团体标准

**T/CECS**

**城市信息模型(CIM)平台安全技术要求**

Technical requirement for platform security of city information modeling

中国工程建设标准化协会 发布

**目　　次**

[前　　言 I](#_Toc92715963)

[引　　言 II](#_Toc92715964)

[1 范围 1](#_Toc92715965)

[2 规范性引用文件 1](#_Toc92715966)

[3 术语和定义 1](#_Toc92715967)

[4 缩略语 2](#_Toc92715968)

[5 基本规定 2](#_Toc92715969)

[6 安全总体保障要求 4](#_Toc92715970)

[7 安全管理保障要求 5](#_Toc92715971)

[8 安全技术保障要求 6](#_Toc92715972)

[9 安全运营保障要求 14](#_Toc92715973)

[10 安全基础支撑要求 17](#_Toc92715974)

[附录A（资料性）数据脱敏常用技术 26](#_Toc92715975)

[附录B（资料性）软件安全技术要求 28](#_Toc92715976)

[参考文献 30](#_Toc92715977)

前　　言

本文件按照GB/T 1.1-2020《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。

本文件根据中国工程建设标准化协会《关于印发<2021年第一批协会标准制订、修订计划>的通知》（建标协字〔2021〕11号）的要求制定。

本文件由中国工程建设标准化协会提出。

本文件由中国工程建设标准化协会归口管理。

本文件负责起草单位：中国工业互联网研究院、中设数字技术股份有限公司。

本文件参加起草单位：中国建设科技集团股份有限公司、中国建筑标准设计研究院有限公司、住房和城乡建设部遥感应用中心、华为技术有限公司、中能融合智慧科技有限公司、北京航天数据股份有限公司、上海益埃毕建筑科技有限公司、中建七局科技创新发展有限公司、广西数广网安科技有限公司、中国建筑第五工程局有限公司、中铁上海工程局集团市政环保工程有限公司、中国交通建设股份有限公司、中建工程产业技术研究院有限公司、中国建筑第八工程局有限公司、中国建筑科学研究院有限公司、长沙市规划信息服务中心、武汉市自然资源和规划信息中心。

本文件主要起草人：卢春雨、李想、李昊冉、高宇阳、于洁、周小丽、罗文斌、魏来、刘丹、黄敏、封帆、张金山、孟建、程嘉楷、李亚青、李兴文、谭文昊、聂锐敏、王爱华、王新平、代丹丹、何爱丽、景浩、郭小波、李渊源、王磊、孙黎、耿介坦、孙金颖、杨超、方能炜，李云鹏。

本文件主要审查人：尚舵、何慧虹、杨柳忠、杨韬、刘占省、王广斌、樊惠萍、张鸿辉、殷农、陈超熙。

引　　言

本文件以工业和信息化部《BIM软件与CIM平台集成开发公共服务平台》项目为依托，是项目标准体系的一项成果。《BIM软件与CIM平台集成开发公共服务平台》项目由住房和城乡建设部遥感应用中心牵头的联合体成员单位共同组织实施，项目同步开展相关标准体系建设并确定了拟编制的标准清单。其中，城市信息模型（CIM）平台安全技术要求是保障CIM平台安全的重要标准。

编制组调查总结了我国城市信息模型（CIM）平台安全技术实践经验，参考了国内外相关的技术标准，进行了必要的理论研究和验证试验，并在广泛征求意见的基础上，制定本文件。

**城市信息模型平台安全技术要求**

1. **范围**

本文件规定了城市信息模型（CIM）平台安全的总体保障要求、管理保障要求、技术保障要求、运营保障要求、基础支撑要求等技术要求。

本文件适用于城市信息模型（CIM）平台安全体系建设和运营。

1. **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/T 25069 信息安全技术 术语

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GM/T 0054 信息系统密码应用基本要求

1. **术语和定义**

GB/T 25069 界定的以及下列术语和定义适用于本文件。



**城市信息模型　city information modeling**

对城市物质空间对象的数字化表达的多重集合。



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

基于城市信息模型，通过计算机信息技术等手段，建立表达和管理城市的信息平台，并能根据平台使用者的不同需求提供对应的数据和应用服务。



**网络安全　cybersecurity**

通过采取必要措施，防范网络的攻击、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。



**基础设施层　infrastructure layer**

包含CIM平台的计算、存储、接入、容灾、传输等共同构建基础的平台中心资源。CIM平台基础设施层的安全防护对象主要有服务器、存储设备、网络、各类虚拟化管理和应用软件等。



