环境中就会自动释放并执行，通过调用相关 API 接口进行修改 / 删除 / 更改注册表信息、关闭杀毒软件进程、创建新文件等行为，实现感染目标主机。而沙箱通过检测这些 API 调用行为来判断是否是正常程序还是含有恶意代码的异常程序。

· 安全态势可视化

提供大屏展示功能，可将网络安全状态信息以图表形式呈现在大屏上，便于汇报、展示、实时监控等。通过威胁地图直观展示智慧城市范围内面临的威胁和发现的威胁事件，方便安全运维分析人员能及时发现威胁；威胁地图支持全球模式和舞台模式。舞台模式可以将客户关注的行政区域显示到屏幕中央，予以重点关注。可以作为舞台的行政区域可以细化到区县。支持从恶意 / 可疑文件和恶意 / 可疑域名等多个维度直观展示威胁分析的结果，帮助有效洞察面临的威胁。

支持从威胁、邮件和文件多个维度展示攻击扩散路径和影响范围。从威胁的攻击扩散维度有效呈现高级威胁的多个攻击阶段，包括：外部渗透阶段、命令与控制阶段、内部扩散阶段、数据窃取阶段，并直观清晰呈现来自不同地区的外部攻击源 / 命令控制服务器和企业内部受到危害和影响的主机。

8.5 安全事件处理

要建立事件处理组织，提升能力，能够有效收集安全事件，并进行处理和响应。在发生安全事件时，除及时采取应急处置措施外，还要依法依规向主管部门报告智慧城市重大安全事件。缩短安全事件破坏和响应修复间的时间差，是减少经济和数据损失的关键。

安全事件的处置除了管理手段，技术措施也是不可或缺的。当软件定义网络的概念出现，过去许多以硬件为载体实现的网络和安全功能，开始以软件和服务的形态出现，其按需调度、不受时间空间限制的特点，极大的适应了业务敏捷变化的要求，对网络安全的处置也带来了很大的好处。全面的网络安全处置方案，应在在控制器层可以实现对网络（交换机、路由等网络设备）、安全（防火墙、IPS 等网络安全设备）以及第三方（终端安全、探针等）上安全能力的统一调度管理，可以提供给用户一体、可视、全局的体验。利用管理员自定义的自动化响应模板，定义出针对不同恶意威胁等级、种类、行为来制定相应的处置方案，从而提升响应效率，将事件发生时的人工处置变为触发响应模板的自动处置。

