FICS 35.040
L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术
智慧城市建设信息安全保障指南

Information security technology-

Guide of information security assurance framework for Smart City

（征求意见稿）

2017-5

- XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　　言

本标准按照GB/T 1.1-2009给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：浙江省经济信息中心、中国电子技术标准化研究院、中国信息安全测评中心、中国管理科学研究院、中电海康集团、中电长城网际系统应用有限公司、西南科技大学、浙江省标准化研究院、浙江省电子产品检验所、陕西省网络与信息安全测评中心、杭州安恒信息技术有限公司、北京匡恩网络科技有限责任公司、浙江省发展信息安全测评技术有限公司、新华三技术有限公司、北京天融信科技有限公司、杭州奕锐电子有限公司、北京易恒信认证科技有限公司、四川万和智联科技有限公司、成都腾甲数据服务有限公司等。

本标准主要起草人：。

引　言

智慧城市建设是一项复杂的大型系统工程，其安全问题尤显重要，为推进在我国智慧城市建设，需要针对智慧信息技术的安全风险分析基础上，提出信息安全管理和技术保障要求，特制定本指导性技术文件。

本指导性技术文件确立了智慧城市安全框架，给出智慧城市建设全过程信息安全保障管理要求及体系规范，着重给出了针对智慧信息技术特征的安全保障技术要求。

本指南用于政府部门或项目单位，有助于信息安全主管部门为智慧城市建设、运营使用、运维服务等相关单位明确智慧城市建设全生命周期各阶段的信息安全保障要求与责任提供指导，确保智慧城市建设运营主体各方的权益、运营秩序和信息安全，增强抵御风险和自主可控的能力。同时可为智慧城市管理、工程技术及第三方服务等相关人员提供管理和技术参考。

信息安全技术 智慧城市建设信息安全保障指南

1 范围

本指南确立了智慧城市建设全过程的信息安全保障体系，包括智慧城市建设从规划与需求分析、勘察设计、实施施工、检测验收、运营维护、监督检查与评估到优化与持续改进的全过程信息安全保障的管理机制与技术规范指南。在全面落实已有信息化建设安全标准规范的基础上，针对云计算、物联网、移动互联网、大数据等智慧城市信息技术，制定信息安全保障管理规范与技术规范框架。

本指南适用于智慧城市管理、建设、运营及运维单位，为智慧城市建设管理人员、工程技术人员等相关人员进行信息安全设计、建设及运维提供管理和技术参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 25069-2010 信息安全技术 术语

GB/T AAAAA—XXXX 智慧城市 术语

GB/T BBBBB—XXXX 智慧城市 技术参考模型

GB/T 20269-2006 信息安全技术 信息系统安全管理要求

GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240-2008 信息系统安全等级保护定级指南

GB/T 18019-1999 信息技术 包过滤防火墙安全技术要求

GB/T 18020-1999 信息技术 应用级防火墙安全技术要求

GB/T 20010-2005 信息安全技术 包过滤防火墙评估准则

GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法

GB/T 20278-2006 信息安全技术 网络脆弱性扫描产品技术要求

GB/T 26268-2010 网络入侵检测系统测试方法

GB/T 26269-2010 网络入侵检测系统技术要求

GB/T 20280-2006 信息安全技术 网络脆弱性扫描产品测试评价方法

GB/T 20281-2006 信息安全技术 防火墙技术要求和测试评价方法

GB/T 28451-2012 信息安全技术 网络型入侵防御产品技术要求和测试评价方法

GB/T 20945-2013 信息安全技术 信息系统安全审计产品技术要求和测试评价方法

GB/T 31167-2014 信息安全技术 云计算服务安全指南

GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

ISO/IEC 27037-2012 数字证据识别、收集、获取和保存指南

ISO/IEC27042 数字证据分析和解释指南

ISO/IEC27032-2012 信息技术 安全技术 网络安全指南

ISO/ IEC TR 15443-2012 信息技术 安全技术 安全保障框架

3 术语和定义

3.1

智慧城市 Smart City

智慧城市是一种城市建设发展的形态，通过利用新一代的信息技术，促进城市中信息空间、物理空间和社会空间的融合，并通过丰富的应用系统，加速城市经济发展、提高政府及公共服务的效率、方便市民的工作生活、有效地保护和利用环境，实现经济、社会、环境和谐发展。

[注：引自GB/T AAAAA—XXXX《智慧城市 技术参考模型》，定义3.1]

3.2

安全域 security domain

网络安全域是指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，且相同的网络安全域共享一样的安全策略。广义可理解为具有相同业务要求和安全要求的 IT 系统要素的集合。

3.3

安全区域边界 secure area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

3.4

虚拟机 Virtual Machine（VM）

虚拟机是指通过软件实现的主机运行环境，包括虚拟化硬件、操作系统、中间件和应用程序。

3.5

多租户技术（或称多重租赁技术）， multi-tenancy technology

是一种软件架构技术，它是在探讨与实现如何于多用户的环境下共用相同的系统或程序组件，并且仍可确保各用户间数据的隔离性。

3.6

多租户隔离 multi-tenancy isolation

在多租户的典型应用环境下，可以通过物理隔离、虚拟化和应用支持的多租户架构等三种方案实现不同租户之间数据和配置的安全隔离，以保证每个租户数据的安全与隐私。

4 缩略语

下列缩略语适用于本文件。

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

DoS：拒绝服务攻击（Denial Of Service）

IPSec：IP安全协议（Internet Protocol Security protocol）

TLS：安全传输层协议（Transport Layer Security）

VPN：虚拟专用网（Virtual Private Network）

5 概述

5.1 智慧城市整体架构

智慧城市技术参考模型如图5.1所示。

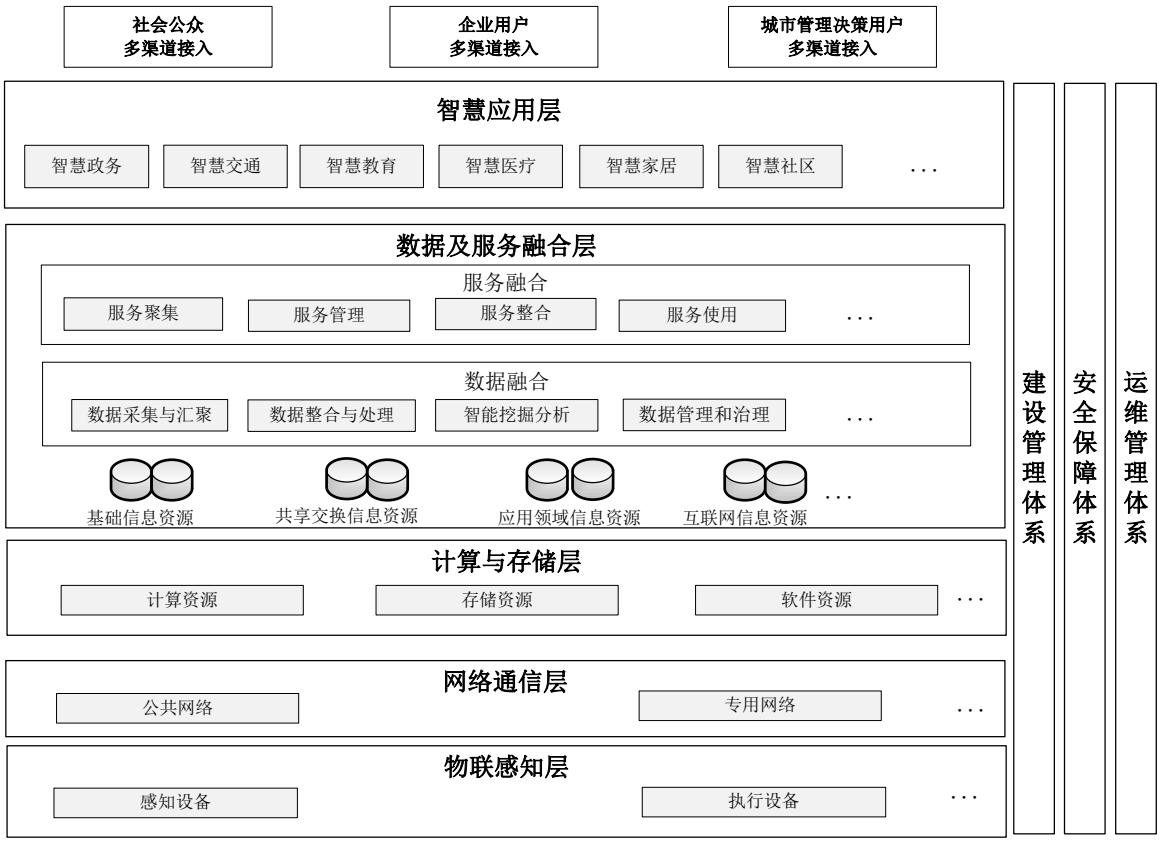


图 5.1　智慧城市技术参考模型

a)　物联感知层：提供对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、建筑、安全等方面的识别、信息采集、监测和控制；

b)　网络通信层：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（如：移动互联网），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；

c)　计算与存储层：包括软件资源、计算资源和存储资源，为智慧城市提供数据存储和计算以及相关软件环境的资源，保障上层对于数据的相关需求；

d)　数据及服务融合层：通过数据和服务的融合支撑，承载智慧应用层中的相关应用，提供应用所需的各种服务，为构建上层各类智慧应用提供支撑，本层处于智慧城市总体参考模型的中上层，具有重要的承上启下的作用；

e)　智慧应用层：在物联感知层、网络通信层、计算与存储层、数据及服务融合层之上建立的各种基于行业或领域的智慧应用及应用整合，如智慧政务、智慧交通、智慧公共服务、智慧医疗、智慧园区、智慧社区、智慧旅游等，为社会公众、企业用户、城市管理决策用户等提供整体的信息化应用和服务；

f)　安全保障体系：为智慧城市构建统一的安全平台，实现统一入口、统一认证、统一授权、日志记录，涉及各横向层次；

g)　运维管理体系：为智慧城市提供整体的运维管理机制，涉及各横向层次，确保智慧城市整体的建设管理和长效运行；

h)　建设管理体系：为智慧城市建设提供整体的建设管理要求，加强智慧城市建设管理机制，指导智慧城市相关建设，确保智慧城市建设的科学性和合理性。

5.2　智慧城市的主要特征

智慧城市是运用物联网、云计算、大数据、空间地理信息集成等新一代信息技术，促进

城市规划、建设、管理和服务智慧化的新理念和新模式。是新一代信息技术创新应用与城市转型发展深度融合的产物，是推动政府职能转变、推进社会管理创新的新手段和新方法，是城市走向绿色、低碳、可持续发展的本质需求。

智慧城市的基础是推进实体基础设施和信息基础设施相融合、构建城市智能基础设施；主线是推进物联网、云计算、大数据、移动互联网、空间地理信息集成等新一代信息技术应用与城市经济社会发展的深度融合；其核心是最大限度地开发、整合、融合、共享和利用各类城市信息资源，构建城市规划、建设、管理和服务的智慧化体系；主要手段包括为居民、企业和社会提供及时、高效、智能的信息服务等；其宗旨是实现城市规划管理信息化、基础设施智能化、公共服务便捷化、产业发展现代化、社会治理精细化。

智慧城市具有以下主要特征：

a) 复杂巨系统。智慧城市是一个要素复杂、应用多样、相互作用、不断演化的综合性复杂系统。通过将功能完全不同的系统互连在一起形成的“系统的系统”，其复杂度将随着构成系统的增加而呈指数增加。

b) 资源集中与大数据融合。云计算 IT 资源的集中化促进资源共用、提高资源伸缩性。按照城市经济社会发展需求，实现相关部门、行业、群体、系统之间的数据融合、信息共享，形成海量数据。社会信息高度集中也将带来巨大的潜在风险。

c) 泛在接入与全面感知。智慧城市通过感知技术，对人、物的相关信息进行全面的感知与互联，形成城市智慧的泛在信息源。机构和个人通过标准接入机制，利用手持设备、传感器、移动电话、平板、机顶盒等各种终端、物联网互联感知设备通过网络随时随地使用智慧城市服务。

d) 协同运作与多安全域。城市中的各个主体之间利用智慧技术实现互连互通，彼此之间实现实时感知，及时传递信息，迅速做出反应。除少数涉及秘密信息的领域之外，大多数信息系统都将是一种开放的协同系统。智慧城市要解决跨部门、跨区域、跨系统的问题，构建跨越不同安全域之间的智能化管理与服务系统。因此，解决不同安全域之间的互联是重点。

e) 移动化和开放性。随着泛载网络和手持终端的普及应用，移动化成为智慧城市的重要特征。智慧城市中广泛应用无线技术，如物联网感知层的电子标签，由于受成本等的限制，未采用很强的密码机制，电子标签内部数据容易被破解。同时，众多机构通过 VPN 等方式将机构网络建构在公共网络之上。开放性导致安全风险增加。

f) 高渗透与个人隐私。物联网、无线宽带网等网络规模大大增加，人们使用网络的时间和位置限制被突破；新的智慧应用让普通民众主动地参与信息创造和发布以及网络运转的其它环节，因此，智慧城市对人类社会的渗透水平大大提升。同时，智慧城市建设以人为本，涉及隐私数据，包括个人基本信息、个人偏好、个人位置及个人行为数据等。高渗透造成个人隐私保护风险剧增。

