海南省城市信息模型（CIM）平台

信息安全标准

（征求意见稿）

海南省住房和城乡建设厅

2022年11月

前　言

海南省CIM平台采用“CIM基础平台”+“特色应用”的“CIM+”的建设模式，将接入和整合全域全量数据资源，搭建和汇集城市三维数字底板，实现多层次信息共享和业务协同，最终建设可支持承载海南省现代化治理和智慧监管、立体防控智慧生态治理、数字政府和智能公共服务的城市信息模型平台。

本标准作为指导海南省城市信息模型（CIM）平台的信息安全体系建设标准，其制定和编写旨在增强城市信息模型（CIM）平台的信息安全保障能力，针对城市信息模型（CIM）平台建设及运维过程中涉及的基础网络、数据以及相关应用，最大化减少城市信息模型（CIM）平台网络安全隐患和数据泄露、滥用等安全事件的发生。

本标准编制过程中，广泛调研了省、市、园区、企业等有关单位，参考了国家及行业相关法律法规，并与《海南省城市信息模型（CIM）基础平台技术导则》安全要求相衔接，认真总结实践经验，在征求了城市管理部门、科研院所、行业专家的意见建议的基础上，制定了本标准。

本标准共分为 6 章，主要技术内容包括：总则，术语和缩略语，基本规定，网络安全要求，软件安全要求，数据安全要求。

本标准由海南省住房和城乡建设厅负责指导实施与监督管理。联通数字科技有限公司、中规院（北京）规划设计有限公司负责具体内容的技术解释。

本标准起草单位：联通数字科技有限公司、中规院（北京）规划设计有限公司。

目　　次

海南省城市信息模型（CIM）平台信息安全标准

1 总则

为指导城市信息模型（CIM）平台的信息安全体系建设，增强城市信息模型（CIM）平台的信息安全保障能力，最大化减少城市信息模型（CIM）平台网络安全隐患和数据泄露、滥用等安全事件的发生，制定本标准。

本标准适用于城市信息模型（CIM）平台建设及运维过程中涉及的信息系统，主要包括基础网络、数据以及相关应用。

城市信息模型（CIM）平台信息系统的安全建设和运维，除应符合本标准外，尚应符合国家现行有关标准的规定。

2 术语和缩略语

2.1. 术 语

2.1.1. **城市信息模型平台** platform of city information modeling

城市信息模型平台是城市信息模型基础平台和基于城市信息模型基础平台构建的各种应用系统的总和，简称CIM平台。

2.1.2. **城市信息模型** city information modeling（CIM）

以建筑信息模型（BIM）、地理信息系统（GIS）、物联网（IoT）等技术为基础，整合城市地上地下、室内室外、历史现状未来多维多尺度空间数据和物联感知数据，构建起三维数字空间的城市信息有机综合体。

2.1.3. **城市信息共享** city information sharing

因履行职责需要使用其他城市相关信息资源和为其他部门提供城市信息资源的行为。

2.1.4. **网络安全** cyber security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

2.1.5. **软件安全性** software safety

软件运行中不引起系统故障的能力。

2.1.6. **数据安全** data security

采用技术和管理措施来保护数据的保密性、完整性和可用性等。

2.1.7. **重要数据** important data

与国家安全、经济发展，以及社会公共利益密切相关的数据。

2.1.8. **敏感数据** sensitive data

由权威机构确定的受保护的信息数据。

2.1.9. **安全保护能力** security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

2.1.10. **物联网** internet of things

通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统。

[GB/T 33745-2017，定义2.1.1]

2.2. 缩略语

CIM—城市信息模型City Information Modeling

APT—高级持续性威胁（Advanced Persistent Threat）

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

DDoS—分布式拒绝服务攻击（Distributed Denial of Service）

SQL—结构化查询语言（Structured Query Language）

IoT—物联网(Internet Of Things)

3 基本规定

3.1 基础设施安全

CIM平台基础设施安全应从安全物理环境、安全通信环境、安全区域边界等层面进行安全防护，信息基础设施安全保障应由信息基础设施的承建单位和运营单位负责。

3.2 安全等级保护

CIM平台信息安全应满足国家信息安全等级保护的要求。CIM平台建设应综合评估各类安全风险，设计安全方案，开展等保定级和备案。

3.3 身份安全

CIM平台应采用CA密码技术及产品，建设相应的身份认证系统和制度，保障平台的物理访问安全、网络接入安全、设备登录安全、应用及接口访问安全、统一身份认证安全；宜充分利用平台依托的网络环境。

3.4 密码安全

CIM平台应采用基于国密的加密技术和产品，从物理访问安全，网络传输安全，设备登录安全，应用及接口访问安全，身份认证安全和数据存储、传输安全等方面进行密码安全保护。

3.5 数据安全

CIM平台的数据安全应符合国家相关法律法规、政策和标准的要求，应采用技术和管理措施来保护数据的保密性、完整性和可用性等，涵盖数据采集、存储、备份、处理、传输、交换及销毁整个数据生命周期。

4 网络安全要求

4.1 安全基础支撑

按照法律法规、政策文件和标准的具体要求，为城市信息模型平台（CIM平台）安全管理、建设和运营提供基础服务活动支撑。

网络安全保护等级评估和风险评估服务，从分级管理和风险管理的角度，针对城市信息模型平台（CIM平台）建设和发展的不同发展阶段进行安全建设和管理，运用科学的方法和手段，系统分析评估城市信息模型平台（CIM平台）信息系统的安全威胁及脆弱性，有助于提出有效的防护对策。

网络安全审查服务由相关部门对涉及国家安全的关键信息技术设施及其采用的网络安全产品和服务进行审查。

1. 城市信息模型平台（CIM平台）基础设施不能设在境外。

2. 建立重大网络安全事件（事故）的应急处置体系。

3. 通过NTP服务器保证城市信息模型平台（CIM平台）时钟源的精度与时间同步的完整性，以保障业务系统的正常运行和城市信息模型平台（CIM平台）安全事件的监测、通报和应急处置的实施。

4. 城市信息模型平台（CIM平台）网络安全产品和服务应以国家发布的相关政策文件《网络产品和服务安全审查办法》为指导，应满足国家相关标准要求。

5. 按照国家相关标准和管理条例，通过城市信息模型平台（CIM平台）信息安全系统的规划设计、建设实施及运营维护，以保障城市信息模型平台（CIM平台）基础安全防护能力。

4.2 安全物理环境

1. 机房场地应选择在具有抗震、防风和防雨等能力的建筑内。

2. 应避开易发生火灾危险程度高的区域;

3. 应避开易产生粉尘、油烟、有害气体源以及存放腐蚀、易燃、易爆物品的地方;

4. 应避开低洼、潮湿、落雷、重盐害区域和地震频繁的地方;

5. 应避开强振动源和强噪音源;

6. 应避开强电磁场的干扰;