网安联动的智能处置能力如下图所示：

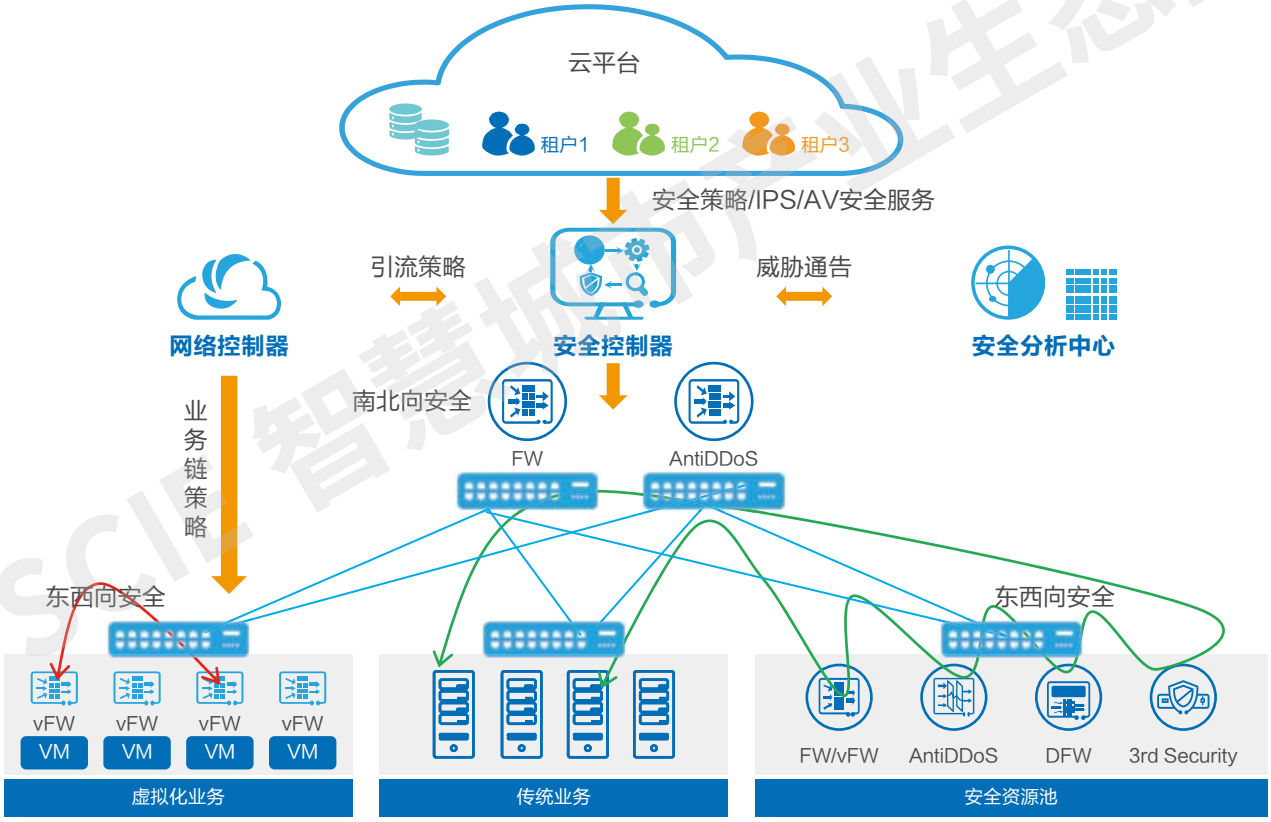

图 3 网络安全联动处置示意图

处置智能的主要组件说明：

1) 分析器：以大数据智能安全分析系统、沙箱为核心组件，具备未知威胁检测、态势感知、威胁溯源等能力，并联动执行器进行智能处置。

· 沙箱：通过旁挂方式（镜像流量）或部署于运维管理区，由防火墙或流探针将可疑文件还原后送至沙箱的方式，进行恶意文件检测，一旦发现安全威胁立即上报网络安全智能分析平台。

· 网络安全智能分析系统：作为安全分析的大脑，采集整网的 Syslog 日志信息、NetFlow 流日志信息、MetaData 元数据信息、可疑文件分析信息，并通过大数据与机器

学习算法相结合，利用多种高级威胁检测模型，识别并发现恶意流量和高级威胁。在检测出安全威胁之后，生成安全联动策略任务交由安全控制器负责执行。

2) 控制器：统一调度管理所有网络和安全网元，包括交换机、路由器、防火墙等网络及安全设备

· 安全控制器：根据网络安全智能分析系统下发的安全联动策略任务自动化生成对应安全控制策略，下发到对应安全执行器或网络控制器进行执行。

· 网络控制器：通过与安全控制器联动，接收其安全联动策略，并下发给路由器、交换机等网络设备进行执行。

3) 执行器：通过与控制器的联动，大数据安全分析平台的引流分析和定位，阻断威胁感染路径，防止内部横向扩散。

· 通过安全执行器（防火墙、IPS 等）、网络执行器（路由器、交换机等）实现对安全威胁的隔离阻断，完成整体闭环响应。

8.6 安全审计

安全运营能力应包括能收集关键设备和系统的日志，并进行安全审计，发现可能的误操作、入侵行为或权限滥用行为。可审计事件包括账号登录、账号管理、客体访问、策略变更、特权功能、系统事件等。审计的范围可覆盖网络设备，安全设备，主机，操作系统等。使用大数据分析系统对安全日志进行准实时连续审计分析。包括的事件有源 IP，日期，时间，请求信息，请求状态，数据大小，查询域名，解析 IP，管理员，登录方式等。

审计记录内容包括事件类型、事件发生的时间和地点、事件来源、事件结果以及与事件相关的用户或主体的身份，审计记录会永久存储在专门的服务器上，并且当审计记录存储量用完时及时报警。

当审计过程失败时，系统自动向运维团队报警，并且启动事件处理程序。运维团队会根据事件具体类型，采用自动或手动机制进行处理；针对上面出现的审计报警或审计问题运维团队每周一次对审计记录进行审查和分析，发现任何异常，均向运维主管报告；此外审计策略的调整会跟进法律法规的变化、客户需求以及信息系统的变化，最终在审查和分析之后，会形成一个审查分析报告。

所有审计信息和审计工具只有授权人员可访问，且生成的原始审计信息不能修改，并且所有被审计的原始信息均为系统的真实记录。所有的用户接入都经过加密措施，具有不可否认性。所有审计的所有日志信息均为真实发生的信息。

