海南省城市信息模型（CIM）平台

运维保障标准

（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。

本标准制定和编写旨在规范整个CIM平台的信息化基础设施、数据资源等方面的运维管理水平。同时推进CIM基础平台的规范化、标准化发展的进程，促进海南省CIM行业健康发展。在贯彻国家相关标准的基础上，认真总结实践经验，征求了城市管理部门、科研院所、行业专家的意见建议，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，平台运维基本规定，运维服务对象，运维过程管理，运维组织体系。

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

城市信息模型（CIM）平台运维保障标准

1. 总则

为规范海南省城市信息模型（CIM）平台运维，推动城市转型和高质量发展，推进城市治理体系和治理能力现代化，制定本标准。

本标准适用于城市信息模型（CIM）平台及其相关应用的运维。

CIM平台的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. 城市信息模型基础平台 basic platform of city information modeling

城市信息模型基础平台是管理和表达城市立体空间、建筑物和基础设施等三维数字模型，支撑城市规划、建设、管理、运行工作的基础性操作平台，是智慧城市的基础性、关键性和实体性的新型信息基础设施，简称CIM基础平台。

2.1.2. 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。

2.1.3. 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，构建的城市信息有机综合体。

2.1.4. 城市三维模型 3D city model

城市地形地貌、地上地下人工建（构）筑物等的三维表达，反映对象的空间位置、几何形态、纹理及属性等信息，简称三维模型。

2.2. 缩略语

下列缩略语适用于本文件

CIM —城市信息模型 City Information Modeling；

BIM—建筑信息模型 Building Information Modeling；

GIS-地理信息系统 Geographic Information System。

3. 平台运维基本规定

3.1. 一般规定

3.1.1. 建设原则

CIM平台运维建设应遵循“政府主导、多方参与，因地制宜、以用促建，融合共享、安全可靠，产用结合、协同突破”的原则，统一管理城市信息模型数据资源，提供各类数据、服务和应用访问接口，满足业务协同、信息联动的要求。

3.1.2. 时间参考系

海南CIM平台日期应采用公历纪元，时间应采用北京时间。

3.1.3. 空间参考系

海南CIM平台空间参考应采用2000国家大地坐标系（CGCS2000），高程基准应采用1985国家高程系，深度基准应采用理论最低潮面。

3.1.4. 平台运维

1.CIM平台由CIM基础平台与CIM+应用构成。CIM基础平台运维应建立由海南省住房和城乡建设厅主导，运维服务机构配合的运维管理团队，CIM+应用系统运维应建立由各建设部门主导，运维服务机构配合的运维管理团队。

2. 运维管理团队组成人员由人民政府政务管理办公室领导、系统管理员及相关部门负责人以及运维服务机构领导组成。主要负责监督、管理外包运维服务工作并进行运维绩效评价。并制定系统性的管理制度，包括但不限于组织架构、权限管理、运行维护、操作规程、数据安全、数据保密等。

3.运维管理团队应定期检查、巡检、评估、通报CIM平台的应用情况，保障CIM平台安全可靠运行。

4.运维服务机构应依照运维模式选定，负责承担具体运维工作。

具体应依照实际情况选用合适的运维模式，运维模式包括自行运维、外包运维、混合运维，如下：

自行维护是运维管理机构作为运维服务机构承担CIM平台的运维服务工作；

外包维护是由运维管理机构以外的专业信息技术服务单位作为运维服务机构承担CIM平台的运维服务工作；

混合维护是CIM平台部分要素采用自行运维，部分要素采用外包运维。

3.1.5. 运行环境

CIM平台应整合海南省现有政务基础设施资源，应配备安全稳定的基础软件，宜采用云计算中心的运行环境，或按照现行国家相关标准的要求建设机房提供运行环境，以安全、可靠的硬件环境，保证平台稳定运行。

3.2. 平台特性

3.2.1. 基础性

CIM平台在充分考虑行政主管主体的职能分工、信息共享、集约化建设、个性化建设需求的基础上，由省级统一建设CIM平台以提供市（县）、园区使用。市县、园区级CIM平台在省级CIM平台上建设特色应用，并将数据信息共享到省级平台。