7. 应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁;

8. 应远离核辐射源;

9. 抗震设防标准应符合当地抗震设防标准。

10. 温湿度应满足计算机设备的要求

11. 供电系统应具有双路市电（或市电、备用发电机）加不间断电源系统

12. 应设置入侵报警系统

13. 应设置视频监控系统

14. 应设置出入口控制系统

4.3 安全通信环境

对城市信息模型平台（CIM平台）的电子政务外网、电子政务内网和互联网之间的融合网络，以及

一些专用网络的网络设施、通信传输以及终端接入等采取安全防护措施，检测其安全风险与威胁，并对其安全威胁响应处置，以最快时间恢复城市信息模型平台（CIM平台）网络及系统安全运行。

4.3.1 网络区域划分

根据城市信息模型平台（CIM平台）业务重要性划分网络安全域，进行分区分级管理，对不同网络分区采取不同安全级别的隔离防护措施。

4.3.2 区域边界安全

对城市信息模型平台（CIM平台）不同网络或区域之间边界采取访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范等防护措施，对网络日志进行管理分析。网络或区域之间边界包括但不限于城市信息模型平台（CIM平台）中各行业应用系统之间以及各行业应用系统与公共支撑信息系统之间。

4.3.3 数据传输安全

保证跨部门、跨行业、跨系统传输数据的安全，保证数据的保密性、完整性、可用性。

4.3.4 安全防护检测

支持对网络设备、通信线路、传输数据、协议和移动终端等的安全防护与检测，避免未授权访问、干扰、窃听和损坏，保证网络通信的连续性和可靠性。

4.3.5 网络访问控制

对关键网络制定访问控制规则和控制粒度，加强网络访问、数据操作和传输的控制。

4.3.6 API安全

各相关应用系统具备向城市信息模型平台（CIM平台）公共支撑与服务平台开放API的功能，保证城市信息模型平台（CIM平台）API安全使用、控制、分析和管理，安全地进行数据读取、修改、存储、删除。

4.3.7 网络统一监管及监测

对网络整体运行状态、网络日志、安全风险和威胁信息进行统一管理。除了基础的网络防御措施外，可考虑增加全网络安全态势检测、分析和防御能力，运营商大网级别抗DDoS技术或产品，以及新型和高级威胁检测、分析、预警和防御能力，以防止DDoS、APT攻击或0Day漏洞攻击等。

4.4 安全区域边界

4.4.1 边界防护

1. 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
2. 应能够对非授权设备私自联到内部网络的行为进行检查或限制。
3. 应能够对内部用户非授权联到外部网络的行为进行检查或限制。
4. 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

4.4.2 访问控制

1. 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控

接口拒绝所有通信。

2. 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

3. 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

4. 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

5. 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

4.4.3 入侵防范

1. 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。

2. 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

3. 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

4. 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

4.4.4 恶意代码和垃圾邮件防范

1. 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

2. 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

4.4.5 安全审计

1. 应在网络边界、重要网络节点进行安全审计，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。

2. 审计记录应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。

3. 应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。

4. 能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

4.4.6 可信验证

基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

4.5 密码管理要求

4.5.1 健全密码保障体系

根据国家密码法及相关政策指导文件要求，城市信息模型平台（CIM平台）网络和信息系统的建设、使用、管理单位应当健全密码保障体系，实施商用密码应用安全性评估。

4.5.2 密码应用评估

应对采用商用密码技术、产品和服务集成建设的城市信息模型平台（CIM平台）网络和信息系统密码应用的合规性、正确性、有效性进行评估。

在规划、建设和运行阶段充分考虑符合要求的密码产品及服务，并在网络安全等级测评中同步开展商用密码应用安全性评估工作。

4.5.3 覆盖系统不同阶段

在系统建设前，结合城市信息模型平台（CIM平台）业务场景提供应用系统商用密码应用设计方案。系统建设中，提供合规的密码技术、密码产品、密码服务和技术支撑。系统建设后，按照密码管理单位要求，定期开展密码应用安全性评估，检查密码应用不合规项，针对性进行整改。

4.5.4 物理和环境安全

1. 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性。
2. 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性。
3. 宜采用密码技术保证视频监控音像记录数据的存储完整性。
4. 采用的密码服务应符合法律法规的相关要求。需依法接受检测认证的应经商用密码认证机构认证合格。
5. 采用的密码产品应达到GB/T 37092二级及以上安全要求。

4.5.5 网络和通信安全

1. 应采用密码技术对通信实体进行身份鉴别保证通信实体身份的真实性。
2. 宜采用密码技术保证通信过程中数据的完整性。
3. 应采用密码技术保证通信过程中重要数据的机密性。
4. 宜采用密码技术保证网络边界访问控制信息的完整性。
5. 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。
6. 采用的密码服务应符合法律法规的相关要求，需依法接受检测认证的应经商用密码认证机构认证合格。
7. 采用的密码产品应达到GB/T 37092二级及以上安全要求。

4.5.6 设备和计算安全

1. 应采用密码技术对登录设备的用户进行身份鉴别。保证用户身份的真实性。
2. 远程管理设备时，应采用密码技术建立安全的信息传输通道。
3. 宜采用密码技术保证系统资源访问控制信息的完整性。
4. 宜采用密码技术保证设备中的重要信息资源安全标记的完整性。
5. 宜采用密码技术保证日志记录的完整性。
6. 宜采用密码技术对重要可执行程序进行完整性保护并对其来源进行真实性验证。
7. 采用的密码服务应符合法律法规的相关要求需依法接受检测认证的，应经商用密码认证机构认证合格。
8. 采用的密码产品应达到GB/T 37092二级及以上安全要求。

4.5.7 应用和数据安全

1. 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。

2. 宜采用密码技术保证信息系统应用的访问控制信息的完整性。

3. 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。

4. 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。

5. 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。

6. 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。

7. 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。

8. 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据。实现数据原发行为的不可否认性和数据接收行为的不可否认性。