5.3 智慧城市风险分析

a) 智慧城市的复杂性导致脆弱性成倍增加。智慧城市是由众多传统市政应用和市政服务应用互连构成的复杂系统。除了原先系统的脆弱性外，系统间互连带来了更多的新的安全挑战。

b) 虚拟化导致安全边界模糊。云计算的核心是虚拟化，而虚拟化将模糊系统间的边界。如果一个系统被攻破，可能发生雪崩效应，使得更多的虚机遭入侵，从而造成灾难性后果。

c) 智慧城市需要跨部门、跨机构和跨系统进行数据移动和数据融合，这将极大地增加数据管理的难度，导致数据在移动和存储过程中数据泄露的可能性。

d) 更多隐私信息的收集与分散存储，使得隐私数据保护更加困难。智慧城市各个构成

系统都根据需要，收集并存储不同的与个人相关的信息。这种分散收集与存储使得个人隐私泄露的风险极大提升。

e) 用户群安全意识与知识水平的差异，使得敏感信息更易泄露。市民作为智慧城市的使用群体，安全意识、知识水平千差万别，非常容易成为攻击者的突破口，是智慧城市极大的脆弱点。

f) 散布城市的采集设备（传感器），可能成为攻击智慧城市的另一类攻击点。智慧城市有一个庞大的传感层，它们负责采集并上传城市的运行数据。由于这些采集设备（传感器）缺乏有效的物理保护，极容易成为攻击者攻击智慧城市的通道。

5.4 智慧城市建设安全框架

智慧城市建设信息安全保障依赖于信息安全，应用安全，网络安全，互联网安全和关键信息基础设施防护。智慧城市建设安全保障包含但不仅限与互联网安全、网络安全、应用安全、信息安全、关键基础设施保护。它有一个独特的范围，要求利益相关者发挥积极的作用，以保持和提高智慧城市系统的实用性和可信性。在智慧城市建设中的利益相关者必须发挥积极的作用，相对于传统意义上仅需保护自身所属资产，在智慧城市建设中需要超越，以提高智慧城市建设的应用效能。智慧城市的应用范围超越原有城市管理模式，发展成为一种多对多的业务服务和相互作用模式，要求个人和组织准备解决新出现的安全风险和挑战，有效防范和应对系统误操作以及网络犯罪的发展。

为了处理智慧城市建设安全保障问题，需要不同的组织专有和公共实体之间的实质性的沟通和协调。因此需要一个基于信息共享和发布或事件协作的基本框架，去为智慧城市建设利益相关者打破隔离提供足够的安全保障。图 5.2 说明了这些概念和关系。

维护智慧城市资产权益是对那些对智慧城市资产的价值关注的利益相关者的责任。实际或假定的威胁载体也可能对智慧城市资产的价值关注，并寻求与利益相关者的利益相反的方式滥用资产。

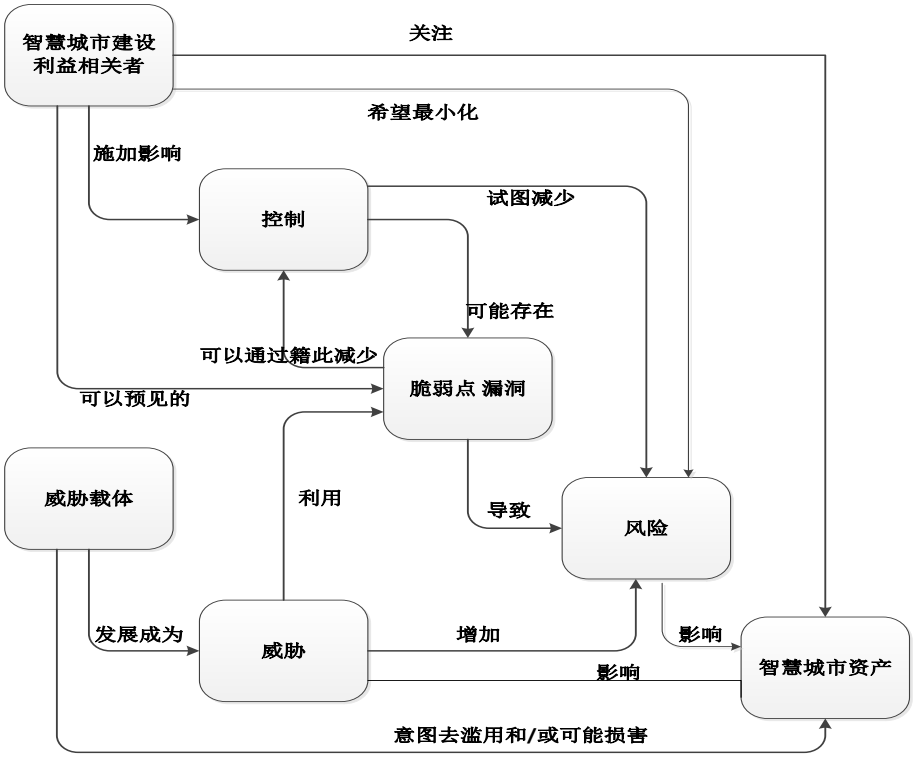


图 5.2 智慧城市建设信息安全概念及其之间的关系框架示意图

智慧城市建设利益相关者在将他们的资产暴露在确定的威胁之前，需要确信控制是足够应对资产威胁的。利益相关者本身可能不具备判断控制的所有方面的能力，因此可以寻求使用外部组织的控制评价。

据此提出智慧城市安全体系框架如图 5.3 所示，包括安全战略、安全技术、安全管理和安全建设运营以及安全基础支持等方面保障。

图 5.3 智慧城市安全体系框架

6 智慧城市建设安全保障机制

6.1 智慧城市安全体系建设主要角色与责任划分

a） 政府主管部门。作为智慧城市决策者和管理协调者，负责智慧城市建设和发展的规划和监管，协调、指导智慧城市建设信息安全保障工作。

b) 规划设计咨询机构。整个智慧城市安全体系建设中承担智慧城市前期规划设计与后期跟踪咨询服务。

c） 智慧城市应用提供商。作为智慧城市服务提供者，为智慧城市开发应用，应保证智慧城市应用符合本标准的安全运维和安全管理要求。

d） 集成商。作为智慧城市建设者，在政府的授权下，负责智慧城市建设。应保证智慧城市建设过程符合指南的安全要求。

e） 智慧城市服务运营商。在政府的监管下，负责智慧城市运营，并保障智慧城市安全。必需有信息安全专业人员承担智慧城市运营安全保障岗位。

f） 第三方安全评估机构。对智慧城市安全体系和应用安全性开展独立的评估。智慧城市风险评估方法和流程见附录 A。

g） 智慧城市服务使用者。依据国家法律法规、政策文件及标准规范，合理使用或应用智慧城市服务运营商提供的应用和服务，以及向智慧城市服务运营商反馈合理的需求诉求。

6.2 责任人机制

智慧城市项目建设单位应指定项目信息安全保障第一责任人；建设项目应及时向信息化主管部门备案；贯彻执行相关法规和技术标准，落实信息化主管部门的要求，编制信息安全保障等相关内容并履行。

6.3 追溯查证机制

智慧城市是一个面向公众提供服务的信息化平台，因此应建立安全取证机制，建立全流程有效的责任追溯查证体系，明确各环节的主体责任，制定信息系统安全保障岗位责任制度，并监督落实。

a）智慧城市各系统应详细记录用户的活动信息，包括时间、地点、操作和操作结果，以建立取证的数据基础。

b）应建立智慧城市调查与取证体系，包括软硬件系统和符合法律的取证过程，以对存在的违法入侵进行快速而有效的调查和取证。

c）应保证证据数据在调查和取证过程数据不被改变和删除。具体措施可以参考ISO/IEC 27037:2012《数字证据识别、收集、获取和保存指南》、ISO/IEC27042《数字证据分析和解释指南》。

6.4 监督检查机制

信息系统的安全保障监督管理由信息安全监管相关职能部门，通过备案、检查、督促整改等方式，对建设项目的信息安全保护工作进行指导监督；

信息化主管部门应会同行业主管或监管部门，以及其他信息安全管理部门，定期对建设项目进行全面的安全检查，排查安全隐患，堵塞安全漏洞，通报发现问题并敦促整改。

项目建设和运营单位对抽查、抽检发现的问题，应认真落实整改意见，并在规定期限向信息化主管部门报告整改情况。

6.5 应急预案演练与处理机制

参照 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》，结合实际业务情况，确定不同级别的具体量化指标，以此指导信息安全故障等级的定级。制定应急预案，包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。定期对应急预案进行演练。随着信息系统的变更应定期对原有的应急预案重新评估，修订完善。安全故障发生时，按应急处理程序处置，及时向主管部门报告项目信息系统发生的重大系统事故或突发事件，并按有关预案快速响应。

6.6 服务外包安全责任机制

安全服务商的选择符合国家的有关规定；与选定的安全服务商签订与安全相关的协议，明确约定相关责任；确保选定的安全服务商提供技术支持和服务承诺，必要的与其签订服务合同。严格管理信息技术服务外包的安全，确保提供服务的数据中心、云计算服务平台等设在境内。

6.7 信息安全保障教育培训机制

制定安全教育和培训计划，对各类人员进行信息安全意识教育和相关信息安全技术培训；建立信息系统安全保障的专业队伍，适应信息智慧技术的发展。

7 智慧城市建设全过程安全保障管理要求

遵循《GB/T 20269-2006 信息安全技术 信息系统安全管理要求》基础上，智慧城市建设信息安全保障根据其特征要求严格全流程信息安全管理，要求加强要害信息设施和信息资源安全防护，包括加大对党政军、金融、能源、交通、电信、公共安全、公用事业等重要信息系统和涉密信息系统的安全防护，确保安全可控。重要系统与网络安全设施，要同步设

计、同步建设、同步管理。

在智慧城市建设的重要信息系统设计阶段，要加强安全风险论证工作，合理确定安全保护等级，同步设计安全防护方案。重点提高网络管理、态势预警、应急处理和信任服务能力。

在实施阶段，要以制度和规范形式，加强对技术、设备和服务提供商的安全审查，同步建设安全防护手段。

在运行阶段，建立重要信息使用管理和安全评价机制。要加强落实个人信息保护。定期开展检查、等级评测和风险评估，认真排查安全风险隐患，增强日常监测和应急响应处置恢复能力。

7.1 政策制定与审查监督

主管部门提出信息安全保障的基本管理政策和工作要求；负责协调、指导智慧城市建设信息安全保障工作；对各智慧城市建设项目的主管、运营、使用单位所开展的信息安全保障实施情况进行监督检查。

明确智慧城市政府及有关部门负责人、要害信息系统运营单位负责人的网络信息安全责任，建立责任追究机制。智慧城市建设项目各相关单位，按照“谁主管、谁负责，谁运营、谁负责”的要求落实信息安全责任，按照“自主审查”和“主管部门审查”的程序开展审查。主管部门在立项环节进行信息安全联合审查，在验收环节进行信息安全专项审查；对信息安全自主审查工作，定期组织监督审查。智慧城市建设项目信息安全审核要求见附录F。