3.2.2. 专业性

CIM平台应能实现在同一场景的下二三维一体的城市多源异构数据汇聚融合、轻量化、模型单体化、模型特征提取、三维可视化表达、查询统计、物联监测和模拟仿真等基本功能。

3.2.3. 集成性

CIM平台应实现与相关平台（系统）对接或集成整合，实现多维信息模型资源共享汇聚，构建并持续完善城市信息模型（CIM）。

1.CIM平台宜对接海南省省级信息化系统：如“多规合一”信息综合管理平台、海南省建筑市场监管公共服务平台、大集中式房产管理信息系统、海南省建设工程质量安全监督管理系统、海南省建设工程质量检测信息平台、海南省城市运行管理平台、海南省工程建设项目审批管理系统、海南省地理信息公共服务平台；

2.CIM平台应能支持“城市管道燃气生命线监管与应急管理、瓶装液化石油气监管、房屋建筑统一编码监管、城市地下市政基础设施监管、城市公共道路照明监管、城市体检监管、业务决策与赋能平台管理、市政设施体征监测、智慧招商管理”等各类CIM+应用。

如图1所示：

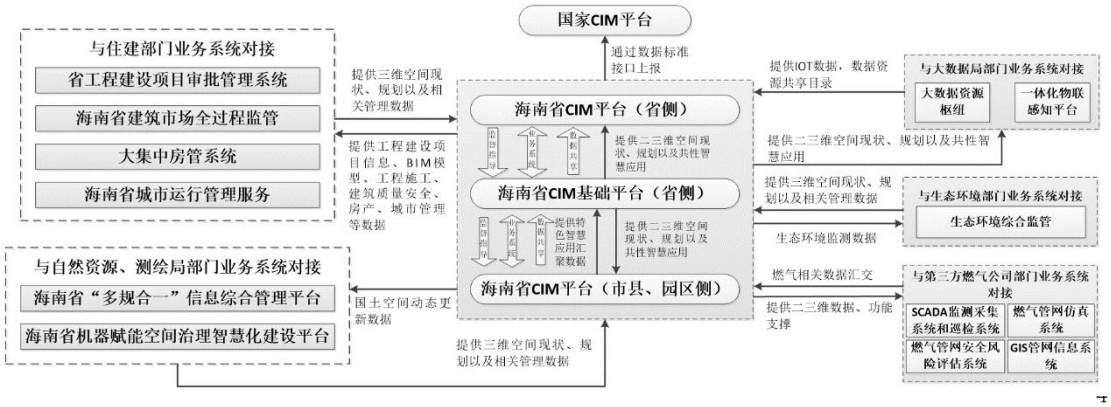

图 1 省级、市（县）级、园区级平台衔接关系

4. 运维服务对象

CIM平台运维服务对象应包括信息基础设施、数据资源等

4.1. 信息基础设施

信息基础设施包括物理环境、网络、主机设备、存储设备、安全设施、基础软件等。

1.物理环境：主要指数据中心运行的机房环境及机房辅助设施，如机房、配线间、空调、不间断电源、供电系统、换气系统、除湿/加湿设备、防雷接地、消防、门禁、环境监控等；

2.网络：进行数据交换与共享、数据同步等服务的系统或平台提供安全网络环境相关的网络设备、电信设施，包括路由器、交换机、防火墙、入侵检测器、负载均衡器、电信线路等。CIM平台应建设满足平台部署运行、数据协同共享、数据安全可靠等需求的网络环境，形成纵向互通、横向互联的网络体系；

3.主机：各类服务器及终端，主要包括服务器、虚拟服务器、台式计算机、移动终端、大屏、VR、AR、便民服务一体机、打印复印机等；

4.存储设备：存储、备份CIM平台信息的各类硬件设备及管理软件等，主要包括存储网络设备、磁盘阵列、磁带库等硬件设备，存储管理系统、备份管理系统等管理软件；

5.安全设施：CIM平台安全防护的硬件设备及软件系统，主要包括安全防控设备、安全检测设备、用户认证设备等硬件设备，安全防控软件、安全监测软件、用户认证系统等软件系统；