9. 采用的密码服务应符合法律法规的相关要求，需依法接受检测认证的应经商用密码认证机构认证合格。

10. 以上采用的密码产品，应达到GB/T 37092二级及以上安全要求。

4.5.8 管理制度

1. 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。

2. 应根据密码应用方案建立相应密钥管理规则。

3. 应对管理人员或操作人员执行的日常管理操作建立操作规程。

4. 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订。

5. 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制。

6. 应具有密码应用操作规程的相关执行记录并妥善保存。

4.5.9 人员管理

1. 相关人员应理解并遵守密码相关法律法规、密码应用安全管理制度。

2. 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限：

1) 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位。

2) 对关键岗位建立多人共管机制。

3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任。

4) 相关设备与系统的管理和使用账号不得多人共用。

3. 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能。

4. 应定期对密码应用安全岗位人员实行考核。

5. 应建立关键人员保密制度和调离制度。签订保密合同，承担保密义务。

4.5.10 建设运行

1. 应依据密码相关标准和密码应用需求，制定密码应用方案。

2. 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期各环节密钥管理要求。

3. 应按照应用方案实施建设。

4. 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行。

5. 在运行过程中应严格执行既定的密码应用安全管理制度。

6. 应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

4.5.11 应急处置

1. 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置。

2. 事件发生后，应及时向信息系统主管部门进行报告。

3. 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

4.6 安全管理要求

1. 应对不同安全级别的网络按其安全技术和机制的不同要求实施相应的安全管理。

2. 应通过正式授权程序指定网络安全管理人员。

3. 应制定有关网络系统安全管理和配置的规定，保证安全管理人员按相应规定对网络进行安全管理。

4.7 安全规章制度

应按有关规程对网络安全进行定期评估，不断完善网络安全策略，建立、健全网络安全管理规章制度。

1. 制定使用网络和网络服务的策略，依据总体安全方针、策略制定允许提供的网络服务、制定网络访问许可和授权管理制度、保证信息系统网络连接和服务的安全技术正确实施。

2. 制定网络安全教育和培训计划，保证信息系统的各类用户熟知自己在网络安全方面的安全责任和安全规程。

3. 建立网络访问授权制度，保证经过授权的用户才能在指定终端，使用指定的安全措施，按设定的可审计路由访问许可的网络服务。

4. 对安全区域外部移动用户的网络访问实施严格的审批制度，实施用户安全认证和审计技术措施，保证网络连接的可靠性、保密性，保证用户外部连接的安全性。

5. 定义与外部网络连接的接口边界，建立信息安全标准，定期对外部网络连接接口的安全进行评估，对通过外部连接的可信信息系统之间的网络信息提供加密服务，有关加密设备和算法的使用按国家有关规定执行。

6. 对外提供公共服务的系统，应采取严格的安全措施实施访问控制，保证外部用户对服务的访问得到控制和审计，并保证外部用户对特定服务的访问不危及内部信息系统的安全，对外传输的数据和信息要经过审查，防止内部人员通过内外网的边界泄露敏感信息。

7. 对可能从内部网络向外发起的连接资源实施严格控制，建立连接资源使用授权制度，建立检查制度防止信息系统使用未经许可和授权的连接资源。

8. 不同安全保护等级的信息系统网络之间的连接按访问控制策略实施可审计的安全措施，如使用防火墙、安全路由器等，实现必要的网络隔离。

9. 保证网络安全措施的日常管理责任到人，并对网络安全措施的使用进行审计。

10. 按网络设施和网络服务变更控制制度执行网络配置变更控制。

11. 建立网络安全事件、事故报告处理流程，保证事件和事故处理过程的可审计性。

12. 对网络连接、网络安全措施、网络设备及操作规程定期进行安全检查和评估，提交正式的网络安全报告。

13. 信息系统的关键网络设备设施应有必要的备份。

4.8 强制监督

1. 建立独立安全审计，对网络服务、网络安全策略、安全控制措施进行有效性检查和监督。

2. 保证网络安全管理人员具备相应的资质。

3. 信息系统网络之间的连接应使用可信路径。

4.9 应急预案与演练

按照法律法规、政策文件和安全标准的要求，制定城市信息模型平台（CIM平台）安全事件应急预案，包括启动条件、处理流程、恢复流程以及事后的教育和培训等。根据城市信息模型平台（CIM平台）应急规划和规程，按照安全事件的危害程度、影响范围等因素对安全事件进行分级，定期进行应急预案演练。

1. 根据法律法规、政策文件和标准的要求，制定城市信息模型平台（CIM平台）安全事件应急预案，定时评估并修订应急预案，可参考GB/T 24363-2009《信息安全技术 信息安全应急响应计划规范》和GB/T 38645-2020《信息安全技术 网络安全事件应急演练通用指南》。

2. 定期开展城市信息模型平台（CIM平台）应急演练活动，验证操作性，向上级主管部门上报演练情况。

4.10 监测预警

围绕城市信息模型平台（CIM平台）安全目标，依据法律法规、政策文件和相关安全标准，监督城

市信息模型平台（CIM平台）的建设和运营过程，对城市信息模型平台（CIM平台）脆弱性、合规性和安全风险检测和扫描，建立城市信息模型平台（CIM平台）安全监测预警和安全事件通报制度，收集分析城市信息模型平台(CIM平台)安全信息,对安全风险及时上报,包括按需发布城市信息模型平台(CIM平台）安全监测预警信息等。

1．定期对城市信息模型平台（CIM平台）的运行状态、脆弱性以及恶意攻击风险进行实时监测。

2．建立城市信息模型平台（CIM平台）安全事件数据库和漏洞库，制定威胁信息共享机制。

3．监控城市信息模型平台（CIM平台）的整体运行状态，感知网络安全态势，保证城市信息模型平台（CIM平台）日常的安全运行和业务连续性。

4．建立城市信息模型平台（CIM平台）安全事件上报和通报机制。

4.11 应急处置

按照应急预案，在发生安全事件时，按照应急预案处理和恢复流程，采取应急处置措施，向主管部门上报城市信息模型平台（CIM平台）重大安全事件，定期对应急预案和处置流程优化完善。

1．建立城市信息模型平台（CIM平台）安全应急工作机制，提高应对安全事件的能力，预防和减少安全事件造成的损失和危害。

2．建立城市信息模型平台（CIM平台）安全运营及维护体系，统筹管理组织、人员、工具、技术、服务和应急流程，保障城市信息模型平台（CIM平台）日常安全维护与应对安全事件时的响应、处理和恢复有序进行。

3．根据安全事件的上报和通报机制，对城市安全事件及时上报、调查和评估，并根据网络安全事件的等级制定有效的应急处理及恢复机制。

4．定期组织城市信息模型平台（CIM平台）风险处置和运营管理经验分享交流活动。

5．建立跨部门协同运作的应急指挥体系，定期进行应急演练，提高协同配合保护能力。

6．根据安全风险等级、城市信息模型平台（CIM平台）安全风险的可接受程度和城市信息模型平台（CIM平台）安全事件处理成本，制定适当的应急处置机制，降低安全风险影响。

4.12 灾难恢复

在城市信息模型平台（CIM平台）安全事件发生后，根据安全事件的影响和优先级，采取合适的恢复措施，确保城市信息模型平台（CIM平台）业务流程按照规划目标恢复。

1．根据城市信息模型平台（CIM平台）业务的重要性对重要系统和资源等进行备份。

2．参考GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》和GB/T 30285-2013《信息安全技术 灾难恢复中心建设与运维管理规范》制定城市信息模型平台（CIM平台）安全灾难恢复策略和流程，建立安全事件处理及恢复中心，实现快速协同解决，减缓或控制信息安全事件的影响，制定恢复制度，及时恢复系统正常运转状态，提供对城市信息模型平台（CIM平台）脆弱性的持续监测和修复能力。