**网络安全等级保护　classified protection of cybersecurity**

对网络实施分等级保护、分等级监管，对使用的网络安全产品按等级管理，对网络中发生的安全事件分等级响应、处置。



**安全域　security domains**

同一系统内有相同的安全保护需求，相互信任，并具有相同的安全访问控制和边界控制策略的子网或网络。

1. **缩略语**

下列缩略语适用于本文件。

BIM——建筑信息模型（Building Information Modeling）

GIS——地理信息系统（Geographic Information System）

IoT——物联网（Internet of Things）

CIM——城市信息模型（City Information Modeling）

1. **基本规定**
   1. **CIM平台安全体系框架**

**5.1.1** CIM平台定位于城市智慧化运营管理的基础平台，宜由城市人民政府主导建设，负责全面协调和统筹管理，并明确责任部门推进CIM平台的规划建设、运行管理、更新维护工作。

**5.1.2** CIM平台安全体系框架建设应包括安全总体保障、安全技术保障、管理保障、建设运营保障和安全基础支撑五个部分（见图1）。

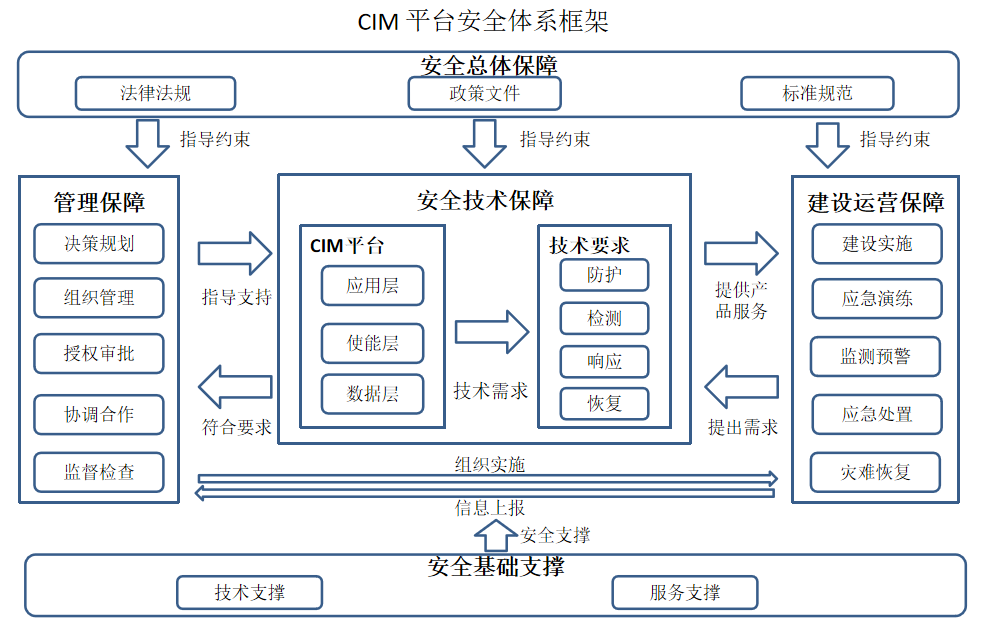


图1CIM平台安全体系框架

**5.1.3** 安全总体保障要素包括国家法律法规、政策文件、标准规范。应通过CIM平台安全总体保障来指导和约束CIM平台的安全管理、技术与建设运营活动；

**5.1.4** 安全管理保障措施包括决策规划、组织管理、授权审批、协调合作和监督检查等方面；

**5.1.5** 安全技术保障以建立纵深防御体系为目标，应围绕CIM平台，从数据、使能、应用等三个层次采用多种安全防御手段实现对系统的防护、检测、响应和恢复，以应对CIM平台安全技术风险；

**5.1.6** 安全建设运营保障是指对CIM平台数据和业务安全工程建设运行状态的监测与维护。CIM平台安全建设运营保障要素宜包含建设实施、应急演练、监测预警、应急处置和灾难恢复；

**5.1.7** 安全基础支撑宜包括CIM平台的安全技术支撑和CIM平台安全服务支撑。安全技术支撑包括密码管理、身份管理和时间同步等。安全服务支撑包括产品和服务的资质认证、安全评估、检测以及咨询服务支撑等。

* 1. **CIM平台安全域**

CIM平台安全域可划分为安全计算域、安全用户域和安全网络域，并应符合下列规定:

1. 应根据各类数据信息在CIM平台中的分布情况，划分并确定安全计算域及其安全等级；
2. 应按照对安全计算域的访问情况，确定安全用户域及其安全等级；
3. 按照连接相同安全等级的安全计算域和/或安全用户域的网络应具有同样安全等级的原则，确定网络安全域及其安全等级。
4. 一个安全域可划分为若干安全子域，安全子域可继续依次细化为次级安全域、三级安全域。
5. 相同的安全域应共享相同的安全策略。
6. 安全域划分的原则和方法可参照《信息安全技术 信息系统通用安全技术要求》GB/T 20271-2006附录B.1.4.1 安全域和安全保护等级划分的原则。
   1. **等级保护定级**

CIM平台等级保护定级应根据业务信息与系统服务受到破坏后对侵害客体的侵害程度判定等级。

1. **安全总体保障要求**
   1. **法律法规**

**6.1.1** CIM平台的规划、设计、建设、运营、维护、应用等全生命周期应遵守《中华人民共和国网络安全法》等法律法规。

**6.1.2** CIM平台各个门类数据的收集、存储、加工、使用、提供、交易和公开等数据活动应符合相关法律法规要求。

* 1. **标准规范**

CIM平台的建设和使用及CIM数据采集、处理、传输、存储、交换和共享应符合有关标准规范的安全要求。

* 1. **政策文件**

　　政府主管部门应出台相关政策文件，组织和指导开展CIM平台安全标准体系规划，研究、制定并实施具有区域特征、行业特性的CIM平台安全标准。

1. **安全管理保障要求**
   1. **相关方**

　　CIM平台建设运营方或政府主管部门应制定CIM平台安全管理保障体系，对CIM平台相关方的安全责任进行界定，并对其活动进行约束、规范及监督。

* 1. **体系要素**

　　安全管理体系宜包括决策规划、组织管理、授权与审批制度、部门合作、安全审核和检查制度。

* 1. **决策规划**

7.3.1 决策规划应从全局高度为CIM平台制定安全管理目标和统一的安全管理策略，选择和调整具体的安全管理措施，形成统一的安全管理体系。

7.3.2 决策规划宜包括但不限于以下方面：

* + 1. 制定网络安全工作的总体方针和安全策略；
    2. 形成全面的安全管理制度体系；
    3. 对各类安全管理活动内容建立安全管理制度；
    4. 制定安全事件报告和处置管理制度；
    5. 对重大安全事件采用分级处理程序和报告程序。
  1. **组织管理**

7.4.1 应明确CIM平台安全管理的领导机构和责任部门，建立CIM平台安全管理岗位和CIM平台安全管理人员管理制度，落实安全责任制。

7.4.2 组织管理宜包括但不限于以下方面：

* + 1. 成立指导网络安全工作的委员会或领导小组；
    2. 设立网络安全管理工作的职能部门；
    3. 设置系统管理员、审计管理员和安全管理员等岗位；
    4. 配备一定数量的系统管理员、审计管理员和安全管理员。
  1. **授权审批**