6.基础软件：支撑CIM平台运行的支撑软件，主要包括数据库管理软件、中间件软件，业务应用软件等。

4.2. 数据资源

数据资源是指支持CIM平台运行及平台运行过程中产生的数据和信息。数据内容主要包括时空基础数据、资源调查数据、规划管控数据、工程建设项目数据、公共专题数据和物联感知数据等。

5. 运维过程管理

CIM平台运维过程管理应包括监控管理、例行维护、响应式维护、故障处置、应急响应、安全运维、服务总结。

5.1. 监控管理

1.运维服务机构应提供监控巡检服务，应实时或定期对CIM平台运行状态进行监控，如网络、用于存储备份的管理软件、用于平台安全防护的软件系统和基础软件等。并定期对物理环境、主机、用于存储备份的硬件设备、安全设施中的硬件设备等进行人工巡检。

3.运维服务机构应根据事先制定的工作流程，服务要求制定监控及巡检计划，做好监控巡检相关记录，对监控巡检中发现的问题进行通知、通告及处置。

3.监控管理模块应监控多个数据存储、计算与服务节点或其他Web应用，并提供系统监控仪表盘，仪表盘应包含监控硬件资源占用、地图访问热点、节点健康状态等指标。

5.2. 例行维护

1.运维服务机构应提供例行维护服务，建立例行维护服务计划，包括但不限于对CIM平台进行保养、健康检查、系统更新等周期性维护；

2.运维服务机构应根据事先制定的工作流程做好例行维护工作记录，发现问题及时进行通知、通告及处置。

5.3. 响应式维护

1.运维服务机构应根据实际业务需求进行配置变更、平台优化、信息更新等响应式维护，应做好响应式维护工作记录；

2.响应式维护开展前宜根据事先制定的工作流程进行申请审批、通知、通告；

3.响应式维护实施前应制定实施方案，重点是应急恢复方案，确保CIM平台的安全可靠及可恢复性。

5.4. 故障处置

1.运维服务机构应提供故障处置服务，在CIM平台发生故障时，根据服务要求在规定的时间内消除故障影响，并最终清除故障；

2.依据GB/T28827.3分类分级标准，CIM平台故障根据故障严重性和受影响系统的重要性分为特别重大、重大、较大和一般四个等级。重大及以上故障应启动应急预案，按预先制定的应急预案进行处置；

3.故障处置宜遵循“先抢通、后修复，先核心、后边缘''的原则，优先保证重要业务的恢复，特殊情况酌情处理；

4.故障处置应根据预设工作流程开展，根据故障情况适时启动应急响应机制；

5.故障处置完成后应及时记录故障处理方法、做好故障总结，并定期进行统计分析，对发生频次较多的故障现象应进行重点分析，采取相应措施，降低故障发生率。

5.5. 应急响应

1.运维服务机构应提供应急响应服务，应制定应急响应流程，应按应急响应流程响应CIM平台的突发事件；

2. 应急响应流程应包含应急流程应急准备阶段、监测与预警阶段、应急处置阶段、总结改进阶段；

3.应急准备阶段应组建应急响应组织，确定应急响应制度，定义应急事件级别，制定预案，开展培训和演练，具体为：

1）应不断更新完善各项安全事件的应急预案。

2）应急预案应包括：

。

3）人员培训保障措施应满足以下要求：

应定期或不定期地举办不同层次、不同类型的技术讲座或研讨会，确保本应急预案有效运行，以便不同岗位的应急人员熟练掌握突发事件的应急处理知识和技能。

4）应急演练应满足以下要求：

应定期或不定期组织应急预案演练，提高平台突发事件应急响应水平；

应检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求；

应通过演习，进一步明确应急响应各岗位责任，并对预案中存在的问题和不足及时补充、完善。

4.监测与预警阶段应对CIM平台的进行日常监测，对应急事件进行核实和评估，应按照规定的程序启动预案，并保持对应急事件的跟踪。

5.应急处置阶段应采取必要的应急调度手段，基于预案开展应急事件的排查与诊断，进行有效、快速的处理与系统恢复。应及时通报应急事件，提供持续性应急服务保障，并进行结果评估。