3．在城市信息模型平台（CIM平台）信息基础设施系统中应建立合理的时间同步机制，保障安全事件监测、上报、应急处置和恢复活动的有效实施。

5 软件安全要求

5.1 软件安全技术要求

软件安全技术要求主要包括对应用软件、智能终端、网站等部署防护措施，检测其安全威胁，对其安全风险和威胁响应进行处置，恢复城市信息模型平台（CIM平台）服务功能。

1. 城市信息模型平台（CIM平台）的各项应用设计和安全满足用户身份鉴别、自主访问控制、安全审计、用户数据。

2. 保证各行业应用系统与城市信息模型平台（CIM平台）应用程序接口的安全。

3. 保证城市信息模型平台（CIM平台）业务信息以及各行业应用系统与城市信息模型平台（CIM平台）之间安全性。

4. 对门户网站、电子邮件、信息系统、终端计算机、存储介质等进行防护。

5. 对涉及境外的产品和服务进行风险评估并满足安全控制要求。

6. 支持城市信息模型平台（CIM平台）监督监管和安全治理，保证业务应用系统和软件开发环境及数据安全。

7. 为各应用建立统一的身份鉴别、访问控制、安全评估和安全审计机制，保证有效的权限管理和安全事件可追溯。

5.2 软件开发安全

5.2.1 组件通信安全

1. 应采用安全通信协议对重要数据进行安全传输（尤其是账号、口令信息），如使用SSL/TLS，HTTPS、SFTP和IPSec等安全协议进行通信。

2. 终端与服务器端之间的WWW服务，宜使用HTTPS安全通信协议。

3. 终端与服务器端之间的FTP服务，宜使用SFTP安全通信协议。

4. 终端与服务器端之间的Telnet服务，宜使用SSH安全通信协议。

5. 终端应用程序应采用加密传输机制对重要信息进行传输。

6. 终端应用程序应采用完整性检查对业务的重要数据或敏感数据进行检查。

7. 终端应用程序应采用抗抵赖攻击技术对重要的交互信息进行保护。

8. 终端应用程序应使用固定的通信端口。

5.2.2 数据库安全

1. 应明确数据库相关的用户管理、资源管理、特权管理和角色管理，明确各种用户的资源权限，并建立标准的权限文档。

2. 数据库原则上应及时更新重要补丁，在安装补丁前应先在测试环境进行，提前进行数据备份，充分准备回退方案和应急预案。

3. 数据库的配置应符合相应的基线配置要求。

4. 应及时修改数据库的默认密码或将默认账号锁定、删除。

5. 数据库的账号应根据业务和维护需要进行合理分配，避免账号共用。

5.2.3 安全隔离

应保证不同业务系统、虚拟机、虚拟网络、虚拟存储之间的安全隔离。

5.3 软件安全评估

1．应定期或在应用系统或运行环境发生重大变更时（包括发现新的威胁和漏洞），进行风险评估。

2．应将评估结果记录在风险评估报告中，并将风险评估结果发布至相关负责人。

3．应根据风险评估报告，有针对性地对城市信息模型平台（CIM平台）的相关应用系统软件等进行安全整改，将风险降低。

5.4 软件安全管理

包括应用基础数据管理、应用动态资源管理、应用业务状态管理、应用访问日志管理、应用系统功能管理、惩罚机制。

5.4.1 应用基础数据管理

1．应实现应用基础数据的集中管理，包括基础数据本地存储以及有关数据本地增加、删除、修改等操作的功能，本地存储基础数据应实时保持与城市信息模型平台（CIM平台）上线的实际业务应用相一致，并且基础数据本地存储时间应不少于12个月。

2．应支持常见数据格式进行基础数据格式的导入和导出，应采用开放式、标准化的数据格式。对于导入的数据，应进行本地数据冲突校验，避免因导入数据可能出现的错漏与既有数据产生冲突。

5.4.2 动态资源使用日志记录

1．应基于用户对城市信息模型平台（CIM平台）虚拟资源、网络资源（IP地址和域名）的成功操作行为，形成用户动态资源使用日志。

2．所记录的用户动态资源使用日志保存时间应满足国家和行业主管部门所规定的要求，并且在规定的保存时间内。

5.4.3 应用业务状态管理

1．应用活跃状态监测管理

1） 应对城市信息模型平台（CIM平台）所有互联网出入口链路上传送的公共信息数据进行全量监测，对通过城市信息模型平台（CIM平台）接入的活跃域名、活跃IP、活跃应用等信息进行统计，形成活跃资源监测记录。对活跃域名监测记录应包括发现的活跃域名、首次采集时间、最后活跃时间、24h累计访问量、IP地址，对于泛解析的域名，应合并监测记录至上级域名。

2） 对活跃IP及应用端口监测记录应包括发现的活跃IP、应用端口、传输层协议类型（TCP/UDP）、首次采集时间、最后活跃时间、24h累计访问量。

3） 应支持通过访问量对活跃域名及活跃IP进行排序，以反映相应资源的活跃程度。同时，应实现活跃资源监测记录的本地存储功能，保存时间不少于30日，并支持查询功能。

2．应用异常状态监测管理

1） 应能基于基础数据记录、动态资源使用日志及活跃资源监测记录，对城市信息模型平台（CIM

平台）接入的IP地址进行全面的监测，自动实时发现异常的IP地址接入、未启用/未分配状态的IP地址接入等异常情况，并形成异常监测记录。

2） 异常监测记录应包括：发现异常的IP地址、登记使用方式和实际使用方式、发现时间/处置时间、当前状态（已处置或未处置）等监测信息。

3） 异常监测结果应按“零报告”的要求定时向城市信息模型平台（CIM平台）维护人员上报，即未监测有异常结果时，应上报零个结果。

4）对于监测发现的异常情况，如在一个上报周期内即完成处置，应实现基础数据监测异常记录的本地存储功能，保存时间不少于60日，并支持查询功能。

5.4.4 应用访问日志管理

1．访问日志记录功能

1） 对于可通过传输层协议或应用层协议头信息区分会话特征的数据流量，应以会话为单位记录访问日志，记录信息应包括源IP、目的IP、源端口（通过这两个网络资源可以反查到它的虚拟资源和物理资源）、目的端口、访问时间［起始时间，精确到秒（s）］，使用域名的访问需留存域名，属于浏览类协议的访问需留存URL。

2） 对于采用加密方式的会话，记录的访问日志应包括源IP、目的IP、源端口、目的端口、访问时间［起始时间，精确到秒（s）］。

3） 对于无法通过传输层协议或应用层协议报文头内容区分会话特征的数据流量，应以数据流（源IP、目的IP、源端口、目的端口均相同，速率大于1帧/s且持续时间大于10s的数据流量）为单位记录访问日志，记录信息应包括源IP、目的IP、源端口、目的端口、起始访问时间［起始时间，精确到秒（s）］、持续时长［精确到秒（s）］。