7.2 信息安全保障规划

智慧城市安全管理应进行整体规划，遵循国家和行业现有的且适合于智慧城市安全的法律、法规、政策、标准规范，建立与智慧城市战略目标相一致的信息安全总体方针，提出全局性、方向性和系统性的规划要求，明确智慧城市安全保障的目标和重点关注领域，分析智慧城市安全方面存在的安全威胁与隐患，加强要害信息设施和信息资源安全防护，包括加大对党政军、金融、能源、交通、电信、公共安全、公用事业等重要信息系统和涉密信息系统的安全防护，确保安全可控；统筹规划容灾备份体系，推行联合灾备和异地灾备；建立重要信息使用管理和安全评价机制；严格落实国家有关法律法规及标准，加强行业和企业自律，切实落实个人信息保护。规划并开展智慧城市安全管理、运维、审核、验收及改进审核标准工作，建立有效的安全风险评估机制。

7.3 信息安全保障需求分析

智慧城市建设信息安全保障需求不能靠传统消极被动的封堵查杀，而是要根据智慧城市的技术特征，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。通过分析所建智慧信息系统的安全保护等级，经过主管部门的论证，并报相关行政主管部门审核、备案；根据信息系统的安全保护等级，判断智慧信息系统现有的安全保护水平与等级保护管理规范和技术标准之间的差距，提出系统的基本安全保护需求；根据安全目标，分析系统运行环境、潜在威胁、资产重要性、脆弱性等，提出补充安全保护需求。

7.4 信息系统安全保障设计

构建可信智慧城市的系统框架，云计算、物联网、大数据、移动互联网、虚拟动态异构计算环境需要可信度量、识别和控制，设计达到体系结构可信、操作行为可信、资源配置可信、数据存储可信、策略管理可信。根据可信系统总体安全方案中要求实现的安全策略、安全技术体系结构、安全措施和要求落实到产品功能或物理形态上，提出能够实现的产品或组件及其具体规范，使得在信息安全产品采购和安全控制开发阶段具有依据；同时，要加强安全风险论证工作，合理确定安全保护等级，同步设计安全防护方案，将总体方案中管理部分

相适应的内容落实，以保证安全技术建设的同时，安全管理的同步建设。最后，将技术措施落实方案、管理措施落实方案汇总，同时考虑工时和费用，最后形成指导安全实施的指导性文件。信息安全建设内容编制要求见附录D。

7.5 信息系统实施安全保障

建立配套的安全管理职能部门，通过管理机构的岗位设置、人员的分工以及各种资源的配备，为信息系统的安全管理提供组织上的保障。

以制度和规范形式，加强对技术、设备和服务提供商的安全审查，同步建设安全防护手段。密码产品采购和使用符合国家密码主管部门的要求；指定或授权专门的部门负责产品的采购；对安全相关产品实行分级管理，确保其安全功能符合相应安全等级的要求；对已有技术信息安全产品，应依据相关标准规范要求，进行安全符合性查验；对新技术相关产品进行安全测评，使其符合系统基本要求保障需求。

自行软件开发环境与实际运行环境物理分开；制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；提供软件设计的相关文档和使用指南，并由专人负责保管。外包软件开发应根据开发要求检测软件质量；提供软件设计的相关文档和使用指南；在软件安装之前检测软件包中可能存在的恶意代码；要求开发单位提供软件源代码，并审查软件中可能存在的后门。

信息系统运行前的系统审阅应关注信息系统的安全控制、权限设置的正确性、连贯性、完整性、可审计性和及时性等内容；在试运行期间，应对信息系统开发过程中所提交的有关文档资料进行评估，指出其中存在的风险，了解是否具有相应的控制措施，并提出评价和建议的过程；明确系统上线前应进行测试和检查，从而确定系统是否满足项目建设、实施规范的要求。

对人员的职责、素质、技能等方面进行培训，保证人员具有与其岗位职责相适应的技术能力和管理能力，以减少人为因素给系统带来的安全风险。

7.6 信息系统安全检测验收

通过专业化、社会化的信息安全认证服务，为保障智慧城市网络信息安全提供支持。在验收前委托具备资质的第三方测试单位对系统进行代码安全性检测，渗透测试和风险评估，并出具安全测评报告;组织相关部门和相关人员对系统安全测评报告进行审定,并签字确认。

制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

对系统控制方法和人员行为准则进行书面规定。

对系统实现的风险控制措施进行评估判断，针对存在的不可接受风险项，需要制定风险处理计划并采取新的安全措施降低、控制风险。

7.7 信息系统运行维护安全保障

建设或修订与信息系统安全管理相配套的行为规范和操作规程，包括但不限于：

a） 机房安全管理制度，对有关机房物理访问，物品带进、带出机房和环境安全等方面的管理作出规定。

b） 资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

c） 介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定。

d） 基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。

e） 网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与补丁、口令更新周期等方面作出规定。

f） 系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程方面作出规定。

g） 个人桌面终端安全管理制度，对个人桌面终端操作系统、周边硬件、通信设备、应用系统的安全使用作出规定。

定期检查安全管理制度的落实情况，确保安全管理制度落实，并不断优化管理制度，使其更加符合单位的实际情况。

定期开展检查、等级评测和风险评估，排查安全风险隐患，增强日常监测和应急响应处置恢复能力。定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并向相关主管部门备案，并采取必要的应对措施。制定安全事件处置预案，结合信息系统的实际情况，分析安全事件对信息系统的破坏程度，所造成后果严重程度，将安全事件依次进行分级，按照分级情况进行处置。

7.8 信息安全保障优化与持续改进

定期对系统进行安全测评，对发现的安全问题进行及时分类处置。系统变更后需评估变更后的部分对系统造成的安全影响。在信息系统正常运行一段时间后进行评估，旨在评估对信息系统各项风险的控制是否恰当，能否实现预定的设计目标。

8 智慧城市建设信息安全保障技术要求

8.1 计算环境安全要求

a）智慧城市系统相关服务器、网络设备、安全设备、终端的物理安全及机房安全应遵循《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）中物理安全部分的安全控制项要求。应对重要设备的安全状态、安全配置和安全状态等进行严格的监控与检测。

b）智慧城市系统相关服务器的操作系统、数据库管理系统应遵循《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）对应安全保护等级中主机安全部分的安全控制项要求，必须覆盖身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制等控制项要求。

c）虚拟机需能提供有效的资源隔离，包括计算隔离、存储隔离、网络隔离，保证不同虚拟机之间的虚拟CPU指令隔离，能隔离不同虚拟机的内存空间、外部存储空间，能提供虚拟网络（vLAN）划分等功能实现虚拟机在网络层面的隔离，提供虚拟机故障屏蔽功能，确保某个虚拟机崩溃后不影响及其它虚拟机。

d）应提供虚拟机资源控制，应对虚拟资源按照策略做统一管理调度与分配，通过技术手段对虚拟机的运行状态、资源占用、迁移等信息进行监控；应提供对虚拟机间网络的流量监控的功能，多租户环境下，针对每个租户的虚拟化安全资源进行诸如CPU/内存，吞吐量、最大并发连接数等参数的限制;通过设定终端接入方式、访问域的范围等条件限制终端登录；应具有计算资源负载均衡能力，保证在业务高峰时虚拟机之间可以根据业务需要线性伸缩。

e）虚拟机监控平台需能提供有效的身份鉴别，采用两种或以上组合的鉴别技术进行身份鉴别；提供访问控制功能，依据安全策略控制管理用户对虚拟资源的访问；提供可信执行保护，实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并采用可信计算等技术在检测到其完整性受到破坏时采取措施恢复；提供入侵防范，应能够检测和记录对虚拟机、虚拟机监控器进行攻击、入侵的行为并提供报警。

f）虚拟机审计范围应覆盖到虚拟化组件的每个用户，审计内容应包括重要用户行为、虚拟机间迁移、虚拟资源调度、虚拟资源分配、虚拟资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，应保护虚拟资源审计进程，避免受到未预期的中断。

8.2 通信网络安全要求

a）应遵循《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）对应安全保护等级中网络安全部分的安全控制项要求，必须覆盖结构安全、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、网络设备防护等控制项要求。

b）应从区域边界访问控制、区域边界包过滤、区域边界安全审计以及区域边界完整性保护几个方面采取措施保护虚拟边界的安全。安全区域边界应设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。应在安全区域边界设置包过滤，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。各个安全域间通信应设置审计机制，由安全管理中心管理，并对确认的违规行为及时报警。安全域划分与管理见附件C。

c）根据数据信息的存储和处理所涉及的范围确定智慧城市网络的安全计算域，并制定确定相应的安全保护等级，根据安全保护等级确定具体防护措施。

d）智慧城市网络应具备网络性能保护机制，防止对网络资源的滥用，确保网络资源的合理使用，防范拒绝服务攻击。

e）应采取数据加密、信道加密等措施加强无线网络及其他信道的安全，防止敏感数据泄漏，同时采取措施保证传输数据的完整性。无线技术安全要求见附录J。

f）应支持SSL/TLS或IPSec等网络安全协议。

g）应建立智慧城市一体化网络平台，包括局域网用户接入认证系统、广域网用户接入认证系统、即时通讯系统和日志文档数据管理系统等，实现网络中的用户身份认证、授权与访问控制、安全审计、网络内的用户重要数据加密存储和用户间数据加密传输等功能。每个网络用户须要有唯一的网络身份标识，凭此网络身份标识能够对上网者进行身份识别和网络接入控制、定位和追溯不当或者违法上网行为。只有合法的用户才能在其中进行网络接入、加密会话、文档安全保管及分发等业务。智慧城市一体化网络平台安全要求见附录H。

8.3 终端安全要求

a)终端安全应满足《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008）对应安全保护等级中的安全控制项要求，覆盖物理安全、身份鉴别、访问控制、安全审计、恶意代码防范、入侵防范、资源控制等部分的内容。智慧城市终端安全要求见附录G。

b）应建设统一的终端安全管理体系，准确掌握终端的软硬件资产、终端健康性、终端使用情况等信息，规范终端的各类访问、操作及使用行为，确保接入终端的安全合规、可管理、可控制、可审计，实现终端的集中、统一、规范化管理，减少维护人员的工作量，提升终端管理维护的水平、效率及安全性。

c）终端接入时应进行自身安全防护，应支持根据安全策略对终端进行操作系统配置，支持根据不同的策略自动选择所需应用软件进行安装，完成配置。并建立有效的补丁管理机制，可自动获取或分发补丁，补丁获取方式应具有合法性验证安全防护措施，如经过数字签名或哈希校验机制保护。应禁止未安装指定防病毒软件的客户端接入。

d）应提供以密码技术为前提的安全接入服务，保证外围终端能够选择加密通信方式安全接入；可在重要终端中嵌入带有密码性安全子系统的终端芯片，以解决应用系统对系统层的访问和控制权限；应采用密码技术保证终端通信数据的完整性、保密性，可采用类似VPN的方式建立通信隧道；加强终端操作的抗抵赖措施，在请求的情况下为数据原发者或接收者提供数据原发证据的功能，在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

e）移动终端应支持数字证书的安装和运行；支持VPN客户端的安装和运行，以及在线升级。应尽量降低数据在移动终端的保存时间，同时根据移动终端的环境特点，对终端环境进行管理和控制，检测和防止各种非法攻击，确保信息和数据的终端安全。

8.4 应用安全要求

a）应用系统安全应满足《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）对应安全保护等级中应用安全部分的安全控制项要求，覆盖身份鉴别、访问控制、安全控制、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等部分的内容。

b）应制定安全开发管理规范，以保证应用系统开发过程得到相应的控制，从而保障系统从开发到生产运行的全过程的安全管控，需要注意代码安全开发，防范不安全的代码给系统带来的安全风险；应加强内存管理，防止驻留在内存中的剩余信息被他人非授权获取。

c）应用系统可参照4A体系，建立统一的帐号、认证、授权和审计系统，实施严格的身份管理、安全认证与访问权限控制，提供用户访问记录，访问可溯。

d）应用程序应进行可信执行保护，构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复。

e）应用系统上线前，应对其进行全面的安全评估，并进行安全加固。应遵循安全最小化原则，关闭未使用的服务组件和端口。应采用专业安全工具对应用系统进行定期评估。在补丁更新前，应对补丁与现有系统的兼容性进行测试。

f）应用系统访问控制应支持结合安全管理策略，对账号口令、登录策略进行控制，应支持设置用户登录方式及对系统文件的访问权限；应对远程访问控制进行限制，限制匿名用户的访问权限，支持设置单一用户并发连接次数、连接超时限制等，应采用最小授权原则，分别授予不同用户各自所需的最小权限。