8.7 安全加固

应定期对各类设备或系统进行安全加固，如更新配置、打补丁等。遇到紧急事件，要立即采取加固措施，修补漏洞。漏洞扫描应提供操作系统、软件、弱口令、端口等综合漏洞探测服务，检查、评估系统内各个环节运行的系统、应用的安全状态，及时发现可能存在的安全漏洞。

例如，对操作系统的基础安全加固可以包含如下内容：

1) 最小化服务：禁用多余或危险的系统后台进程和服务，如邮件代理、图形桌面、telnet、编译工具等。

2) 服务加固：对 SSH、Xinetd 等常用服务进行安全加固。

3) 内核参数调整：修改内核参数，增强操作系统安全性，如禁用 IP 转发、禁止响应广播请求、禁止接受 / 转发 ICMP 重定向消息。

4) 文件目录权限设置：结合业界加固规范及应用要求，保证文件权限最小化。

5) 账号口令安全：启动口令复杂度检查、口令有效期、登录失败重试次数等。

6) 系统认证和授权：禁止 root 远程登录、尽量不用 root 账号安装运行进程。

7) 日志和审计：记录服务、内核进程运行日志，可以与日志服务器对接。

8.8 策略管理

应能统一考虑智慧城市方案中的安全策略，并通过安全运营中心或在设备上操作，下发和修改安全策略。当城市的网络中部署多台防火墙等安全设备，客户需要集中配置管理城市不同安全域间的安全策略。传统安全管理基于单台设备的维护方式，会导致维护方式不统一，策略配置不一致等问题。管理员根据业务应用场景以及设备的安全管理规划，集中创建需要在策略中应用的对象。对象创建完毕之后，在策略管理中，集中规划创建策略，将创建完的策略应用到多个使用此策略的设备上，完成策略的集中规划管理。

9 未来与展望

全球都在大力发展数字经济、推动产业转型、构建智能社会，数字化的浪潮已经到来。随着信息技术在智慧城市建设中的应用越来越广泛，信息通信技术本身不断更新升级，面临的安全挑战也越来越多。智慧城市的建设者和运营者应将智慧城市安全建设与智慧城市建设同步规划、同步建设、同步使用。同时也要意识到智慧城市的安全建设也不可能一蹴而就，是一个长期运营，不断完善的过程。统一规划、分步实施、长期坚持，逐步构建完善的智慧城市网络安全体系。

后续智慧城市产业生态圈安全技术组将继续组织智慧城市相关的城市管理部门、政府安全主管部门、研究机构、企业等各方力量，在智慧城市安全领域针对安全产业政策、安全技术、安全运营管理等方面开展深入研究，为保障智慧城市的安全建设贡献力量。

参考文献

[1]《中华人民共和国网络安全法》

[2]《中华人民共和国密码法》

[3]《网络安全等级保护条例（征求意见稿）》

[4]《关键信息基础设施安全保护条例（征求意见稿）》

[5]《网络安全审查办法（征求意见稿）》

[6]《云计算服务安全评估办法》

[7]《数据安全管理办法（征求意见稿）》

[8]《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》

[9]《儿童个人信息网络保护规定》

[10]《关于印发促进智慧城市健康发展的指导意见的通知》

[11]《关于加强智慧城市网络安全管理工作的若干意见》

[12]《关于组织开展新型智慧城市评价工作务实推动新型智慧城市健康快速发展的通知》

[13]《关于继续开展新型智慧城市建设评价工作 深入推动新型智慧城市健康快速发展的通知》

[14] GB/T 31167-2014《云计算服务安全指南》

[15] GB/T 31168-2014《云计算服务安全能力要求》

[16] GB/T 35273—2017《信息安全技术 个人信息安全规范》

[17] GB/T 22239-2019《信息安全技术 信息系统安全等级保护基本要求》

[18] GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》

[19] GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》

[20] GB/T 37971-2019《信息安全技术 智慧城市安全体系框架》

[21]《信息安全技术 智慧城市建设信息安全保障指南》（报批稿）

智慧城市产业生态圈

智慧城市产业生态圈由邬贺铨院士担任联席会议主席，中国雄安集团有限公司、华为技术有限公司、北京航空航天大学、中国电子技术标准化研究院、中国电子学会、住房和城乡建设部 IC 卡应用服务中心、深圳市标准技术研究院联合发起，由智慧城市全产业链参与方组成的非营利性组织，致力推动解决智慧城市发展中遇到的问题，从而把数字世界带入每个城市，促进智慧城市产业发展，为中国及全球城市数字化转型提供最佳实践和推广应用的组织。

秘书处地址：深圳市福田区深南中路 1033 号档案大厦

电话：0755-23942266

邮编：518033