2．日志查询方式

应支持对访问日志记录有关字段内容的精确查询、检索功能。

3．日志记录查询结果

1） 依据源IP地址、源端口及查询时间，应上报：目的IP地址、目的端口、用户访问URL（仅浏览类协议的访问日志）、用户访问应用程序（仅应用程序的访问日志）、访问时间。

2） 依据源IP地址及查询时间，应上报：目的IP地址、目的端口、用户访问URL（仅浏览类协议的访问日志）、用户访问应用程序（仅可识别应用程序的访问日志）、访问时间。

3） 依据目的IP地址、目的端口及查询时间，应上报：源IP地址、源端口、用户访问URL（仅浏览类协议的访问日志）、用户访问应用程序（仅可识别应用程序的访问日志）、访问时间。

4） 依据用户访问URL（仅浏览类协议的访问日志）及查询时间，应上报：源IP地址、源端口、目的IP地址、目的端口、访问时间。

4．日志留存时间

所记录访问日志的保存时间应满足国家和行业主管部门所规定的要求。

5.4.5 应用系统功能管理

1．权限管理

1）应实现对系统管理人员、操作人员、维护人员的身份认证和权限管理，根据不同的角色授予相应的权限，未经授权的用户不得使用平台的相应功能。

2）应严格限制默认账号的权限，各账号应依据最小授权原则授予为完成各自承担任务所需的权限。

3）应记录系统登录和操作日志，记录应包括登录/操作账号、时间、登录用户IP及操作内容等。

4）应对下发指令及其执行状态进行有效保护，防止受到未授权的干扰与影响，且应能根据下发指令中的可读标记，来实现平台侧全部用户对特定指令及其执行结果的权限控制。

2．运行维护

1）应实现各子系统、组件程序的集中配置管理，对各系统、服务程序的运行状态进行实时监控，为系统的正常运行提供保障。

2）应能对系统设备及接口状态进行持续监测，定期上报系统运行状态监测结果。

5.5 软件安全测试

1．应通过多种身份鉴别，验证用户身份标识的唯一性。

2．应使用安全扫描工具进行安全扫描，检测应用是否存在网络钓鱼，跨站点攻击，SQL注入等安全隐患。

3．测试各个应开放业务系统的接口，能够进行源代码审查。

4．应对应用的数据库安全进行测试，包括但不限于用户操作、用户权限、数据的加密等。

5．应对应用构件库和构件封装进行安全测试，测试内容包括但不限于认证管理、访问控制、构件上传、构件交付等。

6．应对业务应用的支撑环境进行安全测试，测试内容包括但不限于不同的业务节点的安全域内、安全域外迁移等。

7．应对业务应用的资源进行安全测试，测试内容包括但不限于访问控制、会话压力、资源分配、资源授权认证、密钥管理、资源控制等。

6 数据安全要求

6.1 数据生命周期安全

对城市信息模型（CIM）平台的数据，采用技术和管理措施来保护数据的保密性、完整性和可用性等，涵盖数据采集、存储、处理、传输、交换及销毁整个数据生命周期。

6.2 数据安全整体要求

6.2.1 建立全生命周期安全管理

应从以下方面建立健全全生命周期安全管理:

1. 数据源统一鉴别。
2. 敏感数据识别。
3. 数据分类分级标识。
4. 数据脱敏。
5. 数据加密。
6. 传输通道加密。
7. 数据血缘关系。
8. 数据备份与恢复。
9. 数据防泄漏。
10. 销毁数据识别。
11. 数据有效销毁。

6.2.2 制定数据安全事件预案

数据安全类事件主要是指城市信息模型（CIM）平台重要数据遭到泄露或者严重破坏的事件。

1. 发现数据大面积泄露或被严重破坏时，当事人应第一时间向相关负责人报告，应急工作小组应首先排查事件源，开展应急处置工作，必要时可关闭服务器，待检测后再开启服务。

2. 应第一时间做好该事件逐级上报工作，根据数据重要程度，决定是否向公安系统或相关监管单位报案。

3. 事件处理完成后，CIM平台数据恢复重建工作由应急工作小组负责组织制定恢复、整改或重建方案，应编写《海南省城市信息模型（CIM）平台数据安全事件处理报告》，做好该事件处理的过程记录。

数据安全事件应急处理过程中可根据不同事件类型参考的应急处理措施:

1. 数据破坏导致的数据安全事件

1）及时从备份数据中恢复受破坏的最新信息数据;

2）检查恢复后的系统状态是否正常运行;