8.5 数据安全要求

a)数据安全应满足《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008）对应安全保护等级中数据安全部分的安全控制项要求，覆盖数据完整性、数据保密性、备份与恢复等部分的内容。

b)在智慧城市建设中，一般的可将信息分为敏感信息和公开信息，在实际应用过程中，根据分类数据的安全属性进行分级，包括对用户权益的影响程度，信息关联度，数据泄露对机构或个人造成不良社会影响的程度等；分类分级应遵循隐私保护优先、强业务保障、稳定性等原则，不同级别的数据被同时处理、应用时，应按照其中级别最高的要求来实施保护，对于非敏感数据关联后可能产生敏感数据的场景,关联后的产生数据对应的级别应高于原始数据。对不同类别的信息采取不同保护措施，重点防范用户越权访问、篡改敏感信息。信息分类分级管理见附录B。

c）应加强数据采集、传输、处理和存储全生命周期的数据安全管理，需要建立灾备中心，保证所有的数据包括所有副本和备份，存储在合同、服务水平协议和法规允许的地理位置，防范由于数据集中存放带来的巨大安全风险。

d）对采集数据的传输、存储及分类级实施严格安全要求。对采集数据的传输、存储及分类级实施严格安全要求。对核心网采集设备用多人分级分权方式进行设备远程维护。对采集到的数据按照重要性及敏感度进行分类级处理，当采集数据涉及到敏感时，能够根据策略进行中断采集，并记录相关的采集行为。

e）虚拟存储系统应支持在不中断正常存储服务的前提下实现对存储容量和存储服务进行任意扩展,透明的添加和更替存储设备，并具有自动发现、安装、检测和管理不同类型存储设备的能力；在多租户的云计算环境下，可通过物理隔离、虚拟化和应用支持的多租户架构等方案实现不同租户之间数据和配置的安全隔离，以保证每个租户数据的安全与隐私；虚拟存储系统应支持按照数据的安全级别建立容错和容灾机制，以克服系统的误操作、单点失效、意外灾难等因素造成的数据损失。

f）需要支持文件系统加密功能，利用技术保证了平台数据不被破坏和窃取。加密 存储安全 可根据数敏感度等，支持分级的加密方法可别进行不加密、部分加密（脱敏）、完全加密等不同存储。由于法律系统持续关注电子证据发现，云服务提供商和数据拥有者需要把重点放在发现数据并确保法律和监管部门要求的所有数据可被找回。

g）敏感数据不能在使用、储存或传输过程中，在没有任何补偿控制的情况下与其他客户数据混合。要进行数据脱敏，对某些敏感信息通过脱敏规则进行数据的变形，实现敏感数据的可靠保护，实现在不泄露用户隐私的前提下保障业务系统的正常运行；应能针对不同用户和不同敏感数据根据需求设置不同的脱敏算法，应能支持管理员可以配置用户查询特定数据库的特定表的特定列的脱敏算法，所选择脱敏算法具有一定的安全性、健壮性，不能被轻易破解或还原，数据脱敏之后不应影响业务连续性，不应对系统性能造成较大影响。

f）不同应用之间需要进行数据关联性隔离，防止不同应用之间的数据关联分析，产生数据泄露；在响应同一应用或同一用户的多个数据访问请求时，也需要做好数据关联性隔离，防止不同的数据访问请求关联分析产生敏感数据；通过数据溯源追踪、管理数据之间的衍生依赖关系，对敏感数据的衍生数据进行安全保护，对敏感数据应用周期的各个环节的操作进行标记和定位，在发生数据安全问题时，可以利用数据溯源技术进行数据追踪，及时准确地定位到出现问题的环节和责任者。

g）数据二次应用安全要求：对数据转移导出进行严格控制，对于系统间和后台数据的导出行为，应予以严格控制；针对外部系统有固定的数据需求时，应建立具有严格安全审批控制互动接口，实现目标数据的自动传递；大数据对外服务时，要防范外部合作方将获得的数据进行二次售卖或者其他未经许可的用途；将整个服务过程中涉及的数据生产、加工、消费链路部署在提供方可监控的环境中，并对外部合作方的数据使用进行监控审计；根据具体的保护策略对合作方所访问数据的行为进行数字水印保护，以便对信息泄露的行为进行追踪；对外服务过程中，针对外部合作方需制定更为严格的安全控制、安全管理和安全审计的管理制度。

h）数据必须彻底有效地去除才被视为销毁。必须具备一种可用的技术，能保证全面和有效地定位云计算数据、擦除/销毁数据，并保证数据已被完全消除或使其无法恢复。

8.6 密码技术要求

a）应用系统应根据业务需要采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。应采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。密码技术要求见附录K。

b）应采用密码技术保证通信过程中数据的完整性；在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；应对通信过程中的敏感信息字段进行加密；应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

8.7 安全产品要求

a）既有技术标准安全产品要求

对既有技术标准信息安全产品，应依据既有相关标准规范要求，进行符合性查证。对传统的FW/IPS/IDS/漏洞扫描等产品的技术标准参考如下：

GB/T 18019-1999 信息技术 包过滤防火墙安全技术要求

GB/T 18020-1999 信息技术 应用级防火墙安全技术要求

GB/T 20010-2005 信息安全技术 包过滤防火墙评估准则

GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法

GB/T 20278-2006 信息安全技术 网络脆弱性扫描产品技术要求

GB/T 26268-2010 网络入侵检测系统测试方法

GB/T 26269-2010 网络入侵检测系统技术要求

GB/T 20280-2006 信息安全技术 网络脆弱性扫描产品测试评价方法

GB/T 20281-2006 信息安全技术 防火墙技术要求和测试评价方法

GB/T 28451-2012 信息安全技术 网络型入侵防御产品技术要求和测试评价方法

GB/T 31167-2014 信息安全技术 云计算服务安全指南

GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

b）新技术安全保障要求

对物联网、移动互联网、大数据等安全技术标准尚在研制中的智慧城市信息技术，根据OSI模型，从物理层到应用层七层协议，对每层技术指标的安全保障要求进行验证性测试。

c）安全管理平台技术要求

应能记录系统相关安全事件，并能对特定安全事件进行报警；审计记录应包括安全事件的主体、客体、时间、类型和结果等内容；应提供审计记录的分类、统计分析和查询等；应提供审计记录的存储保护，确保审计记录不被破坏或非授权访问。安全管理平台技术要求见附录I。

8.8 智慧城市产品（系统）安全接口要求

智慧城市产品选型应满足统一安全管理和安全运维的接口要求。具体包括：

a）应满足统一用户管理接口要求。智慧城市应为每个市民、企业分配唯一标识符（如居民身份证、企业注册号），并统一管理。统一管理系统通过用户管理接口实现各产品/系统的用户同步。

b）应满足统一认证和授权接口要求。智慧城市全系统实现基于CA的统一认证和授权机制。各系统通过统一认证和授权接口实现对用户的认证和操作授权。

c）应满足统一安全监控接口要求。智慧城市安全运维系统通过安全监控接口获取各系统的安全状态，进而分析智慧城市整体安全态势。

d）应对高安全等级数据提供安全访问接口。如果产品涉及高安全等级的数据的访问，各产品应提供加密访问接口。

e）应满足统一安全策略配置接口要求。智慧城市需要实现全系统统一安全策略管理。因此，各产品应提供安全策略配置接口，以实现对各产品安全策略的统一配置和管理。

8.9 一体化安全维护管理平台

a）包含系统平台框架、资产管理、安全事件管理、基础关联分析、标准脆弱性管理、风险评估、报表模块、响应管理模块、权限管理、知识管理、系统自身管理。

b）用户可以自定义资产类型，并且可以针对每个资产类型自定义资产扩展属性，包括属性名称和类型。

c）系统能够自动进行网络拓扑发现，自动描绘网络中资产节点之间网络连接关系。

d）能够实时监控来自不同厂商的网络设备、安全设备、安全系统、主机操作系统、数据库、中间件以及各种应用系统的日志、警报等信息。

e）通过发布内部及外部的早期预警信息，分析可能受影响的资产，提前了解业务系统可能遭受的攻击和潜在的安全隐患；同时可以将告警和任务形成工单，提供标准的工单任务处理流程。

8.10 智慧城市物品标识认证要求

智慧城市物品标识应采用满足超大规模标识管理的标识认证体系，满足超大规模标识认证和离线认证要求。具体包括：

a）应满足超大规模物品标识认证要求。智慧城市应为每个参与活动的物品分配唯一标识，作为物品的电子身份证。

b）应满足物品标识离线认证要求。智慧城市应实现物品标识离线验证机制，而无需第三方参与。

c）所用的物品标识应充分满足大众鉴真识别要求，满足大众免费、快速、离线（可在线）的鉴真识别。

附 录 A
（规范性附录）
智慧城市风险评估方法和流程

A.1 实施计划

信息化主管部门制定检查评估年度实施计划。

A.2 评估机构

信息化主管部门委托符合条件的风险评估服务机构，对试点项目中的重要信息系统实施检查评估。

A.3 系统规划风险评估

对总体规划、设计方案等相关配套文件的合理性和正确性以及安全控制措施的有效性进行评估；评估结果应体现在信息系统整体规划或项目建议书中。

A.4 总体风险评估

对本机构所有信息系统共有的公共部分进行评估，实施总体风险控制；根据信息系统的总体风险状况确定评估频率，但至少每三年评估一次。

A.5 系统风险评估

对研发、运行及废弃的全过程进行风险评估，分别包括试运行与运行后的风险评估。

A.6 试运行系统评估

对信息项目开发过程中所提交的有关文档资料进行评估，指出其中存在的风险，了解是否具有相应的控制措施，并提出评价和建议的过程。信息系统运行前的系统审阅应关注信息系统的安全控制、权限设置、正确性、连贯性、完整性、可审计性和及时性等内容。

A.7 运行后系统评估

在信息系统正常运行一段时间后进行的评估，旨在评估对信息系统各项风险的控制是否恰当，能否实现预定的设计目标。运行后的系统评估应在信息系统正常运行半年后进行，评估报告应对被评估的信息系统提出改进或增加风险控制、能否继续运行等内容的评估建议。

A.8 专项风险评估

对被评估系统发生信息安全事故进行的调查、分析和评估，或原有信息系统进行重大结构调整的评估，或信息化主管部门认为需要对信息系统某项专题进行评估。

附 录 B
（规范性附录）
信息分类分级管理

B.1 政府信息分类

B.1.1 信息分类原则

客户将信息部署或迁移到云计算平台之前，应先明确信息的类型。

本标准中的政府信息是指政府机关，包括受政府委托代行政府机关职能的机构，在履行职责过程中，以及政府合同单位在完成政府委托任务过程中产生、获取的，通过计算机等电子装置处理、保存、传输的数据，以及相关的程序、文档等。

涉密信息的处理、保存、传输、利用按国家保密法规执行。

本标准将非涉密政府信息分为**敏感信息**、**公开信息**两种类型。

B.1.2 敏感信息

敏感信息的概念

敏感信息指不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁可能造成以下后果：

a) 损害国防、国际关系；
b) 损害国家财产和公共利益，以及个人财产或人身安全；
c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；
d) 影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为；
e) 干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；
f) 危害国家关键基础设施、政府信息系统安全；
g) 影响市场秩序，造成不公平竞争，破坏市场规律；
h) 可推论出国家秘密事项；
i) 侵犯个人隐私、企业商业秘密和知识产权；
j) 损害国家、企业、个人的其他利益和声誉。

敏感信息的范围

敏感信息包括但不限于：

a) 应该公开但正式发布前不宜泄露的信息，如规划、统计、预算、招投标等的过程信息；
b) 执法过程中生成的不宜公开的记录文档；
c) 一定精度和范围的国家地理、资源等基础数据；
d) 个人信息，或通过分析、统计等方法可以获得个人隐私的相关信息；
e) 企业的商业秘密和知识产权中不宜公开的信息；
f) 关键基础设施、政府信息系统安全防护计划、策略、实施等相关信息；
g) 行政机构内部的人事规章和工作制度；
h) 政府部门内部的人员晋升、奖励、处分、能力评价等人事管理信息；
i) 根据国际条约、协议不宜公开的信息；
j) 法律法规确定的不宜公开信息；
k) 单位根据国家要求或本单位要求认定的敏感信息。