7.5.1 应对CIM平台生命周期内的各个环节与活动的实施以文件形式明确授权与审批制度。

7.5.2 授权审批宜包括但不限于以下方面：

1. 根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
2. 针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序；
3. 对重要活动建立逐级审批制度；
4. 定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
   1. **协调合作**

7.6.1 各业务部门应共同参与和密切配合，与外联单位通畅协调与合作，及时获取网络安全最新动态，在网络安全事件发生时快速采取有效措施。

7.6.2 部门合作机制包括但不限于以下方面：

1. 加强各类管理人员、组织内部机构和网络安全管理部门之间的协调与合作，定期召开协调会议，协作处理网络安全问题；
2. 加强与网络安全职能部门、各类供应商、业界专家及安全组织的协调与合作；
3. 建立外联单位联系列表，外联单位包括公安机关、兄弟单位、供应商等。
   1. **监督检查**

7.7.1 应制定安全审核和检查制度，定期监督检查。

7.7.2 监督检查宜包括但不限于以下方面：

1. 定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
2. 定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
3. 制定安全检查清单列表，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
4. **安全技术保障要求**
   1. **数据安全保护**
      1. **一般规定**

　　数据安全保护应至少包括以下：

1. 应使用安全可靠的数据库及数据存储设备；
2. 对CIM平台中的数据安全分级，并实施分级保护和脱敏访问；
3. 常用数据脱敏技术可参见附录A。
   * 1. **涉密数据划分**

CIM模型涉密数据划分应符合相关法律法规或标准规范要求，存储、处理涉及国家秘密的数据应遵守有关法律法规及标准规范的规定。

* + 1. **涉密数据处理**

涉密数据脱密处理应明确数据脱密场景，包括数据治理、应用程序调用、运维操作处理等，制定各场景的数据脱密规范、脱密方法和使用限制。使用满足数据治理等应用场景需求的脱敏技术和工具，实现数据根据分级分类快速脱密。

* + 1. **数据使用制度**

应制定数据使用制度和内部责任制度，保证分析处理和使用数据不超出声明的数据使用目的和范围。

* + 1. **数据安全风险识别**

　　应采用技术手段进行数据安全风险识别，对数据滥用的行为进行有效识别、监控和预警，应通过数字水印或采集数据交换、共享及发布等过程实现数据安全溯源机制，确保出现数据泄露时可以有效进行溯源。

* + 1. **数据安全保护措施**

　　应采取有效数据保护措施，并满足以下要求：

1. 应支持不同数据类型、容量和用户的逻辑存储管理；
2. 应支持数据逻辑存储隔离授权操作；
3. 应建立数据逻辑分层分级保护，支持存储授权管理和操作；
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记录；
5. 应支持安全管理员操作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、下载等重要操作权限；
7. 应采用信息流控制机制，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. 应建立数据泄露的发现、阻断等安全机制；
11. 应建立数据存储冗余策略和管理制度，建立数据备份及恢复操作规范；
12. 应提供适当的加密算法，对敏感字段予以加密后进行存储。
    * 1. **数据共享**

　　数据共享应建立信息共享数据安全评估机制，从共享目的合理性、共享数据的范围和合规性、共享方式的安全性、共享后管理责任和约束措施等方面进行评估。应建立统一的数据共享在线审核审批机制和系统，制定和落实数据共享审计策略和审计日志管理规范，为数据共享安全事件的处置、应急响应和事后调查提供帮助，并应满足以下要求：

1. 应明确数据提供者与共享使用者的数据安全责任和安全防护能力；
2. 应明确数据共享涉及机构或部门相关用户的职责和权限，保证数据共享安全策略有效性；
3. 应审核共享数据应用场景，确保没有超出数据服务提供者的数据所有权和授权使用范围；
4. 应采用个人信息去标识、数据加密、安全通道等措施，保护数据共享过程中的个人信息﹑重要数据等敏感信息；
5. 应对数据接收方在共享数据过程的安全防护能力进行评估。
6. 应定期审查公开发布的数据中是否含有非公开信息，采取必要措施建立数据公开事件应急处理流程；
7. 应建立统一数据发布系统，实现公开数据登记、用户注册等发布数据和发布组件的验证机制；
8. 应明确数据接口安全要求和安全控制策略，明确规定使用数据接口的安全限制和安全控制措施；
9. 应具备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；
10. 应具备对数据共享流通过程存证机制，对数据共享前安全评估过程、敏感数据加密过程、数据流通过程、共享后数据使用情况等全流程存证，满足安全审计需要。
    * 1. **数据传输**

　　数据传输应满足以下要求：

1. 应采用符合GM/T 0054有关密码算法的规定，保证通信过程中数据的保密性和完整性；
2. 应具备监控数据传输过程的能力，发现问题时能及时告警并进行阻断；
3. 应定期检查或评估数据传输的安全性和可靠性。
   * 1. **数据销毁**

　　数据销毁应满足以下要求：

1. 应依照数据分类分级建立数据销毁策略和管理制度，明确数据销毁的场景、销毁对象、销毁方式和销毁要求；
2. 应建立规范的数据销毁流程和审批机制，设置相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制；
3. 应明确已共享或者已被其他用户使用的数据销毁管控措施；
4. 应配置必要的数据销毁技术手段，确保以不可逆方式销毁敏感数据及其副本内容。
   * 1. **数据备份和恢复**

　　数据备份和恢复应满足以下要求：

1. 应提供重要数据的本地数据备份与恢复功能，并提供任意时间点数据回溯和零丢失功能；
2. 应提供重要数据的快速恢复、应急使用的功能应提供备份数据的快速查验功能，能快速查验备份数据的完整性、一致性、可用性；
3. 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；
4. 应明确数据备份与恢复的操作规程，明确定义数据备份和恢复的范围、频率、工具、过程、日志记录、数据保存时长等；
5. 应使用数据备份与恢复的统一技术工具，保证相关工作的自动执行；
6. 应定时进行恢复测试，根据业务需求配置异地备份策略；
7. 平台受到破坏后根据安全日志确认时间节点，查找最接近的备份文件进行备份恢复，保证系统正常运行。
   1. **系统安全保护**
      1. **身份鉴别**