3）分析信息数据受破坏的原因，人为恶意破坏的应进行追溯，系统故障导致的应分析CIM相关软件故障点，及时联系软件开发商进行修复。

2. 信息内容导致的数据安全事件

1）暂时切断网站对外服务；

2）网站维护人员即刻登录后台，上传换回原始页面；

3）网站、网页由安全监控平台随时密切监视信息内容；

4）保存有关日志审计记录；

5）备份不良信息出现的目录。

3．设备设施故障导致的数据安全事件

1）分析、确认故障设备，准确定位设备位置；

2）切换备用设备；

3）联系设备供应商分析设备故障原因，及时进行修理，涉外修理的应清理数据；

4）无法修理的应采购新的设备，保证设备冗余状态。

4．灾害性事件导致的数据安全事件

1）评估灾害性事件对机房、CIM平台的影响程度；

2）受灾机房网络及信息系统受破坏不能提供服务的，应及时启动容灾机房业务系统；

3）回收受灾机房的数据处理、存储设施，无法使用的进行彻底数据清理；

4）重建受灾机房。

整体应急处理流程如下：

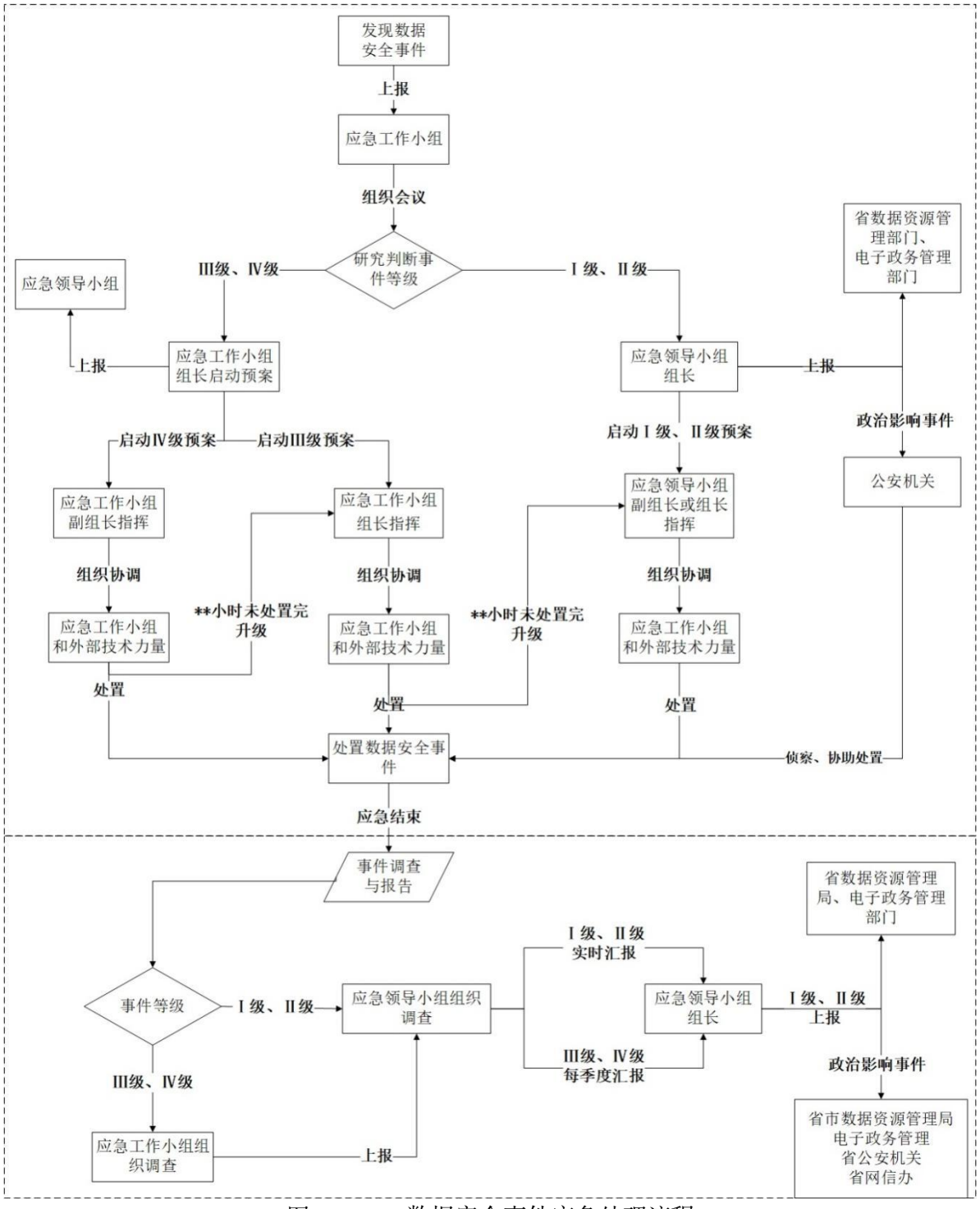

图6. 2. 2 数据安全事件应急处理流程

6.2.3 建立数据分级分类制度

1. 整个CIM平台数据内容主要包括CIM成果数据、时空基础数据、资源调查数据、规划管控数据、工程项目建设数据、公共专题数据、物联感知数据等；同时，宜接入海南省大数据管理局的人口基础库、法人基础库、社会信用库、电子证照库、空间地理库等5大基础库和海南省其它已建信息系统数据。

2. 城市信息模型（CIM）平台数据宜分为以下六个门类:

1）时空基础数据

2）资源调查数据

3）规划管控数据

4）工程建设项目数据

5）公共专题数据

6）物联感知数据

3．对数据进行重要程度分级分类时，应城市信息模型（CIM）平台不同类别数据，应充分考虑其对国家安全、社会秩序、公共利益、个人利益的影响程度，以及数据是否涉及国家秘密、社会秩序、用户隐私等敏感信息。应该考虑不同敏感级别的数据在遭到破坏后对国家安全、社会秩序、公共利益以及个人、行业和组织的合法权益（受影响对象）的危害程度来确定数据的级别。

序号	重要程度	数据特征描述	举例
1	极高/敏感	1．数据的安全属性（完整性、保密性、可用性）遭到破坏数据损失后，影响范围是国家安全和社会秩序，影响程度一般是“特别严重”。 2．一般特征：数据仅针对特殊人员公开，且仅为必须知悉的对象访问或使用。	地理时空基础数据，城市规划、遥感测绘等数据。
2	高	1．数据的安全属性（完整性、保密性、可用性）遭到破坏数据损失后，影响范围是社会秩序，影响程度一般是“严重”。 2．一般特征：数据仅针对内部人员公开，且仅为必须知悉的对象访问或使用。	土地、房屋、海洋、交通、城市地质、地下管线等数据。
3	较高	1．数据的安全属性（完整性、保密性、可用性）遭到破坏数据损失后，影响范围是社会秩序和公共利益，影响程度一般是“中等”或“轻微”。 2．一般特征：数据针对内部人员公开，且仅限内部人员访问或使用。	生态环境、市容市貌、园林绿化、气象监测等数据。

表6．2．3 数据重要程度分类表

6.3 数据采集安全

6.3.1 数据真实性

数据采集应满足数据源鉴别安全技术要求，应采用身份鉴别、数据源认证等安全机制保障城市信息模型（CIM）平台数据来源的真实性，包括边缘环境的IoT设备数据。

1．应按照相关要求对数据分级分类并进行标记，根据标记可对数据安全等级进行识别，并保留标记记录。

2．应按照数据级别确定并实施必要的安全管理策略和保障措施。

3．应对城市信息模型（CIM）平台数据分级分类的变更进行记录，并通知相关数据使用方。

4．应按照数据级别明确使用方对城市信息模型（CIM）平台数据的使用权限。

6.3.2 针对敏感数据采集中的安全防护

针对采集过程中涉及的敏感数据，在数据采集阶段，应从以下方面加强安全防护：

1 身份鉴别：应对数据采集相关的数据处理系统、服务器操作系统、数据库系统的访问进行身份鉴别，数据提供方及接收方需持有有效的数字证书，与相应的软硬件程序配合使用，并妥善保护好自己的数字证书；

2 访问控制：应针对服务器系统、数据库系统、文件管理系统等重要系统设置用户访问策略，阻断对数据、应用、系统等的任何非授权访问，提出告警、并记录审计日志；

3 授权管理安全：应明确授权目的和范围，保留授权记录，并遵照授权执行；并采用技术手段防止数据受到未授权的使用，对敏感数据的采集应经过二次授权；

4 数据脱敏：对数据采集过程中涉及的敏感数据应进行数据脱敏，并建立对敏感数据脱敏有效性的评价机制；

5 数据加密：数据采集过程中，应建立适合CIM平台数据的加密数据透明处理能力，宜选用国密算法对数据进行加密与特征值计算；

6 数据防泄漏：按数据分级分类预先对每类数据设置访问策略、传播策略和传播范围等；

7 安全审计：对数据采集过程进行安全审计，对数据库日志和系统日志进行审计；且具备跟踪和记录数据集成、分发等能力，以支持数据溯源。

6.4 数据存储安全

6.4.1 存储安全要求

1. 应对数据存储环境进行分域分级设计。
2. 应根据数据重要性、量级、使用频率等因素将数据分域分级存储。
3. 应对敏感数据分布式存储。
4. 宜对敏感数据设置在线双活或多活存储机制。
5. 应建立数据冗余一致性校验策略。