6.总结改进阶段应对应急事件发生的原因，处理过程和结果进行总结分析，持续性改进应急工作，完善CIM平台应急响应服务。

7. 应建立预警与应急处理的技术平台，进一步提高CIM平台突发事件的发现和分析能力，从技术上逐步实现发现、预警、处理、通报等多个环节和不同的专项业务系统、系统以及相关部门之间应急处理的联动机制。

8.应建立硬件资源保障措施，满足以下要求：

必须为相应的核心业务平台提供必要的备份设备与线缆等硬件资源，并配备与现有设备兼容的设备，确保在平台设备发生故障时能够尽量降低业务系统的受影响程度，确保相似或

兼容的设备可以在应急情况下调配使用；硬件资源应预先采购并保存在专门位置；
文档资料准备保障措施应满足以下要求：应包括平台工维护手册、操作手册、设备配置参数、拓扑图以及IP地址规范及分布情况等。

5.6. 安全运维

1.环境运维管理

1）应指定专门的部门或者人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

2）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理做出规定；

3）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸质文档和移动介质等。

2.资产运维管理

1）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

2）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

3）应对信息分类与表示方法作出规定，并对信息的使用、传输和存储等进行标准化管理。

3.设备运维管理

1）应对各种设备、线路等指定专门的部门或人员进行定期的维护管理；

2）应建立配套设施、软硬件维护方面的管理制度，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

3）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；

4）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

4.数据传输安全

应通过保障传输介质安全、传输通道安全等措施保障CIM平台的数据传输安全。应满足以下要求：

1）应选择电磁辐射低的数据传输介质，或者采用有效的措施防止数据传输介质的电磁泄漏；

2）应确保数据传输介质（如电缆、光纤等）的物撞环境安全，有效防雷击、防鼠害、防盗、防水、防人为破坏；

3）应确保信息设备接入可靠的无线网络或传感网络；

4） 应采取有效措施保障敏感信息和重要数据传输过程的机密性；

5） 应对采取有效措施保障敏感信息和重要数据传输过程的完整性；

6） 数据管理存储系统应采用安全协议连接，防范非授权访问和管理信息泄露。

5.数据存储安全

运维服务机构应采用数据存储访问控制、数据存储安全审计、数据存储设备与介质安全、数据存储加密、数据离散存储等措施保障数据存储安全。

1）CIM平台的数据存储访问控制应满足以下要求：

应对数据文件进行访问控制，严格控制不同权限的用户对于不同文件的访问和操作，应对文件系统、数据库管理系统、操作系统等采取对应的访问控制措施；

数据库管理系统和操作系统依据最小授权原则设计安全访问控制策略，依据业务要求实现不同用户对不同数据的访问权限；

数据库管理系统和操作系统不得使用相同的用户名和密码，防范入侵操作系统的攻击者直接入侵数据库。

2）数据存储安全审计应满足以下要求：

应对数据文件的操作行为进行安全审计，至少对用户操作、存储事件和文件变更信息进行记录；

应对虚拟化组件的活动进行监控，至少对虚拟网络、虚拟主机、虚拟桌面、虚拟CPU、虚拟存储的活动进行监控；

应对虚拟资源使用情况进行记录，至少对CPU、内存、存储的容量、可用空间、使用比例信息进行记录，并设置报警阈值，提供报警功能；

应使用内容发现机制扫描存储数据，识别已泄漏的敏感数据；

应对平台系统管理员的操作和系统管理员的权限进行审计；