　　身份鉴别应满足以下要求：

1. 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度并定期更换；
2. 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
3. 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
4. 应采用口令、密码技术、生物技术等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密码技术来实现。
   * 1. **访问控制**

访问控制应在系统中实施访问控制，用户仅根据自己的权限大小来访问系统资源，不得越权访问。并应满足以下要求：

1. 应对登录的用户分配账户和权限；
2. 应重命名或删除默认账户，修改默认账户的默认口令；
3. 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
4. 应授予管理用户所需的最小权限，实现管理用户的权限分离；
5. 应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；
6. 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
7. 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
   * 1. **安全审计**

应对系统进行安全审计，保持对系统的运行情况及用户行为的跟踪，以便事后追踪分析。并应满足以下要求：

1. 应启用安全审计功能，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；
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. 应对审计进程进行保护，防止未经授权的中断。
   * 1. **入侵检测**
        1. 入侵防范应在边界处入侵检测的基础上，对系统进行入侵检测，补充检测出现在“授权”的数据流或其它遗漏的数据流中的入侵行为。
        2. 入侵检测应满足以下要求：
5. 应遵循最小安装的原则，仅安装需要的组件和应用程序；
6. 应关闭不需要的系统服务、默认共享和高危端口；
7. 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
8. 应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；
9. 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
10. 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
    * 1. **恶意代码防范**
         1. 恶意代码防范应在系统层面进行恶意代码防范，结合边界处恶意代码防范进行双重防范。为防止各种移动存储设备接入系统导致感染病毒，从而通过网络内部感染其它系统。
         2. 恶意代码防范应满足以下要求：
11. 应严格控制各种外来介质的使用，防止恶意代码通过介质传播；
12. 应在所有恶意代码可能入侵的网络连接部位设置防护网关，拦截并清除企图进入系统的恶意代码；
13. 应设置恶意代码防护管理中心，通过对全系统的服务器、工作站和客户机，进行恶意代码防护的统一管理，及时发现和清除进入系统内部的恶意代码；
14. 应将恶意代码防护与网络管理相结合，在网络管理所涉及的重要部位设置恶意代码防护软件，在所有恶意代码能够进入的地方都采取相应的防范措施，防止恶意代码侵袭；
15. 宜采用实时扫描、完整性保护和完整性检验等不同层次的防护技术，将恶意代码检测、多层数据保护和集中式管理功能集成起来，提供全面的恶意代码防护功能，检测、发现和消除恶意代码，阻止恶意代码的扩散和传播。
    1. **边界安全保护**
       1. **边界防护**

　　边界防护应满足以下要求：

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；
5. 应在检测到端口异常流量传输、存在非授权设备私自联到内部网络、内部用户非授权联到外部网络、未通过受控边界接入的无线网络时能够及时阻断并报警；
   * 1. **访问控制**

　　访问控制应满足以下要求：

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，删除多余或无效的访问控制规则，优化访问控制列表，并对源地址、目的地址、源端口、目的端口和协议等进行检查，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；
2. 应提供自主访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
3. 应将自主访问控制的范围覆盖到与信息直接相关的主体、客体及它们之间的操作；
4. 应提供对其自身运行状态的实时监测，对安全管理平台服务水平降低到预先规定的最小值进行检测和报警；
5. 应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。
6. 应根据CIM平台的业务需求配置访问控制策略，合理优化访问控制策略的逻辑关系，并保证最后一条访问控制策略为禁止所有网络通信；
7. 应每日为访问控制策略进行备份，保证能够进行备份恢复；
8. 应在检测到端口异常流量传输时能够及时阻断并报警，由安全管理员判断访问控制策略是否失效并采取恢复措施。
   * 1. **入侵防范**

　　入侵防范应满足以下要求：

1. 应在平台边界及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；
2. 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，应具有实时获取受保护网段内的数据包的能力；
3. 应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击、网络蠕虫攻击、文件脆弱性攻击、浏览器脆弱性攻击、应用层安全漏洞攻击等，并能够及时防止或限制；
4. 应监视整个网络或者某一种特定协议、地址、端口的报文流量和字节流量，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；
5. 应维护入侵防护机制的升级和更新。
   * 1. **恶意代码防范**

　　恶意代码防范应满足以下要求：

1. 应在区域边界及关键网络节点处对恶意代码和垃圾邮件进行检测和清除，并维护恶意代码防护机制、垃圾邮件防护机制的升级和更新；
2. 应具备对一种或多种编程语言检测源代码缺陷的能力，具有对源代码编译后的字节码进行检测的能力；
3. 应能够检测出目前主要的代码应用安全漏洞和严重的质量缺陷，至少包括跨站脚本、未释放的资源、空指针引用、内存泄漏。
   * 1. **安全审计**

　　安全审计应满足以下要求：

1. 应在区域边界进行安全审计，对所有用户的重要行为和重要安全事件进行审计，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，并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；
2. 应提供覆盖到每个用户的安全审计功能，记录所有用户对安全管理平台重要操作和安全事件进行审计；
3. 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
4. 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；
5. 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；
6. 应根据统一安全策略，提供集中审计接口。
7. **安全运营保障要求**
   1. **保障要素**

　　CIM平台安全建设运营保障要素宜包含建设实施、监测预警、应急处置和灾难恢复等内容。

* 1. **建设实施**
     1. CIM平台安全建设者应围绕CIM平台安全目标，按照总体规划和规程，开展CIM平台安全工程实施工作，符合法律法规和标准要求，确保CIM平台信息安全工程和信息化工程同步建设，保证CIM平台信息系统和相关组件在采购、开发、组装、集成、调试、试运行以及运行过程满足安全要求，保障CIM平台安全工程建设过程操作规范、可追溯，所提供的安全服务水平可评估。
     2. **CIM平台安全建设应包含以下方面：**