6.4.2 数据防护

1. 应支持数据逻辑存储，满足不同数据类型、容量和用户的逻辑存储管理。
2. 应支持数据逻辑存储授权与操作。
3. 应建立分层的逻辑存储授权管理和授权操作规则，实现对数据逻辑存储结构的分层和分级保护。
4. 应对访问用户进行身份鉴别和权限控制，并对用户权限变更进行审核并记录。
5. 应为存储系统安全管理员提供用户标识与鉴别策略、数据访问控制策略，包括访问控制时效的管理和验证，以及接入数据存储的合法性和安全性认证。
6. 应严格限制批量修改、拷贝、下载等操作的权限。
7. 应提供控制机制限制获得访问权的用户将数据传递给非授权的用户。
8. 应对访问通道进行授权许可和访问方式限制。
9. 应建立敏感数据防护区域或敏感数据集群管控访问方式。
10. 应具备数据泄露的发现、阻断等安全机制。

11. 应进行数据血缘关系梳理，建立数字表字段级的上下游关系，建立不同数据源数据合并的分析、核对机制。

6.4.3 数据加密

1. 应对敏感数据采用加密技术，加密存储于数据库、文件系统和存储介质上。

2. 应根据需求对数据库采取整库加密、表加密、字段加密等方式。

3. 应采用符合GM/T 0054等国家相关标准规定的密码技术。

4. 宜根据需求实现数据分级加密。

6.4.4 安全审计

1. 应对数据存储过程的身份鉴别、策略管理、备份作业、恢复作业等事件，以及管理员和用户的各类操作进行安全审计。

2. 审计记录应包括事件的日期和时间、事件类型、主体身份、事件内容、事件的结果（如成功或失败）等内容。

3. 应保证只有经过授权的人员才能查询和访问相应的审计记录，并且只有经过授权的管理员才能对审计记录进行检索、导出和删除操作。

4. 应保存日志记录和审计报告应不少于6个月。

6.4.5 数据备份

1. 应制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、介质替换频率、数据离站运输方法、备份周期/频率、备份范围等。

2. 应具备本地数据备份与恢复功能，备份介质场外存放，敏感数据备份时应进行加密。

3. 应对敏感数据采取异地备份方式，利用通信网络将数据实时批量传送至备用场地，备份传输时应采用加密机制进行保护。

4. 应支持数据管理系统的系统级备份和回滚，应根据数据安全等级要求确定备份周期。

5. 应具备验证备份数据可用性的能力。

6.5 数据处理安全

6.5.1 身份鉴别

1. 应对访问数据处理系统、服务器操作系统、数据库系统、备份系统的管理员进行身份鉴别。

2. 应建立用户口令长度、口令生存周期、口令复杂度等口令管理策略，保证基于口令的身份鉴别安全性。

3. 应对敏感数据或重要模块的操作复合采用两种或两种以上的鉴别技术进行身份认证。

6.5.2 访问控制

1. 应针对服务器系统、数据库系统等重要系统设置用户访问控制策略，为不同用户授予其完成自承担任务所需的最小权限，限制超级管理员等默认角色。

2. 应及时清除系统中无用账号、默认账号，杜绝多人共用同一个系统账号的情况。

3. 用户和管理员账号应采用实名认证，实现追责溯源。

4. 应阻断对数据、应用、系统等的任何非授权访问，提出告警并记录审计日志。

5. 应限制对重要服务器的远程管理，若需要远程管理时应采用SSH等安全方式实现。

6. 应只开启业务所需的最少系统服务及端口，并定期核查。

6.5.3 数据脱敏

1. 应根据不同的业务、应用、部门等采用不同的数据脱敏方式对数据处理过程中产生的敏感数据进行数据脱敏。

2. 应实现动态适配不同数据类型的数据脱敏机制。

3. 应建立对敏感数据脱敏有效性的评价机制，实现效果量化管理。

6.5.4 数据防泄漏

1. 应按数据分级分类预先对每类数据设置访问策略、传播策略和传播范围等。

2. 应采取技术措施防止所有数据在未授权条件下的下载、复制、截屏等方式的数据输出，同时应采取措施防止敏感数据泄露。

3. 应禁止数据处理过程中调试信息的输出。

4. 应防止数据处理过程中日志记录数据的泄露。

5. 应采取通过水印嵌入算法，在数据泄露前在结构化数据（关系表）载体中隐藏水印标记信息。在数据泄露后可提取水印，可作为泄露主体溯源追责的有效技术手段。

6.6 数据传输安全

6.6.1 加强数据传输过程措施安全

1) 应加强软件开发安全管理，保障数据传输工具的安全性，工具上线前应开展必要的渗透测试、支持库漏洞查找等工作，以防止工具使用过程中遭受恶意破坏、功能篡改、信息窃取等攻击。

2) 应采用防火墙、入侵检测等安全技术或设备，确保数据传输网络的安全性。

3) 不同网络区域或者安全域之间应进行安全隔离和访问控制。

4) 终端应采取准入控制、终端鉴别等技术措施，防止非法或未授权终端接入内部网络。

5) 应对通信双方进行身份认证，确保数据传输双方是可信任的。

6) 应采用数字签名、时间戳等方式，确保数据传输的抗抵赖性。

7) 应采用密码技术或非密码技术等方式，确保数据的完整性。

8) 应选用安全的密码算法，禁用如MD5．DES-CBC、SHA1等不安全的算法。

9) 数据内部传输，应采取数据加密、安全传输通道或安全传输协议进行数据传输。

10) 部分敏感数据原则上不应对外传输，若因业务需要确需传输的，应经过事先审批授权，并采取技术措施确保数据保密性。

11) 应在数据传输不完整时清除传输缓存数据。

12) 应在数据传输完成后立即清除传输历史缓存数据。

13) 应定期检查或评估数据传输的安全性和可靠性。

14) 向国家机关、行业主管和监管单位传输数据，应按照国家及行业相关管理要求进行传输。

6.6.2 保障运营商网络传输安全

通过运营商网络传输数据，在满足基本要求的基础上，重要数据应采用专线或VPN等技术确保传输通道的安全，确保数据传输的安全性。

6.6.3 保障物理介质传输安全

通过物理介质批量传递敏感数据时应对数据进行加密或脱敏，并由专人负责收发、登记、编号、传递、保管和销毁等，传递过程中可采用密封、双人押送、视频监控等确保物理介质安全到位，传递过程中物理介质不应离开相关责任人、监控设备等的监视及控制范围，且不应在无人监管情况下通过第三方进行传递，国家及行业主管部门另有规定的除外。