B.1.3 公开信息

公开信息指不涉及国家秘密且不是敏感信息的政府信息，包括但不限于：

a) 行政法规、规章和规范性文件，发展规划及相关政策；
b) 统计信息，财政预算决算报告，行政事业性收费的项目、依据、标准；
c) 政府集中采购项目的目录、标准及实施情况；
d) 行政许可的事项、依据、条件、数量、程序、期限以及申请行政许可需要提交的全部材料目录及办理流程；
e) 重大建设项目的批准和实施情况；
f) 扶贫、教育、医疗、社会保障、促进就业等方面的政策、措施及其实施情况；
g) 突发公共事件的应急预案、预警信息及应对情况；
h) 环境保护、公共卫生、安全生产、食品药品、产品质量的监督检查情况等；
i) 其他根据相关法律法规应该公开的信息。

B.2 政府业务分类

B.2.1 业务分类原则

确定了信息类型后，还需要对承载相关信息的业务进行分类。根据业务不能正常开展时可能造成的影响范围和程度，本标准将政府业务划分为**一般业务、重要业务、关键业务**等三种类型。

B.2.2 一般业务

一般业务出现短期服务中断或无响应不会影响政府部门的核心任务，对公众的日常工作与生活造成的影响范围、程度有限。

通常政府部门、社会公众对一般业务中断的容忍度以**天**为单位衡量。

B.2.3 重要业务

重要业务一旦受到干扰或停顿，会对政府决策和运转、对公服务产生较大影响，在一定范围内影响公众的工作生活，造成财产损失，引发少数人对政府的不满情绪。此类业务出现问题，造成的影响范围、程度较大。

满足以下条件之一的业务可被认为是重要业务：

——政府部门对业务中断的容忍程度小于 24h；
——业务系统的服务对象超过 10 万用户；
——信息发布网站的访问量超过每天 500 万人次；
——出现安全事件造成 100 万元以上经济损失；
——出现问题后可能造成其他较大危害。

B.2.4 关键业务

关键业务一旦受到干扰或停顿，将对政府决策和运转、对公服务产生严重影响，威胁国家安全和人民生命财产安全，严重影响政府声誉，在一定程度上动摇公众对政府的信心。

满足以下条件之一的业务可被认为是关键业务：

——政府部门对业务中断的容忍程度小于 1h；
——业务系统的服务对象超过 100 万用户；
——出现安全事件造成 5000 万元以上经济损失，或危害人身安全；

——出现问题后可能造成其他严重危害。

B.3 优先级确定

在分类信息和业务的基础上，综合平衡采用智慧城市建设后的效益和风险，确定优先部署到云计算平台的数据和业务，如图 C.1 所示。

a) 承载公开信息的一般业务可优先采用包括公有云在内的智慧城市建设，尤其是那些利用率较低、维护和升级成本较高、与其他系统关联度低的业务应优先考虑采用社会化的智慧城市建设。
b) 承载敏感信息的一般业务和重要业务，以及承载公开信息的重要业务也可采用智慧城市建设，但宜采用安全特性较好的私有云或社区云。
c) 关键业务系统暂不宜采用社会化的智慧城市建设，但可采用场内私有云（自有私有云）。

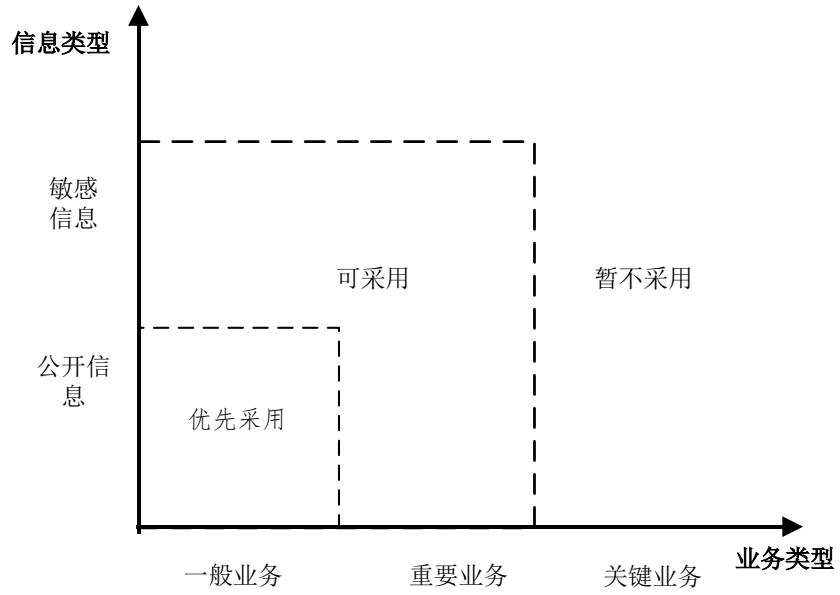


图 C.1 采用智慧城市建设的优先级

B.4 安全保护要求

所有的客户信息都应该得到适当的保护。对于公开信息主要是防篡改、防丢失，对于敏感信息还要防止未经授权披露、丢失、滥用、篡改和销毁。

所有的客户业务都应得到适当保护，保证业务的安全性和持续性。

不同类型的信息和业务对安全保护有着不同的要求，客户应要求云服务商提供相应强度的安全保护，如图 C.2 所示。

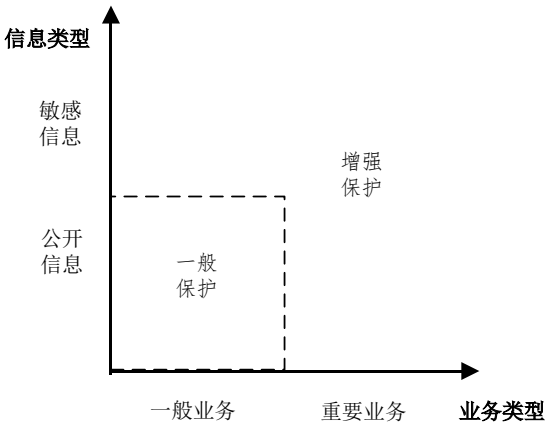


图 C.2 安全保护要求

对智慧城市建设的安全能力要求如下：

a) 承载公开信息的一般业务需要一般安全保护；
承载敏感信息的一般业务和重要业务，以及承载公开信息的重要业务需要增强安全保护；

b) 关于一般安全保护和增强安全保护的具体指标要求，见相应的国标要求。

附 录 C
（规范性附录）
安全域划分与管理

网络安全域是指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，且相同的网络安全域共享一样的安全策略。广义可理解为具有相同业务要求和安全要求的IT系统要素的集合。

C.1 划分原则

在安全域划分时应该遵循以下的一些基本原则：

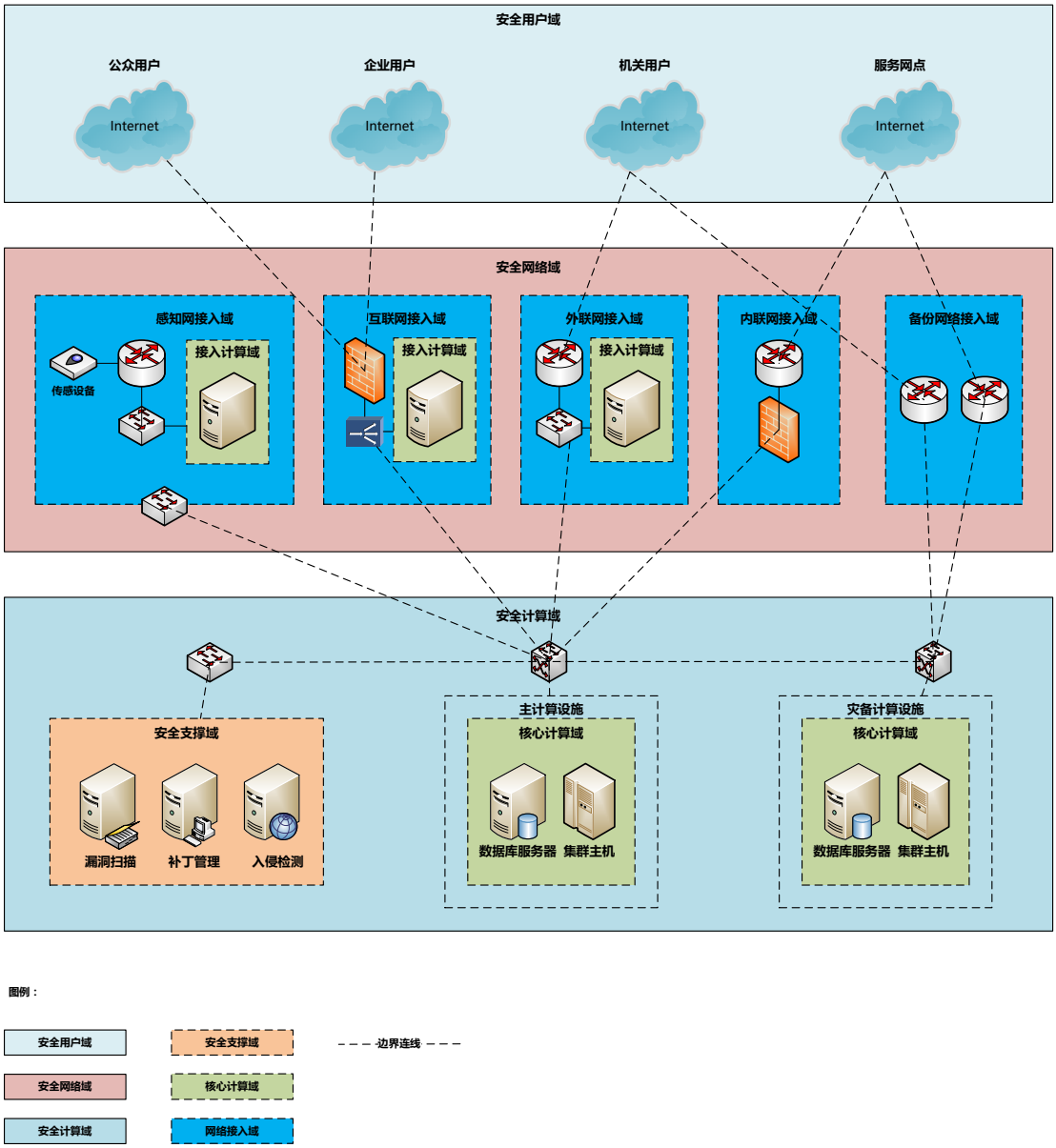
1、根据系统中各设备其所承担的工作角色和对安全方面要求的不同进行行划分；在划分的同时有针对性的考虑安全产品的部署。从网络构架层面来讲，系统整体结构安全域的划分与安全产品的部署密不可分的，一方面安全域的划分为安全产品的部署提供了一个健康规范灵活的网络环境；另一方面，将安全域划分为域内划分和域外划分两种，域和域之间主要采用通过交换设备划分VLAN 和防火墙来彼此策略隔离；在域内主要根据不同被保护对象的安全需求采用部署AAA、IDS和防病毒系统等来完成，因此，安全域的划分不能脱离系统的部署。

2、安全域的个数不应过多，否则在策略设置上过于复杂，会给今后管理带来很大不便；在划分的保证各个安全域之间路由戒者交换跳数不应该过多；

3、安全域划分的目的是发挥系统的整体效能，并不是对原有系统整体结构的彻底颠覆。因此在对网络结构改造的同时需要考虑保护已有投资，避免重复投入建设。

根据上述原则，为了建立智慧城市网络的整体安全防护体系，安全域可以分为安全计算域、安全用户域、安全网络域。

对安全域进行进一步细分，安全网络域可以进一步细分为感知网接入域、互联网接入域、外联网接入域、内联网接入域、备份网络接入域。安全计算域可以细分为核心计算域和安全支撑域。网络安全域划分如下图所示：



图D.1 网络安全域划分图

安全计算域：由一个主机/服务器组成的，或者多个主机/服务器经局域网连接组成的存储和处理数据信息的区域，是需要进行相同安全保护的主机/服务器的集合。

安全用户域：由一个活多个用户终端计算机组成的存储、处理和使用数据信息的区域。

安全网络域：支撑安全域的网络设备和网络拓扑，是安全域的承载子域，防护重点是保障网络性能和进行各子域的安全隔离与边界防护。连接安全计算域和安全计算域、安全计算域和安全用户域之间的网络系统组成的区域。