1. 安全工程实施、供应链保障、人员安全管理及合规性管理的策略和制度；
2. 安全管理的责任部门和责任人；
3. 安全保护对象、目标、等级、定级依据以及CIM平台安全建设方案的论证、审定和报备；
4. 安全需求分析和安全措施；
5. 供应链中相关方的责任与义务；
6. 政府部门信息安全防护要求；
7. 专业的CIM平台安全建设安全支撑服务团队、安全服务机制、人员安全管理制度；
8. 安全监督、审核与风险评估；
9. 关键系统、设备、组件等的配置信息和保存记录；
10. 产品和服务的备案机制。确保采用通过国家相关部门安全审查和资质认证的产品和服务；
11. 项目实施进度和质量控制；
12. 安全工程实施的测试验收、交付以及等级测评。
    1. **监测预警**
       1. CIM平台安全运营者应围绕CIM平台安全目标，依据法律法规、政策文件和相关安全标准，建立CIM平台安全监测预警体系，监测CIM平台各系统运行状况，发现CIM平台信息系统的脆弱性和安全风险，收集分析CIM平台安全事件信息，对安全风险及时报告和通报，按需发布CIM平台各类安全监测预警信息。
       2. CIM平台监测预警应包含以下方面：
13. 按照《国家网络安全事件应急预案》的规定进行预警分级、监测预警、预警研判及预警响应发布与解除；
14. 网络和设备的监测监控；
15. 公共信息支撑平台等基础设施的监测监控；
16. 安全威胁信息交换系统和信息共享机制；
17. 安全漏洞和恶意代码识别、修补和防范机制；
18. 安全事件报告与通报机制；
19. 安全态势感知。
    1. **应急处置**
       1. CIM平台安全运营者应该按照法律法规、政策文件和标准规范的要求，制定CIM平台安全事件应急预案，对不同级别的事件，明确启动条件、处置流程、恢复流程。应部署安全保护措施，预防CIM平台安全事件的发生。当发生安全事件时，应确保及时采取应急处置措施，并向主管部门报告CIM平台重大安全事件。
       2. CIM平台应急处置应包含以下方面：
20. 安全事件应急预案及其有效性评估；
21. 应急处置机制；
22. 应急演练；
23. 安全事件教育培训；
24. 应急指挥体系。
    1. **灾难恢复**
       1. 在CIM平台发生安全事件后，CIM平台安全运营者应根据安全事件的影响程度和业务的优先级，采取措施确保CIM平台信息系统业务流程按照规划目标恢复。
       2. CIM平台灾难恢复应包含以下方面：
25. 灾难恢复演练；
26. 针对主机故障、存储故障、操作系统故障、应用系统故障等局部系统故障的防御及快速恢复手段；
27. 业务信息、重要系统和数据资源的容灾备份；
28. 数据严重毁损的防御及快速恢复手段；
29. 灾难恢复策略和流程，包括快速协同处理，降低或控制各类信息安全事件的影响，及时恢复CIM平台各信息系统正常的运转状态等。
30. **安全基础支撑要求**
    1. **一般要求**
       1. **安全基础支撑要素**

　　CIM平台安全基础支撑宜包括安全技术支撑和安全服务支撑。

* + 1. **安全技术支撑**

　　安全技术支撑宜包括用户身份鉴别、密码管理、自主访问控制。

* + 1. **安全服务支撑**

　　安全服务支撑宜包括风险评估和安全检测。

* 1. **用户身份鉴别**
     1. **用户类别**

　　用户身份鉴别应包括对一般用户和系统用户的身份进行标识和鉴别。

* + 1. **鉴别要求**

　　用户身份鉴别应包含以下要求：

1. 需进入应用软件系统的全部用户，应先进行标识（建立注册账号）；
2. 应用软件系统的用户应以用户名和用户标识符（UID）等信息进行标识，并在应用软件系统的整个生存周期实现用户的唯一性标识，以及用户名或别名、UID等之的一致性；
3. 采用强化管理的口令鉴别/基于令牌的动态口令鉴别/生物特征鉴别机制进行用户身份鉴别，并在每次用户登录系统时进行鉴别；
4. 鉴别信息应是不可见，具有相应的抗攻击能力，并在存储和传输时进行安全保护；
5. 通过对不成功的鉴别尝试的值（包括尝试次数和时间的阈值）进行预先定义，并明确规定达到该值时所应采取的具有规范性和安全性的措施来实现鉴别失败的处理；
6. 将用户进程与所有者用户相关联，使用户进程的行为可以追溯到进程的所有者用户；
7. 将系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务要求者用户。
   1. **密码控制**
      1. **密码控制一般要求**

　　密码控制应实现保密性、完整性/真实性、抗抵赖性、可鉴别性。

* + 1. **控制方法**

　　密码控制的管理方法应包含以下要求：

1. 应基于风险评估来识别需要的保护级别，同时考虑需要的加密算法的类型、强度和质量；
2. 对通过移动介质、可拆卸的介质设备或通信线路来传输的信息应使用加密保护；
3. 应制定密钥管理办法，包括密钥保护方法，以及在密钥丢失、损害或毁坏后加密信息的恢复方法；
4. 应明确部门（岗位）职责分工，以及为确保有效实现而采用的标准；
5. 当实现组织的密码策略时，应符合我国应用密码技术的规定和限制，以及加密信息跨越国界时的问题。
   1. **自主访问控制**
      1. **控制类别**