应定期提供平台运行报告，报告内容包括平台运行状态、安全情况、事故情况、变更情况等；

应引入第三方审计机构，对CIM平台定期进行审计，评估是否实现了合理的安全控制措施；

应采取有效措施保障日志不会被非授权的访问、修改和覆盖，确保审计措施不会带来新的安全问题。

3）数据存储设备与介质安全应满足以下要求：

存储设备和介质保存环境必须保持清洁，且需要防盗、防震、防火、防雷、防高温、防潮湿、防静电、防电磁干扰；

制定存储设备和介质资产清单，清单内容包括存储设备和介质名称、责任人、用途、采购时间等，并定期更新存储设备和介质资产清单信息；

正确移动存储设备和介质，存储设备和介质移动时避免碰撞和大幅度震荡；

严格规范存储设备和介质数据读写操作，避免对存储设备和介质超频使用，保障读写数据时的持续供电；

存储设备和介质维修时，必须安排陪同人员对维修过程进行监控，严格控制数据知悉范围，对于重要数据，要求维修人员到指定地点进行维修；

制定存储设备和介质使用管理制度，规范存储设备和介质使用人员权限、使用审批流程、使用操作规范、故障处理流程等。

4)数据存储加密应满足以下要求：

应对敏感数据提供数据加密功能，宜对不同安全要求数据进行不同强度的加密；

应制定和实施密码控制策略，并符合GB/T22081-2008中12.3.1的相关要求；

应采用成熟的密钥管理方案，对密钥的生命周期进行有效的管理，密钥管理应符合GB/T22081中12.3.2的要求。

5)数据离散存储应满足以下要求：

应选择数据离散存储，对数据离散存储的敏感数据片进行加密；

应对数据离散存储的数据进行完整性校验，确保有效的数据重构恢复。

6.数据共享安全

应提供严格的共享数据访问权限控制功能，访问控制粒度细化到用户的具体操作；

应采用有效的措施控制共享数据，确保已授权的用户才能对共享数据进行增加、删除、查看、修改、上传和下载；

应采用有效措施，保障存储的敏感信息和重要数据的机密性和完整性；

在数据共享的过程中使用切片后的数据发布服务进行便用的，前端通过请求调用相关级别、范围的瓦片数据进行业务应用搭建，禁止使用矢量数据服务格式，确保源数据安全和保密。

7.数据备份恢复安全

CIM平台数据备份应采用磁带，有容错能力的磁盘阵列(RAID),光学存储设备等介质；

CIM平台应采取增进物理安全、实施密码及策略、正确分配备份人员的权限等措施进行数据库备份；

应强化本地与异地的物理安全与制度管理，减少人员与备份设备和介质接触的机会，对操作维护人员的操作过程进行审核；

应打印并异地保存备份操作的文档，经常整理并归档备份，把备份和操作手册的副本 与介质共同异地保存；

备份内容的安全应采用密码保护，应包括备份前的数据加密与备份时对备份集的加密两种。密码应具有一定的复杂性，密码必须为大写字母、小写字母、数字、特殊字符的组合，而且不能少于8位；

备份工作应由三人完成：高层管理人员，备份操纵员和备份日志管理员；

应依据GB/T20988的要求制定灾难恢复策略，建立灾备中心；

应设计数据备份与恢复方案，确定数据备份的范围、策略、方法和流程，确定数据恢复的目标、流程；

应依据业务安全目标要求，制定数据备份措施，并及时根据业务需求更新备份措施；应定期组织数据恢复测试；

异地备份中心建设选址，应符合国家政策要求和业务安全要求；

应对介质的废弃处理有明确的规定，对介质安全低级格式化处理。

8.数据安全隔离

采用有效措施隔离CIM平台不同用户的数据和备份数据；

应依据终端、物理主机和虚拟主机的业务类别、地理位置、部门属性和安全级别划分不同的安全域；

应规划合理的虚拟化网络安全控制措施，划分虚拟化网络子网，对CIM平台流入数据和流出数据设置访问控制策略；

应对不同安全级别的业务数据进行物理隔离或强逻辑隔离，即必须部署在不同的物理主机、不同子网、不同集群或者不同虚拟机上；

相同安全级别的业务数据之间，管理终端与业务系统之间的不同安全域需要实现逻辑隔离，需要采用物理防火墙技术、划分子网等方式进行隔离、虚拟化系统实现集群隔离、多租户隔离、资源池隔离、操作系统隔离和数据隔离。