C.2 安全计算域

C.2.1 划分和管理技术要求

安全域的划分需要遵循以下方面：

a) 根据数据信息处理和存储进行划分

安全计算域可以由一台主机/服务器组成，也可以由一个局域网环境组成，划分依据取决于确定出数据信息处理和存储的计算机系统。

C.2.2 防护技术要求

根据数据信息的存储和处理所涉及的范围确定智慧城市网络的安全计算域并制定确定相应的安全保护等级，根据安全保护等级确定具体防护措施。一般的，应遵循以下要求：

a) 自主访问控制

应在安全策略控制范围内，使用户/用户组对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户/用户组。访问控制主体的粒度为用户/用户组级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。

b) 恶意代码防范

应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。

c) 程序可信执行保护

可构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复，例如采用可信计算等技术。

C.2.3 网络和边界技术要求

安全域的网络和边界的设计需要遵循以下方面：

a) 通信网络数据传输完整性保护

可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。

b) 通信网络数据传输保密性保护

可采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

c) 区域边界包过滤

可根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。

d) 区域边界恶意代码防范

可在安全区域边界设置防恶意代码软件，并定期进行升级和更新，以防止恶意代码入侵。

C.3 安全用户域

C.3.1 划分和管理技术要求

安全域的划分需要遵循以下方面：

a) 根据数据信息处理和存储进行划分

安全用户域是信息系统中由一个或多个用户终端计算机组成的存储、处理和使用数据信息的区域。

C.3.2 防护技术要求

根据用户所能访问的计算域中的数据信息类和用户计算机所处的物理位置来确定安全用户域。同时，根据安全用户域确定明确的边界和防护措施。一般的，应遵循以下要求：

a) 用户身份鉴别

应支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度

的两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

b) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

c) 标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

d) 系统安全审计

应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警；确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

e) 用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

f) 用户数据保密性保护

采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

C.3.3 网络和边界技术要求

安全域的网络和边界的设计需要遵循以下方面：

a) 通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心管理。

b) 通信网络数据传输完整性保护

可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。

c) 通信网络数据传输保密性保护

可采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

d) 区域边界访问控制

应在安全区域边界设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。

e) 区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。

f) 区域边界安全审计

应在安全区域边界设置审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。

g) 区域边界完整性保护

应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。

C.4 安全网络域

C.4.1 划分和管理技术要求

安全域的划分需要遵循以下方面：

a) 按照物理的或逻辑的网络结构进行划分

安全网络域是信息系统中连接安全计算域与安全计算域、安全计算域与安全用户域之间的网络系统组成的区域，安全域的确定依赖于物理或者逻辑的网络结构。

b) 用户身份鉴别

应支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他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，并对鉴别数据进行保密性和完整性保护。

c) 自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

d) 标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

e) 系统安全审计

应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警；确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

f) 用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

g) 用户数据保密性保护

采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

C.4.2 防护技术要求

安全域的防护需要遵循以下方面：

a) 通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心管理。

b) 通信网络数据传输完整性保护

可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。

c) 通信网络数据传输保密性保护

可采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

C.4.3 网络和边界技术要求

安全域的网络和边界的设计需要遵循以下方面：

a) 区域边界访问控制

应在安全区域边界设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。

b) 区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。

c) 区域边界安全审计

应在安全区域边界设置审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。

d) 区域边界完整性保护

应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。

附 录 D
（资料性附录）
信息安全建设内容编制要求

D.1.1 项目建议书编制要求

在“必要性”、“需求分析”、“建设方案”等篇章专设一节描述“信息安全”相关内容。

1．项目建设的必要性

增加“信息安全保障现状与差距”：阐述目前信息安全软硬件装备和应用情况，梳理信息安全有关规定和要求，分析存在的主要问题和差距。

2．需求分析

增加“信息安全风险与需求分析”：识别影响网络与信息安全的主要因素，分析可能面临的信息安全主要风险。

3．本期项目建设方案

专设“网络与信息安全保障体系建设”一节：描述保障本项目基础网络安全、重要系统安全和信息内容安全的软硬件配置方案、标准规范建设框架以及信息安全检测与审查措施。

D.1.2 项目可行性研究报告\建设方案编制要求

在“必要性”、“需求分析”、“建设方案”等篇章专设一节描述“信息安全”相关内容。

1．项目建设的必要性

增加“信息安全保障现状与差距”：阐述目前信息安全软硬件装备和应用情况，梳理信息安全有关规定和要求，分析存在的主要问题和差距。

2．需求分析

增加“信息安全风险与需求分析”：识别影响网络与信息安全的因素，分析可能面临的信息安全风险及危害程度。

从业务需求出发，进行信息安全风险评估。对信息资产的重要性、威胁发生的频率、系统自身脆弱性进行识别和关联分析，判断信息系统面临的风险及应采取什么强度的安全措施将风险可能造成的影响控制在可接受的范围内，分析信息及信息系统对国家安全、经济建设和社会生活的重要程度及遭到破坏后对其的危害程度。

3．本期项目建设方案

专设“网络与信息安全保障体系建设”一节，按照信息安全等级保护要求，确定等级，阐述保障本项目基础网络安全、重要系统安全和信息内容安全的软硬件配置方案、标准规范建设内容、信息安全检测计划、项目建设与运行维护过程的信息安全审查与控制措施。

附 录 E
（资料性附录）
智慧城市建设项目信息安全评估要求

建设单位向投资主管部门或电子政务管理部门，报送项目建议书、可行性研究报告、建设方案等申报资料，应符合附录 E 规定要求，联合具有风险评估及等保测评资质的信息安全服务机构，共同出具《信息安全评估意见》。

<table>
<tr><td rowspan="3">本情况</td><td>单位名称</td><td colspan="2"></td><td>员工人数</td><td></td></tr>
<tr><td>信息化负责人</td><td colspan="2"></td><td>信息技术部门员工人数</td><td></td></tr>
<tr><td>系统建设时间</td><td colspan="2"></td><td>系统规划建设周期</td><td></td></tr>
<tr><td rowspan="3">信息安全必要性分析</td><td rowspan="3">信息安全保障现状与差距分析</td><td colspan="4">是否清晰描述信息安全软硬件装备和应用情况的现状</td></tr>
<tr><td colspan="4">有否梳理信息安全有关规定和要求</td></tr>
<tr><td colspan="4">对信息安全存在的主要问题和差距是否分析到位</td></tr>
<tr><td>信息安全风险与需求分析</td><td>识别影响网络与信息安全的主要因素，分析可能面临的信息安全主要风险</td><td colspan="4">对信息资产的重要性、威胁发生的频率、系统自身脆弱性进行识别和关联分析，判断信息系统面临的风险及应采取什么强度的安全措施将风险可能造成的影响控制在可接受的范围内，分析信息及信息系统对国家安全、经济建设和社会生活的重要程度及遭到破坏后对其的危害程度。</td></tr>
<tr><td>信息安全建设方案</td><td>网络与信息安全保障体系建设</td><td colspan="4">按照信息安全等级保护要求，确定系统保护等级，制定安全策略，明确系统的安全域划分，提出安全解决方案。阐述保障本项目基础网络安全、重要系统安全和信息内容安全的技术和管理措施，包括但不限于软硬件配置方案、标准规范建设内容、信息安全检测计划、项目建设与运行维护过程的信息安全审查与控制措施等。</td></tr>
<tr><td rowspan="3">安全建设</td><td rowspan="3">本期项目信息安全建设内容</td><td>硬件类</td><td>金额</td><td>国产化比例</td><td>设计要求</td></tr>
<tr><td>软件类</td><td>金额</td><td>国产化比例</td><td>设计要求</td></tr>
<tr><td>服务类</td><td>金额</td><td>国产化比例</td><td>设计要求</td></tr>
</table>

内容		其他	金额	国产化比例	设计要求
	在本期项目建设内容之外所依托的信息安全设施情况	包括依托前期项目、依托外部资源和服务等情况			
等级保护定级	信息系统 1	安全保护等级	业务信息安全等级		系统服务安全等级
	信息系统 2	安全保护等级	业务信息安全等级		系统服务安全等级
	信息系统 3	安全保护等级	业务信息安全等级		系统服务安全等级
	……				
信息安全建设规划情况	短期建设目标				
	中期建设目标				
	长期建设目标				

附 录 F
（资料性附录）
智慧城市建设项目信息安全审核要求

项目竣工验收前，项目建设单位应将项目概况、信息安全自主审查（包括《信息安全审核情况表》和第三方信息安全风险评估报告和等级保护测试报告等材料），报信息安全主管部门审查，审查通过后方可组织竣工验收。

<table>
<tr><td rowspan="3">基本情况</td><td>单位名称</td><td colspan="2"></td><td>员工人数</td><td></td></tr>
<tr><td>信息化负责人</td><td colspan="2"></td><td>信息技术部门员工人数</td><td></td></tr>
<tr><td>项目完成时间</td><td colspan="2"></td><td>项目试运行时间</td><td></td></tr>
<tr><td rowspan="8">安全建设目标的符合性</td><td rowspan="4">信息安全保护系统建设内容实现情况</td><td>硬件类</td><td>金额</td><td>国产化比例</td><td>是否满足设计要求</td></tr>
<tr><td>软件类</td><td>金额</td><td>国产化比例</td><td>是否满足设计要求</td></tr>
<tr><td>服务类</td><td>金额</td><td>国产化比例</td><td>是否满足设计要求</td></tr>
<tr><td>其他</td><td>金额</td><td>国产化比例</td><td>是否满足设计要求</td></tr>
<tr><td>信息安全部署及配置情况</td><td colspan="4">是否按设计要求进行部署配置</td></tr>
<tr><td rowspan="2">信息安全培训情况</td><td colspan="4">是否按要求进行操作培训和安全培训</td></tr>
<tr><td colspan="4">信息安全相关人员是否持证上岗</td></tr>
<tr><td rowspan="4">等级保护测评</td><td>信息系统 1</td><td colspan="2">安全保护等级</td><td colspan="2">测评结果</td></tr>
<tr><td>信息系统 2</td><td colspan="2">安全保护等级</td><td colspan="2">测评结果</td></tr>
<tr><td>……</td><td colspan="2">……</td><td colspan="2">……</td></tr>
<tr><td rowspan="4">信息安全风险评估</td></tr>
<tr><td>信息系统 1</td><td colspan="2">风险结果分析</td><td colspan="2">综合评价</td></tr>
<tr><td>信息系统 2</td><td colspan="2">风险结果分析</td><td colspan="2">综合评价</td></tr>
<tr><td>……</td><td colspan="2">……</td><td colspan="2">……</td></tr>
<tr><td rowspan="2">产品</td><td>政府投资信息化项目整体风险评估</td><td colspan="4">有无不可接受风险</td></tr>
<tr><td>服务商</td><td colspan="4">单位资本构成（外资成分）；
企业资质（集成资质、涉密资质、安全服务资质等）</td></tr>
</table>

<table>
<tr><td>和服务</td><td>产品/服务</td><td colspan="4">是否开展产品认证、销售许可、密码检测等产品与服务准入情况梳理；是否开展著作权、专利等情况梳理；
是否有不符合国家规定准入要求的产品</td></tr>
<tr><td rowspan="4">安全防护概况</td><td rowspan="3">网络防护</td><td colspan="2">与其他网络间的隔离措施</td><td colspan="2">□逻辑强隔离□逻辑隔离□未隔离</td></tr>
<tr><td colspan="2">网络区域划分</td><td colspan="2">□已划分 □未划分</td></tr>
<tr><td colspan="2">区域间防护措施</td><td colspan="2"></td></tr>
<tr><td>主机防护</td><td colspan="4">□安全操作系统 □已加固 □未加固</td></tr>
<tr><td rowspan="3">管理制度</td><td>信息安全管理方针</td><td>□有
□无</td><td>机房安全管理制度</td><td>□有
□无</td></tr>
<tr><td>系统运行维护管理制度</td><td>□有
□无</td><td>备份和恢复管理制度</td><td>□有
□无</td></tr>
<tr><td>安全事件报告和处置管理制度</td><td>□有
□无</td><td>教育培训制度</td><td>□有
□无</td></tr>
<tr><td rowspan="3">信息安全建设规划情况</td><td>短期建设目标</td><td colspan="4"></td></tr>
<tr><td>中期建设目标</td><td colspan="4"></td></tr>
<tr><td>长期建设目标</td><td colspan="4"></td></tr>
</table>