　　自主访问包含控制功能和控制策略，即命名用户应以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问。

* + 1. **控制策略**

　　当有多个自主访问控制功能时，其访问控制策略应具有一致性。

* + 1. **自主控制要求**

　　应提供用户按照确定的访问控制策略对自身创建的客体的访问进行控制的功能，并应包含以下要求：

1. 客体创建者有权以各种操作方式访问自身所创建的客体；
2. 客体创建者有权对其他用户进行“访问授权”，使其可对客体拥有者创建的指定客体能按授权的操作方式进行访问；
3. 客体创建者有权对其他用户进行“授权传播”，使其可以获得将该拥有者的指定客体的访问权限授予其他用户的权限；
4. 客体创建者有权收回其所授予其他用户的“访问授权”和“授权传播”；
5. 未经授权的用户不得以任何操作方式访问客体；
6. 授权用户不得以未授权的操作方式访问客体。
   * 1. **控制粒度**

控制粒度应满足以下要求：

1. 以文件形式存储和操作的用户数据，在操作系统的支持下，应实现文件级粒度的自主访问控制；
2. 以数据库形式存储和操作的用户数据，在数据库管理系统的支持下，应实现对表级/记录、字段级粒度的自主访问控制；
3. 在应用软件系统中，应通过设置自主访问控制的安全机制，实现文件级粒度的自主访问控制。
   1. **用户数据完整性保护**

对用户数据应满足以下要求：

1. 对应用软件系统中通过网络传输的用户公开数据，应进行完整性检测，并及时发现其完整性被破坏的情况；
2. 对在应用软件系统中存储的用户一般数据，应进行完整性检测，并在数据被使用前发现其完整性破坏的情况；
3. 对应用软件系统中通过网络传输的用户一般数据，应进行完整性检测，并发现其完整性被破坏的情况；
4. 对应用软件系统中进行处理的用户一般数据，应通过操作序列的回退等措施实现完整保护。
   1. **风险评估**
      1. **整体要求**

风险评估应贯穿于信息系统生命周期的各阶段中，每个阶段风险评估的具体实施应根据该阶段的特点有所侧重地进行。

1. 在规划设计阶段，应通过风险评估以确定系统的安全目标；
2. 在建设验收阶段，应通过风险评估确定系统的安全目标达成与否；
3. 在运行维护阶段，应实施动态风险评估以识别系统面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现。
4. 宜采用风险评估工具开展风险评估活动。
   * 1. **规划阶段风险评估**

　　规划阶段的评估应能够描述信息系统建成后对现有业务模式的作用，包括技术、管理等方面，并根据其作用确定系统建设应达到的安全目标，评估结果应体现在信息系统整体规划或项目建议书中，应包含以下方面：

1. 是否依据相关规则，建立了与业务战略相一致的信息系统安全规划，并得到最高管理者的认可；
2. 系统规划中是否明确信息系统开发的组织、业务变更的管理、开发优先级；
3. 系统规划中是否考虑信息系统的数据及系统连续运行的威胁、环境，并制定总体的安全方针；
4. 是否提供断网可用功能；
5. 系统规划中是否描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；
6. 系统规划中是否描述所有与信息系统安全相关的运行环境，包括物理和人员的安全配置，以及明确相关的法规、组织安全策略、习惯、专门技术和知识等。
   * 1. **设计阶段风险评估**

　　设计阶段的风险评估结果应对设计方案中所提供的安全功能符合性进行判断，并应作为采购过程风险控制的依据。本阶段评估中，应详细评估设计方案中对系统面临威胁的描述，将使用的具体设备、软件等资产及其安全功能需求列表，评估结果应体现在信息系统需求分析报告或建设实施方案中，包含以下方面：

1. 设计方案应符合系统建设规划，并得到最高管理者的认可；
2. 设计方案应对系统建设后面临的威胁进行了分析，重点分析来自物理环境和自然的威胁，以及由于内、外部入侵等造成的威胁；
3. 设计方案中的安全需求应符合规划阶段的安全目标，并基于威胁的分析，制定信息系统的总体安全策略；
4. 设计方案应采取了一定的手段来应对系统可能的故障；
5. 设计方案应对设计原型中的技术实现以及人员、组织管理等方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性。
6. 设计方案应考虑可能随着其他系统接入而产生的风险；
7. 系统性能应满足用户需求，并考虑到峰值的影响，是否在技术上考虑了满足系统性能要求的方法；
8. 应用系统（含数据库）应根据业务需要进行了安全设计；
9. 设计方案应根据开发的规模、时间及系统的特点选择开发方法，并根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；
10. 设计阶段的评估可采用安全建设方案评审的方式判定方案所提供的安全功能与信息技术安全技术标准的符合性。
11. 在安全需求变更和设计变更后，应重新进行评估。
    * 1. **实施阶段风险评估**

　　应根据系统安全需求和运行环境对系统开发、实施过程进行风险识别，并对系统建成后的安全功能进行验证，在实施及验收时应进行质量控制，并基于设计阶段的资产列表、安全措施，对规划阶段的安全威胁进行进一步细分，同时评估安全措施的实现程度，进而确定安全措施能否抵御现有威胁、脆弱性的影响。本阶段风险评估可采取对照实施方案和标准要求的方式，主要对系统的开发与技术/产品获取、系统交付实施两个过程进行评估，并应满足以下要求：

1. 应满足法律法规、政策、标准规范等；
2. 应满足信息系统的功能需要；
3. 应根据信息系统的资产、威胁和脆弱性的分析结果，确定在符合相关法律、政策、标准和功能需要的前提下选择最合适的安全措施。
4. 应明确系统建设后应进行怎样的测试和检查。
5. 应进行资产面临的威胁和脆弱性分析；
6. 系统的安全功能进行应满足验收测试要求，安全措施应能够抵御安全威胁；
7. 评估应建立与整体安全策略一致的组织管理制度；
8. 系统风险控制效果应满足预期要求。
   * 1. **运行阶段风险评估**