9.CIM平台安全[1]

CIM平台应对所有数据进行严格的控制，应根据用户身份和现实工作中的角色和职责，确定访问数据资源的权限，对用户以及业务数据的访问权限进行配置。数据分类分范围（行政区）进行授权控制；

CIM平台应对系统的所有用户进行分级管理，设置不同的角色，对每个角色分配不同的数据权限。用户管理应包括标识和鉴别，应对授权用户进行识别；

CIM平台应采用三权分立的安全管理体制：系统管理员分为数据库管理员 DBA，数据库安全管理员 SSO，数据库审计员 Auditor 三类。DBA 负责自主存取控制及系统维护与管理方面的工作，SSO 负责强制存取控制，Auditor 负责系统的审计。

10.网络安全

运维服务机构应采用防火墙、入侵检测、漏洞扫描、病毒防治、运营商4G的VPN/APN等网络安全技术，实现对各种不同的安全防御设备的统一管理、配置、监控、分析等，提供全面的、基于统一安全策略的网络安全防御，避免来自各个不同目的的攻击、干扰和非法访问等。

5.7. 服务总结

1.运维服务机构应定期进行运维服务的分析总结；

2.分析总结应包括对CIM平台运行状况的分析总结、例行维护工作的分析总结、突发事件处置情况的分析总结、安全运维的分析总结，并提出优化完善建议，不断优化改进运维工作；

3.应做好相关技术文档的收集、整理和归档工作，宜明确文档的使用范围并严格控制。应做好运维工作过程的记录；

4. 应制定运维操作规程，规范各项维护工作。应定期对运维对象、备品备件进行盘点。

6. 运维组织体系

6.1. 人员组织

1.运维服务机构应成立专职的队伍负责运维工作；

2.运维队伍宜由技术人员和管理人员组成，并根据工作内容配备相应专业技术人员；

3.运维队伍宜根据运维工作对象类别分成多个专业服务组，各专业组分工协作，共同完成运维工作。

6.2. 工作模式

1.运维队伍应根据运维实际建立高效的工作模式，合理利用资源；

2.应建立由热线（服务台）、一线（运维工程师）、二线（运维专家）、专业机构组成的多级技术支持体系。热线不能解决的问题提交一线；一线负责监控遇检、一般性的问题处理，并配合二线进行复杂问题处置，一线不能处理的问题提交二线；二线负责解决复杂问题，并进行深度的运行状况分析、评估，二线不能解决的问题提交设备生产厂商、软件开发商或第三方服务单位等专业机构。

6.3. 岗位职责

1.应进行岗位设计，明确运维岗位，规定岗位职责，岗位职责规定至少应包括维护对象范围、工作内容及工作要求等；

2.根据实际情况，每位运维人员可以任职多个岗位，重要岗位应有两人或两人以上任职。

6.4. 技能要求

1.运维人员应具备信息技术基础知识、运维岗位所需的专业知识及CIM平台所支撑业务的相关业务知识，宜具有专业技能资质证书；

2.应加强人才队伍的建设和培养，定期组织各类培训，运维人员每年参加专业技术培训时间宜不少于48学时。

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：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

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20270 信息安全技术 网络基础安全技术要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 30318 地理信息公共平台基本规定

GB/T 30998 信息技术 软件安全保障规范

GB/T 32399 信息技术云计算参考架构

GB/T 35301 信息技术云计算平台即服务 (PaaS) 参考架构

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 36626 信息安全技术 信息系统安全运维管理指南

GB/T 36092 信息技术 备份存储 备份技术应用要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28827.1-2012 信息技术服务 运行维护 第1部分通用要求

GB/T 28827.3-2012 信息技术服务 运行维护 第3部分：应急响应规范

GA/T 1347 信息安全技术 云存储系统安全技术要求

CJJ/T 296 工程建设项目业务协同平台技术标准