附 录 G
（资料性附录）
智慧城市终端安全要求

G.1.1 智慧城市终端总体安全要求

智慧城市终端系统应采用自主可控的系统，防范恶意代码入侵；智慧城市终端系统须要完成身份认证请求后才能接入智慧城市中心网络，且登录智慧城市的用户也得通过合法网络身份认证才能取得相应的智慧城市服务的权限；智慧城市终端和智慧城市中心网络之间的数据交互应充分满足在全密态并一次一密的环境下进行。

G.1.2 智慧城市固定终端安全要求

智慧城市固定终端是可以供任一市民使用的固定系统，应安置在有视频监控的安全场所；智慧城市固定终端须要集成密码标识认证芯片，以此作为接入智慧城市网络的登录身份凭证；智慧城市固定终端须要有接收用户身份标识信息的系统接口，方便智慧城市网络对市民进行身份认证；同时，固定终端和智慧城市服务网络之间的全密态数据交互也以用户身份标识信息作为重要密钥签名及交换工具。

G.1.3 智慧城市移动终端安全要求

智慧城市移动终端是每个用户私人使用的智慧城市服务终端，在此移动终端中，用户身份标识信息可以芯片的形式集成进入终端，也可以移动终端配件的形式在需要进行身份认证时，与智慧城市移动终端进行身份数据的交互；移动终端和智慧城市服务网络之间的全密态数据交互以用户身份标识信息作为重要密钥签名及交换工具。

G.1.4 智慧城市用户身份认证安全要求

智慧城市用户身份信息应是基于标识发放的，可以静态分发、静态管理，不需要在线的第三方认证中心支持的；智慧城市用户身份信息既可以软密钥的加密数据形式存放在终端系统中，也能够以密码标识认证芯片的形式集成进入终端系统。

附 录 H
（资料性附录）
智慧城市一体化网络平台安全要求

H.1.1 智慧城市一体化网络平台总体要求

一体化网络平台应由局域网用户接入认证系统、广域网用户接入认证系统、即时通讯系统和文档数据管理系统等组成，实现了互联网中的用户身份认证、授权与访问控制、安全审计、网络内的用户重要数据加密存储和用户间数据加密传输等功能。

H.1.2 局域网用户安全接入认证要求

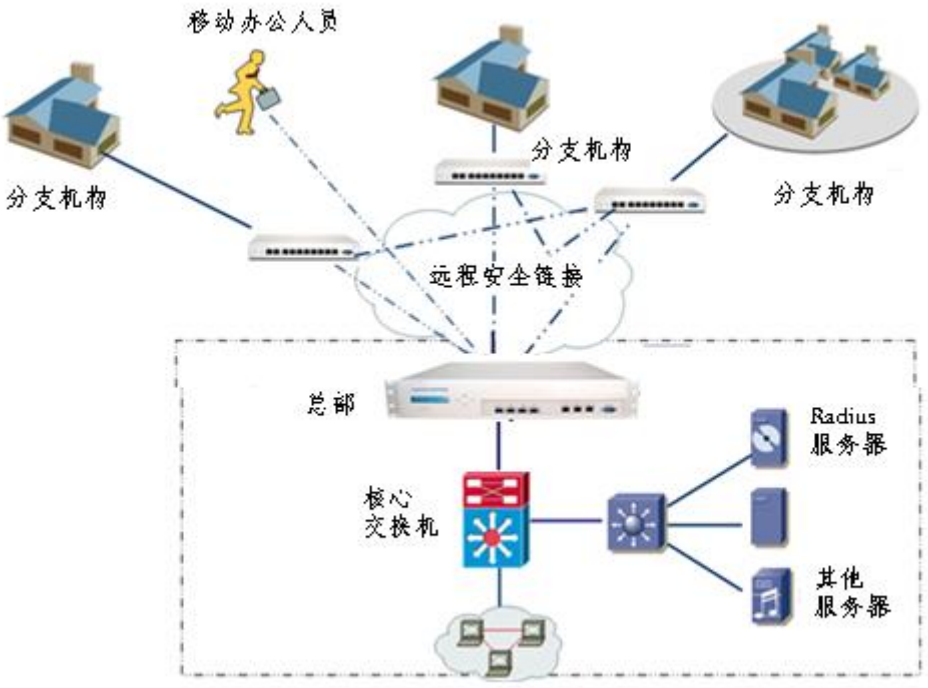
局域网作为各个单位的核心网络，为单位的各种日常工作提供了强大的业务支持；但因内部网络目前缺乏有效监管手段，导致暴露出多种安全问题——非法用户访问网络资源、无法审计和追溯到具体网络违法行为或信息泄露的责任人。

局域网用户接入认证系统应对接入有线或无线局域网的每个用户进行接入控制和身份认证，有效监控网络使用情况，减少信息安全等问题；且当网络中出现违法行为时，通过密码技术进行定位追溯违法行为。

H.1.3 广域网用户安全接入认证要求

广域网用户接入认证系统应提供分支机构或移动端用户通过互联网远程访问总部网络或远程服务器资源的接入控制和身份认证，只有合法的用户通过身份认证后，才能接入到总部网络或服务器资源，进行可控可信的网络资源访问。

典型的应用组网图：



H.1.4 即时通讯信息安全传输要求

即时通讯系统应支持全密态的数据信息交互，其所传输的消息或文件都是在发送过程中自动用对方的标识公钥加密，且对方收到消息或文件后，会自动用自己的标识私钥来解密，从而实现了网络内的消息、文件等安全传输；且只有合法的用户才能连接上即时通讯软件服务器、才具有权限去查看或接受相关消息或文件。

H.1.5 文档数据安全管理要求

文档数据管理系统提供了一个易用、安全、高效的数据管理系统，该系统提供了严谨和灵活的权限管理机制和文档共享机制。通过该系统，文档管理单位可以集中存储和管理海量的文档和各类的数字资产，也可以很安全和便捷的管理文档的存储、分发、打印和下载——只有授权的用户才能解密和使用的相应的文档，保证了数据的完整性和保密性。

附 录 I
（资料性附录）
安全管理平台技术要求

I.1 安全管理平台技术要求

安全管理平台要求能够对安全事件进行集中收集与统一分析，对收集到的事件进行高度聚合存储及分析，实时监控全网安全状况，并可根据不同用户需求提供各种网络安全状况的审计报告。需要满足如下要求：

1. 高性能全面的日志采集：根据各业务系统中的主机、网络设备、应用系统类型和网络分布，采取多种日志采集方式，对网络安全设备、应用以及网络中的各类操作进行全面高性能的日志采集。
2. 审计记录的规范化：由于网络设备种类繁多，各设备日志信息存储格式、字段含义、通信协议存在一定差异。需要对采集到的各种安全日志进行归一化处理，提取审计记录完整信息，为后续审计分析提供依据。
3. 基于策略的日志过滤、归并：面对海量原始日志，需要按照相关策略进行过滤和归并，减轻日志数据传输压力和存储压力。
4. 多维关联分析：对于来自各个资源的日志信息，提供多维的关联分析功能。
5. 大容量日志存储：原始日志信息是来自网络的第一手数据，需要长期存储，并确保它们的完整性、保密性，不得随意访问、修改和删除。
6. 全面丰富的统计报表：提供针对性的统计报表，包括基于源、目的、协议、端口、攻击类型等多种统计项目的top报表。
7. 多租户环境支持，支持虚拟化实例，能够区分不同租户，记录不同租户的日志以及为不同租户提供统计报表；
8. 应该支持基于虚拟化实例的独立的安全管理，以便在云计算多租户环境下，各个租户可以同时对自身的安全资源进行管理。每个租户的虚拟化实例应该具备独立的配置文件和安全事件的发送机制，为安全即服务的理念提供支撑。

I.2 审计内容技术要求

安全管理平台应能记录系统相关安全事件，并能对特定安全事件进行报警；审计记录应包括安全事件的主体、客体、时间、类型和结果等内容；应提供审计记录的分类、统计分析和查询等；应提供审计记录的存储保护，确保审计记录不被破坏或非授权访问。具体要求如下：

1. 支持记录来自外部网络的被安全策略允许的访问请求；
2. 支持记录来自内部网络和DMZ的被安全策略允许的访问请求；
3. 支持记录任何试图穿越或到达防火墙的违反安全策略的访问请求；
4. 试图登录网络安全设备管理端口和管理身份鉴别请求；
5. 支持记录网络安全设备的管理行为；
6. 支持控制日志的访问授权；
7. 支持日志的统计分析和报表生成；
8. 对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；
9. 支持记录来自不同部件的安全事件数据，如病毒事件、异常登录事件、异常操作事件、漏洞检测事件、系统资源异常占用事件、流量异常事件等；

10. 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功,如果失败要记录失败原因;以及其他与审计相关的信息,包括协议类型、源地址、目标地址、源端口和目标端口；

11. 安全审计应可以根据记录数据进行分析，并生成审计报表；

12. 安全审计应可以对特定事件，提供指定方式的实时报警；

13. 审计记录应受到保护避免受到未预期的删除、修改或覆盖等；

14. 应能够定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施（如报警并导出）；

15. 对于多租户环境，应能够区分租户记录上述内容。

I.3 开放性及应急响应技术要求

安全管理平台需要考虑到和周边系统的互联互通，相互传递有价值的安全信息，以便进行协同联动，因此要支持开放的API，第三方系统可以通过API获取相关信息，安全管理平台也可以通过API主动触发第三方系统，便于快速实施应急响应，具体要求如下：

1. 提供REST API，可以供第三方系统调用，查看审计记录及统计报告；

2. 支持采集第三方系统输出的日志，支持Syslog，SNMP Trap等采集方式；

3. 应能够支持紧急事件定义，记录紧急事件，发生紧急事件时能够向第三方系统进行报警，告警信息包含：事件ID、事件主体、事件客体、事件发生时间、事件危险级别和事件描述；

4. 能够支持报告定制，定期生成安全事件统计报告，并发送给第三方系统，供更高层管理人员及时掌握网络安全状况；

5. 以上内容通过Email、XML、SNMP Trap接口实现。

附 录 J
（资料性附录）
无线技术安全要求

J.1 WLAN 设备通用安全要求

本规范所指的设备为 Wi-Fi 使用的 WLAN 设备。本规范提出的安全功能要求，在未特别说明的情况下，均适用于各类 WLAN 设备。

本规范从 WLAN 设备的认证授权功能、安全日志功能以及 IP 网络安全功能， 其他自身安全配置功能和 WLAN 具体设备类型提出安全要求。

J.1.1 账号管理及认证授权要求

认证功能用于确认登录 WLAN 的用户真实身份。认证功能的具体实现方式包括静态口令、动态口令、指纹等生物鉴别技术等。授权功能赋予系统账号的操作 权限，并限制用户进行超越其账号权限的操作。账号口令管理功能是实现正确认证和授权的基础。

对于存在字符或图形界面（WEB 界面）的人机交互的 WLAN 设备，应提供账号管理及认证授权功能，并应满足以下各项要求。

1、 账号

WLAN 设备应能支持按用户分配账号。

WLAN 设备应支持增加、删除、锁定、修改账号功能。

WLAN 应能够限制允许远程登录的账号。

2、 口令安全要求

对于采用静态口令认证技术的 WLAN 设备，应支持数字、小写字母、大 写字母和特殊符号 4 类字符构成的口令。应支持配置口令复杂度检查。 在配置了复杂度后检查，WLAN 设备自动拒绝用户设置不符合复杂度要求的口令。

对于采用静态口令认证技术的 WLAN 设备，应支持按天配置口令生存期功能。在配置了口令生存期后，WLAN 设备在口令超过生存期的用户登录时，应提示并强迫该用户设置新口令。

对于采用静态口令认证技术的 WLAN 设备，应支持配置用户不得重复使 用其最近已用口令的功能。当配置相应功能后，WLAN 设备拒绝用户重复使用在限制次数内的口令，具体限制次数可配置。

对于采用静态口令认证技术的 WLAN 设备，应支持配置用户连续认证失 败次数上限。当用户连续认证失败次数超过上限时，WLAN 设备自动锁 定该用户账号。必须由其他账号，通常为具有管理员权限的账号，才可以解除该账号锁定