6.7 数据交换安全

6.7.1 用户管理

1. 应支持对用户进行角色分立管理，设立管理角色、审计角色及操作角色。
2. 应根据业务需求、管理范围、组织架构等设置访问控制策略，建立完整的用户管理机制，能够统一设置、统一注销、统一鉴别、统一授权、集中鉴权、集中审计。
3. 应实时将监测到的用户行为和数据、权限、岗位等进行相关性分析。
4. 应支持对特定数据的访问主体进行实时授权和取消授权的管理方式。
5. 应支持基于角色的用户分组，并支持对用户组整体管理。

6.7.2 授权管理

1. 应支持针对用户访问权限、数据操作权限、应用访问数据权限等维度的授权管理机制。
2. 应支持基于数据分级分类的多级授权和操作监管。
3. 应对权限范围外的数据、应用的尝试操作提出告警。
4. 应支持资源文件、库表、接口等各共享方式上不同粒度的权限控制。
5. 资源目录发布应获得授权，明确授权目的和范围，保留授权记录，并遵照授权执行。
6. 数据发布应获得授权，明确授权目的和范围，保留授权记录，并遵照授权执行。
7. 数据申请应获得授权，明确授权目的和范围，保留授权记录，并遵照授权执行。
8. 应遵循数据共享最小化原则，仅授权对业务必需的数据共享访问。
9. 应检查数据的使用请求符合规定条件。
10. 应可设定授权的有效期并定期检查授权的有效性。
11. 应根据安全策略，生成数据访问授权凭证、安全配置信息，并将这些配置信息安全分发到信息交换系统。

6.7.3 数据导出

1. 应对敏感数据建立数据脱敏安全策略，并按照安全策略进行脱敏。
2. 应能根据应用需要保留敏感数据的原数据格式、属性或关联。

3. 应对数据脱敏操作过程进行记录，记录内容应包括操作时间、操作人、操作对象等。

4. 宜提供敏感数据检查工具，对数据进行分析，发现敏感数据。

5. 在数据导出过程中可采用符合国家相关标准规定的密码技术，对敏感数据加密保护后再导出。

6.7.4 数据交换

1. 应对数据交换两端进行用户身份鉴别或设备认证，保证数据交换两端身份的真实性。

2. 应采用如用户名/口令、一次性口令、数字证书、标识密码、生物特征等技术实现交换两端的用户身份鉴别。

3. 在交换敏感数据时，应对数据访问主体复合采用两种或两种以上鉴别技术进行身份鉴别。

4. 应采用数字证书、标识密码等方式实现设备认证。

5. 仅对通信端设备认证时，应确定被授权使用方与被认证设备间关系的真实性，应在多方数据交换时对各接入方进行交叉认证。

6. 应在安全周期范围内对交换两端定期重新认证。

7. 应使用安全协议完成身份鉴别过程，鉴别失败后应实施安全控制措施。

8. 宜在安全周期范围内对交换两端持续实时评估安全风险，并根据风险等级适时发起身份鉴别。

6.7.5 数据导入

1. 应具有数据导入过程保护和回退机制，保证获取过程中产生问题时能有效还原和恢复数据。

2. 应具有故障恢复后数据自动加载能力。

3. 应检验数据的质量，包括对数据格式和接口提出统一要求，并对获取数据是否满足要求做出认定。

4. 应定义空缺值、内容冲突、不合规约束等数据源质量评价条件，并评价数据获取质量。

6.8 数据销毁安全

6.8.1 数据销毁

数据销毁是指城市信息模型（CIM）平台在停止部分或全部业务服务、数据使用以及存储空间释放再分配等场景下，对数据库、服务器和终端中的剩余数据以及硬件存储介质等采用数据擦除或者物理销毁的方式确保数据无法复原的过程。其中，数据擦除是指使用预先定义的无意义、无规律的信息多次反复写入存储介质的存储数据区域。物理销毁是指采用消磁设备、粉碎工具等设备以物理方式使存储介质彻底失效。

6.8.2 数据销毁安全要求

1. 应制定数据存储介质销毁操作规程，明确数据存储介质销毁场景、销毁技术措施，以及销毁过程的安全管理要求，并对已共享或者已被机构内部部门使用的数据提出有针对性的数据存储介质销毁管控规程。

2. 存储数据的介质如不再使用，应采用不可恢复的方式如消磁、焚烧、粉碎等对介质进行销毁处理。

3. 存储介质如还需继续使用，不应只采用删除索引、删除文件系统的方式进行数据销毁，应通过

多次覆写等方式安全地擦除数据，确保介质中的数据不可再被恢复或者以其他形式被利用，具体措施包括但不限于:

1) 采用数据擦除方式销毁数据时，明确定义数据填充方式与擦除次数如全零、全一以及随机零一最少填写7次，并保证数据擦除所填充的字符完全覆盖存储数据区域。

2) 通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据销毁结果。

3) 针对数据擦除后擦除失败的存储介质，进一步采用物理方式进行销毁。

4. 应明确数据销毁效果评估机制，定期对数据销毁效果进行抽样认定，通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据删除结果。

5. 应采取双人制实施数据销毁，分别作为执行人和复核人，并对数据销毁全过程进行记录，定期对数据销毁记录进行检查和审计。

6. 重要数据存储介质不应移作他用，销毁时应采用物理销毁的方式对其进行处理，如消磁或磁介质、粉碎、融化等。

7. 敏感数据存储介质的销毁应参照国家及行业相关载体管理有关规定，由具备相应资质的服务机构或数据销毁部门进行专门处理，并由相应岗位人员对其进行全程监督。

本标准用词说明

1.为便于在执行本导则条文时区别对待,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: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. 《城市信息模型（CIM）基础平台技术导则》（住建部，2021 修订版）
2. 《计算机信息系统 安全保护等级划分准则》GB 17859
3. 《信息安全技术 信息系统安全管理要求》GB/T 20269
4. 《信息安全技术 网络基础安全技术要求》GB/T 20270
5. 《信息技术 备份存储备份技术应用要求》GB/T 36092
6. 《信息安全技术 信息系统通用安全技术要求》GB/T 20271
7. 《计算机信息系统 安全保护等级划分准则》GB 17859
8. 《信息安全技术 网络安全等级保护基本要求》GB/T 22239
9. 《信息安全技术 网络安全等级保护安全设计技术要求》GB/T 25070
10. 《信息安全技术 网络安全等级保护定级指南》GB/T 22240
11. 《信息安全技术 网络安全等级保护实施指南》GB/T 25058-2019
12. 《信息安全技术 智慧城市安全体系框架》GB/T 37971
13. 《信息安全技术智慧城市建设信息安全保障指南》（GB/Z38649）
14. 《城市运行管理服务平台数据标准》（CJ/T545-2021）