　　运行维护阶段风险评估应包含以下方面：

1. 在真实环境下较为细致的评估，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等；
2. 应全面地分析威胁的可能性和影响程度，对非故意威胁导致安全事件的评估可以参照安全事件的发生频率，对故意威胁导致安全事件的评估主要就威胁的各个影响因素做出专业判断；
3. 应是全面的脆弱性评估，可以采取核查、扫描、案例验证、渗透性测试的方式实施，安全保障设备的脆弱性评估应考虑安全功能的实现情况和安全保障设备本身的脆弱性，管理脆弱性评估可采取文档、记录核查等方式进行验证；
4. 对重要资产的风险宜进行定性或定量的风险分析，描述不同资产的风险高低状况。
5. 运行维护阶段的风险评估应定期执行；
6. 当组织的业务流程、系统状况发生重大变更时，也应进行风险评估。重大变更包括：增加新的应用或应用发生较大变更；网络结构和连接状况发生较大变更；技术平台大规模的更新；系统扩容或改造；发生重大安全事件后，或基于某些运行记录怀疑将发生重大安全事件；组织结构发生重大变动对系统产生了影响。
   * 1. **废弃阶段风险评估**

　　废弃阶段风险评估应包含以下方面：

1. 应确保硬件和软件等资产及残留信息得到了适当的处置，并确保系统组件被合理地丢弃或更换；
2. 若被废弃的系统是某个系统的一部分，或与其他系统存在物理或逻辑上的连接，还应考虑系统废弃后与其他系统的连接是否被关闭；
3. 若在系统变更中废弃，除对废弃部分外，还应对变更的部分进行评估，以确定是否会增加风险或引入新的风险；
4. 是否建立了流程，应确保更新过程在一个安全、系统化的状态下完成。
   1. **安全检测**
      1. **网络安全检查**

　　网络安全检查应包含以下方面：

1. 网络安全脆弱性是指网络通信设备及网络安全设备、网络通信线路、网络通信服务在安全方面存在的脆弱性，包括：非法使用网络资源、非法访问或控制网络通信设备及网络安全设备、非法占用网络通信信道、网络通信服务带宽和质量不能保证、网络线路泄密、传播非法信息等。
2. 核查网络安全所采取的安全措施及其有效性，包括：网络拓扑图、VLAN划分、网络访问控制、网络设备防护、安全审计、边界完整性检查、入侵防范、恶意代码防范等。
3. 网络安全脆弱性核查应该进行结构、功能、安全功能分析和性能分析；可采取白盒测试、黑盒测试、灰盒测试等方法。
4. 网络安全脆弱性核查方法包括：查看网络拓扑图、网络安全设备的安全策略，配置等相关文档，询问相关人员，查看网络设备的硬件配置情况，手工或自动查看或检测网络设备的软件安装和配置情况，查看和验证身份鉴别、访问控制、安全审计等安全功能，检查分析网络和安全设备日志记录，利用工具探测网络拓扑结构，扫描网络安全设备存在的漏洞，探测网络非法接入或外联情况，测试网络流量、网络设备负荷承载能力以及网络带宽，手工或自动查看和检测安全措施的使用情况并验证其有效性等。
   * 1. **主机安全检查**

　　主机安全检查应包含以下方面：

1. 主机系统安全脆弱性是指主机硬件设备、操作系统、数据库系统以及其他相关软件在安全方面存在的脆弱性，包括：非法访问或控制操作系统、数据库系统以及其他相关软件系统，非法占用网络或系统资源等；
2. 核查主机系统所采取的安全措施及其有效性，包括：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制等；
3. 主机系统安全脆弱性核查应该进行结构、功能、安全功能和性能分析；可采取白盒测试、黑盒测试、灰盒测试等方法；
4. 主机系统安全脆弱性核查方法包括：手工或自动查看或检测主机硬件设备的配置情况以及软件系统的安装配置情况，查看软件系统的自启动和运行情况，查看和验证身份鉴别、访问控制、安全审计等安全功能，查看并分析主机系统运行产生的历史数据（如鉴别信息、上网痕迹），检查并分析软件系统日志记录，利用工具扫描主机系统存在的漏洞，测试主机系统的性能，手工或自动查看或检测安全措施的使用情况并验证其有效性等。
   * 1. **应用安全检查**

　　应用安全检查应包含以下方面：

1. 应用系统安全脆弱性是指应用系统在安全方面存在的脆弱性，包括；非法访问或控制业务应用系统，非法占用业务应用系统资源等；
2. 核查应用系统所采取的安全措施及其有效性，包括：身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等；
3. 应用系统安全脆弱性核查应进行结构、功能、安全功能和性能分析；
4. 应用系统安全脆弱性核查可采取白盒测试、黑盒测试、灰盒测试等方法；
5. 软件安全技术要求可参见附录B。
   * 1. **数据安全检查**

　　数据安全检查应包含以下方面：

1. 数据安全脆弱性是指数据存储和传播在安全方面存在的脆弱性，包括：数据泄露、数据篡改和破坏、数据不可用等。
2. 核查数据安全所采取的安全措施及其有效性，包括：数据完整性保护措施、数据保密性保护措施、备份和恢复等。
3. 数据安全核查宜采用通信协议分析、数据破解、数据完整性校验等方法。

**附录A  
（资料性）  
数据脱敏常用技术**

**A.**1**泛化技术**

泛化是指在保留原始数据局部特征的前提下使用一般值替代原始数据，泛化后的数据具有不可逆性，具体的技术方法包括：

1. 数据截断：直接舍弃业务不需要的信息，仅保留部分关键信息，例如将手机号码1350001000截断为135；
2. 日期偏移取整：按照一定粒度对时间进行向上或向下偏移取整，可在保证时间数据一定分布特征的情况下隐藏原始时间，例如将时间20150101 01：01：09按照5秒钟粒度向下取整得20150101 01：01：05；
3. 规整：将数据按照大小规整到预定义的多个档位，例如将客户资产按照规模分为高、中、低三个级别，将客户资产数据用这三个级别代替。

**A.**2**抑制技术**

抑制是指通过隐藏数据中部分信息的方式来对原始数据的值进行转换，又称为隐藏技术，具体的技术方法包括：

1. 掩码：用通用字符替换原始数据中的部分信息，例如将手机号码13500010001经过掩码得到135\*\*\*\*0001，掩码后的数据长度与原始数据一样。

**A.**3**扰乱技术**

扰乱是指通过加入噪声的方式对原始数据进行干扰，以实现对原始数据的扭曲、改变，扰乱后的数据仍保留着原始数据的分布特征，具体的技术方法包括：

1. 加密：使用加密算法对原始数据进行加密，例如将编号12345加密为abcde；
2. 重排：将原始数据按照特定的规则进行重新排列，例如将序号12345重排为54321；
3. 替换：按照特定规则对原始数据进行替换，如统一将女性性别替换为F；
4. 重写：参考原数据的特征，重新生成数据。重写与整体替换较为类似，但替换后的数据与原始数据通常存在特定规则的映射关系，而重写生成的数据与原始数据则一般不具有映射关系。例如对雇员工资，可使用在一定范围内随机生成的方式重新构造数据；
5. 均化：针对数值性的敏感数据，在保证脱敏后数据集总值或平均值与原数据集相同的情况下，改变数值的原始值；
6. 散列：即对原始数据取散列值，使用散列值来代替原始数据。

**A**.4**有损技术**

有损是指通过损失部分数据的方式来保护整个敏感数据集，适用于数据集的全部数据汇总后才构成敏感信息的场景，具体的技术方法包括：

1. 限制返回行数：仅仅返回可用数据集合中一定行数的数据，例如商品配方数据，只有在拿到所有配方数据后才具有意义，可在脱敏时仅返回一行数据；
2. 限制返回列数：仅仅返回可用数据集合中一定列数的数据，例如在查询人员基本信息时，对于某些敏感列，不包含在返回的数据集中。

**附录B  
（资料性）** **软件安全技术要求**

**B**.1 **软件开始阶段**  
软件开始阶段的安全技术要求应包含如下要素：

1. 详细说明相应安全等级的应用软件系统的保密性、完整性和可用性指标；
2. 详细说明应用软件系统中需要保护的用户资产；
3. 完成初步的应用软件系统风险评估；
4. 详细说明应用软件系统安全应采用的整体安全策略。

**B**.2 **软件获得或开发阶段**软件获得或开发阶段的安全技术要求应包含如下要素：

1. 选择并确定相应安全等级的应用软件系统的安全技术要求；
2. 自主开发的应用软件，应按照确定的安全技术要求进行安全设计和实现；
3. 获得的应用软件，应确认其满足所确定的安全技术要求；
4. 自主开发的应用软件，应对其开发和运行中的安全附加开销和性能进行分析，并对成本和风险进行折中平衡；
5. 获得的应用软件，应对其运行中安全附加开销和性能进行分析，确认其成本和风险符合折中平衡的要求。

**B**.3 **软件实现和评估阶段**软件实现和评估阶段的安全技术要求应包含如下要素：

1. 编程语言、编译器和程序库应按照确定的满足相应安全等级要求的安全准则进行鉴定；
2. 应用程序的代码应被检验，以确保保密性、完整性和可用性目标已经达到，并且安全性没有降低；
3. 测试软件成分和评估一个系统需要一个静态方法的组合（例如，按照适当选择的设想测试软件和固件）；
4. 软件部件的安全测试和分布式软件的安全测试是关键性的开发活动之一；
5. 对高等级的应用软件系统，应使用形式化方法对应用软件的安全设计进行验证；
6. 通过测试与评估确认应用软件的安全性是否达到所确定的安全技术要求，对于未达到安全技术要求的，应从应用软件获得或开发阶段重新开始开展工作。

**B**.4 **软件运行和维护阶段**软件运行和维护阶段的安全技术要求应包含以下方面：

1. 按照相关文档的操作说明和所确定的操作规程，进行应用软件系统安全机制的配置和操作；
2. 定期或根据情况的变化及时进行应用软件系统安全性评估，并在必要时对安全性要求进行重新定义和设计，形成新的修订版本；
3. 对应用软件系统的修订版本进行严格的测试和必要的控制，确认其达到新目标的要求，且未产生不良影响。

**B**.5**软件结束和处置阶段**软件结束和处置阶段的安全技术要求应包含以下方面：

1. 对于结束运行的应用软件，应进行认真处置，确保该软件系统在结束运行后，不会带来安全相关问题；
2. 对于信息系统中所有与该应用软件系统相关的程序和数据信息均应进行妥善处理，除了根据信息系统的需要保留一些与业务应用无关的数据信息（如用户名和标识）以外，信息系统中不应有与该应用软件的业务有关的残留信息；
3. 对于该应用软件系统运行过程中使用过的可移动的记录介质，应进行记录内容的消除，并应确保介质中无任何与该应用软件相关的残留信息。

**参考文献**

1. GB 17859-1999　计算机信息系统安全保护等级划分准则
2. GB/T 18336.1-2015　信息技术　安全技术　信息技术安全评估准则
3. GB/T 20269-2006　信息安全技术　信息系统安全管理要求
4. GB/T 20271-2006　信息安全技术　信息系统通用安全技术要求
5. GB/T 20984-2007　信息安全技术　信息安全风险评估规范
6. GB/T 20985.1-2017　信息技术　安全技术　信息安全事件管理　第1部分：事件管理原理
7. GB/T 22239-2019　信息安全技术　网络安全等级保护基本要求
8. GB/T 22240-2020　信息安全技术　网络安全保护定级指南
9. GB/T 25058-2020　信息安全技术　网络安全等级保护实施指南
10. GB/T 37964-2019　信息安全技术　个人信息去标识化指南
11. GB/T 37971-2019　信息安全技术　智慧城市安全体系框架
12. GB/Z 38649-2020　信息安全技术　智慧城市建设信息安全保障指南
13. GA/T 708-2007　信息安全技术　信息系统安全等级保护体系框架
14. GA/T 709-2007　信息安全技术　信息系统安全等级保护基本模型
15. GA/T 710-2007　信息安全技术　信息系统安全等级保护基本配置
16. CJJ/T 157-2010　城市三维建模技术规范