对于采用静态口令认证技术的 WLAN 设备，必须支持口令修改，口令修改后不影响设备中业务的正常使用。

对于采用静态口令认证技术的 WLAN 设备，支持静态口令加密存放。

LAN 设备应具备密码字典能力，能够进行弱密码检测，对于用户设置预先配置在弱密码列表中的弱密码进行密码设置拒绝。

WLAN 设备应支持设备之间需要进行用户名、密码配置的，密码应密文 处理存放，同时密码可以修改，且修改后不影响相关业务和直接关联系统业务的运行。

3、授权安全要求

WLAN 应支持对不同用户授予不同权限。

对于用户可通过人机交互界面访问文件系统的 WLAN 设备，应支持对文件系统中的目录和文件，给不同用户或用户组分别授予读、写、执行权限。

J.1.2 日志安全要求

WLAN 设备日志应支持对用户登录/登出进行记录。记录内容包括用户登 录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址。

WLAN 设备日志应支持记录用户对设备的操作，包括但不限于以下内容： 账号创建、删除和权限修改，口令修改，读取和修改设备配置，读取和 修改业务用户的话费数据、身份数据、涉及通信隐私数据。记录需要包含用户账号，操作时间，操作内容以及操作结果。

WLAN 设备应支持远程日志功能。所有设备日志均能通过远程日志功能传 输到日志服务器。设备应支持至少一种通用的远程标准日志接口，如SYSLOG、FTP 等。

WLAN 设备日志应支持记录与 WLAN 相关的安全事件。

WLAN 设备应能够按账号分配日志文件读取、修改和删除权限，从而防止日志文件被篡改或非法删除。

日志保存时间应满足：通过 WLAN 设备本地端口直接操作的系统操作日志本地保存不小于 7 天。

J.1.3 IP 协议安全要求

对于具备 TCP/UDP 协议功能的 WLAN 设备，应支持配置基于源 IP 地址、目的 IP 地址、通信协议类型（如 TCP、UDP、ICMP）、源端口、目的端口的流量过滤。

对于通过 IP 协议进行远程维护的 WLAN 设备，设备应支持使用 HTTPS、SSH 等加密协议。

对于通过 IP 协议进行远程维护的 WLAN 设备，应支持对允许登录到该设备的 IP 地址范围进行设定。

对于具备 TCP/UDP 协议功能的设备，应支持列出当前开放端口列表以及 WLAN 和其他设备连接情况。

J.1.4 设备其他安全要求

对于具备字符交互界面的 WLAN，应支持超时账户自动登出。登出后用户需再次登录才能进入系统。

对于具备图形界面（含 WEB 界面）的 WLAN，应支持手动和定时自动屏幕锁定。锁屏后需再次进行身份认证后才能解除屏幕锁定。

对于具备 console 口的 WLAN，应具备 console 口密码保护功能。

WLAN 应具备通过补丁升级消除软件安全漏洞的能力。

WLAN 应能够实现原厂安全补丁的加载，且不会对相关设备与业务运行造成不利影响。

J.2 AC 安全要求

无线控制器应支持无线频率自动选择，数据率设置，输出功率调整，信标间隔，前导帧设定和多 AP 间的负载均衡。

无线控制器应支持虚拟 AP 设置，以应用不同的安全接入策略。

无线控制器应支持配置文件的备份与恢复。

无线控制器应支持无线客户端隔离功能。

无线控制器应支持无线拒绝服务攻击检测功能。

无线控制器应支持各端口信息统计功能。
无线控制器应支持瘦 AP 在线监控功能。
无线控制器应支持无线终端监控功能。
无线控制器应支持非法 AP 识别功能。
无线控制器应支持日志记录功能。
无线控制器应支持 VLAN 设置，支持 VLAN 接口设置。
无线控制器应支持 MAC 与 AP 的绑定功能。
无线控制器应支持细化到 IP 的 DNS 访问控制策略。
无线控制器应支持 DNS 安全检测功能。
无线控制器应支持扩展型访问控制列表。
无线控制器应支持三/四层 DoS 防护功能。
无线控制器应支持 DHCP FLOOD 攻击检测功能。
无线控制器应能解析 AP 与 AC 之间的数据报文并且对内容进行有效识别，具体包括 STA 真实 IP 地址、STA 的 MAC 地址、STA 登录的用户名、STA 的源端口、STA 的目的端口、STA 的协议类型。
无线控制器应能支持对 IP、TCP、UDP 及 ICMP 协议的访问控制。
无线控制器应能够阻断异常的 CAPWAP 会话报文，防止 AC 的 AP 列表被恶意欺骗。
无线控制器应能检测 STA 提交大量的 DHCP 请求，防止 AC 的 DHCP地址池耗光攻击。
无线控制器应能检测针对 AC 的 Authentication Flood 攻击。
无线控制器应能检测具有欺骗性畸形特性的 Authentication Flood攻击。
无线控制器应能维护 STA 的真实 MAC 地址表。
无线控制器应能检测针对 AC 的 De-authentication Flood 攻击。
无线控制器 应能检测针 对 AC 的 Association Flood 攻 击 ， Association Flood 将导致 AP 过载，造成 AP 的拒绝服务，对 AP 上线、下线的跟踪。
无线控制器应能检测针对 AC 的 Disassociation Flood 攻击。

J.3 AP 安全要求

接入点应支持接入 VLAN 管理功能。
胖 AP 应能支持访问控制列表功能。
接入点应能支持对 AP 的扫描探测的检测与防护。
接入点应能支持对 AP 的缓冲区溢出攻击的防护。
接入点应能支持对 AP 的 config 文件泄露的检测与防护 。
接入点系统应能对 AP 开放的服务进行有效防护。
接入点应能提供一张可信 AP MAC 地址表，内容需要包括 AP 的 MAC地址和 IP 地址。
接入点应能支持无线钓鱼欺骗攻击的入侵检测。
接入点应能支持基于 WAPJack 攻击检测。
接入点应能支持 ARP 欺骗的检测。
接入点应能支持 AP 基于 IEEE 的 DOS 攻击检测。
接入点应能支持 Auth Dos 攻击入侵检测。
接入点应能支持 DNS 缓存服务器欺骗的的入侵检测。
接入点应能支持非法客户端连接 AP 检测。
接入点应能支持防止广播风暴抑制。
接入点应能支持 MAC/IP 用户限制策略。

接入点应能支持非法 AP 检测与干扰功能。
接入点应能支持 SSID 与 VLAN 绑定的功能。
接入点应能支持智能 RF 自愈合。
接入点应能支持 AD-HOC 网络检测。

J.4 热点交换机安全配置要求

热点交换机应能支持 VLAN 划分功能。
热点交换机应支持 ARP 攻击防护。
热点交换机应能支持端口安全检测功能。
热点交换机应能配置具有一定复杂度的 SNMP Community String。
热点交换机应能支持管理员权限的用户远程登录。
热点交换机应能支持网络监控管理的功能。
热点交换机应支能持 VTY 使用用户名和密码的方式进行连接验证。
热点交换机应能支持 ARP 入侵检测报警。
热点交换机应能支持 ACL 访问控制列表访问功能。
热点交换机应能支持 VPN 隧道接入功能。
热点交换机应能支持配置日志功能，记录用户对设备的操作，如账号创建、删除和权限修改，口令修改，读取和修改设备配置，读取和修 改业务用户的话费数据、身份数据、涉及通信隐私数据。记录需要包含用户账号，操作时间，操作内容以及操作结果。
热点交换机应能支持远程日志功能。所有设备日志均能通过远程日志 功能传输到日志服务器。设备应支持至少一种通用的远程标准日志接口，如 SYSLOG、FTP 等。
热点交换机应能支持端口镜像抓包功能。
热点交换机应能支持流量统计和限速功能。
热点交换机应能提供对 SNMP 的攻击防护检测。
热点交换机应能提供对 SSH 的攻击防护检测。
热点交换机应能提供对 FTP 的攻击防护检测。

J.5 Portal 系统安全功能要求

Portal 传输的 URL 中不应该包含 ACIP 等敏感信息。
用户登录时 Portal 应当针对用户提交数据进行加密传输。
在 PORTAL 服务器、AC 和 RADIUS 之间，通过 CHAP 协议保证用户认证信息的安全。
Potral 页面应支持保留用户 session 功能做鉴权。
鉴权提示信息要隐蔽关键业务逻辑，防止用户枚举账户。
Portal 相关页面中如果含有 js 代码，需要进行混淆，防止通过查看源代码对业务流程的攻击。
用户登录失败一定次数后系统自动锁定账号一段时间，以防止暴力猜测密码。
用户登录需提供图片验证码，以防止固定密码暴力猜测账号。
不能明文传输用户登录密码。
不能提供“保存登录”功能，该功能可能被利用于 CSRF 攻击。
合理进行纵向访问控制，不允许普通用户访问管理功能。
合理进行横向访问控制，不允许用户访问其他用户的敏感数据。
需要限制对敏感资源的访问，例如后台管理，日志记录等。

系统要防止将用户输入未经检查就直接输出到用户浏览器，防范跨站脚本攻击。

系统要防止将用户输入未经检查就用于构造数据库查询，防范 SQL注入攻击。

系统要防止将用户输入未经检查就用于构造文件路径，防止路径遍历攻击。

系统要防止将用户输入未经检查就用于构造操作系统命令并执行。

防止系统存在 LDAP 注入、XML 注入、XPATH 注入、SMTP 注入等漏洞。

系统需保证在正常与异常流程时都能正确释放不需要的资源，例如打开的文件，数据库连接等。

J.6 Radius 服务器安全功能要求

动态密码的下发时应下发具有一定复杂度的密码。

Radius 服务器应定期 30S 向客户端采集 session。

根据业务要求制定数据库审计策略。

用户数据存储采用不可逆的加密方式。

在 PORTAL 服务器、AC 和 RADIUS 之间，通过 CHAP 协议保证用户认证信息的安全。

附 录 K
（资料性附录）
密码技术要求

K.1 密码算法和密码协议

系统应用的密码算法应该采用国家密码管理部门认可的密码算法，并采用经国家密码管理部门安全性评审的密码协议实现密码功能。

1）对称密码算法

对称密码算法（SM1和SM4算法）。其中SM4密码算法的实现遵循GM/T 0002-2012。对称算法的工作模式应该使用CBC模式。对称密码算法主要用于数据加解密和密钥保护等。

2）非对称密码算法

SM2密码算法是非对称密码算法，SM2算法的实现遵循GM/T 0003-2012。

非对称密钥算法主要用于数字签名和验签、密码信封、密钥分发。

3）密码杂凑算法

SM3算法是密码杂凑算法，SM3算法的实现遵循GM/T 0004-2012。同时，SM2密码算法应用在数字签名验签和计算消息认证码时，算法要求配用SM3杂凑算法，在SM2密码算法中使用的SM3杂凑算法的实现遵循GM/T 0003-2012。

杂凑算法用于数字签名和验证、消息认证码生成与验证以及随机数生成。

K.2 密钥管理

密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档和销毁等环节进行管理和策略制定的全过程，并满足：

1）密钥生成：密钥生成过程中需要用到的随机数应使用SM3杂凑算法生成或者使用国家密码管理部门批准的硬件物理噪声源来产生随机数，随机数必须满足GM/T 0005-2012；系统应具备检查和剔除弱密钥的能力；生成密钥审计信息，密钥审计信息包括：种类、长度、拥有者信息、使用起始时间、使用终止时间。

2）密钥存储：密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；应具有密钥可能泄露时的应急处理和响应措施。

3）密钥分发：密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截获、假冒、篡改、重放等攻击，保证密钥的安全性。应具有密钥可能泄露时的应急处理和响应措施。

4）密钥导入与导出：密钥的导入与导出应采取有效的安全措施，保证密钥的导入与导出安全，以及密钥的正确；密钥的导入与导出应采用密钥分量的方式或者专用设备的方式；密钥的导入与导出应保证系统密码服务功能不间断。

5）密钥使用：密钥必须明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；应按照密钥更换周期要求更换密钥，密钥更换允许系统中断运行；密钥泄露时，必须停止使用，并启动相应的应急处理和响应措施。

6）密钥备份与恢复：应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

7）密钥归档：应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只

能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

9）密钥销毁：应具有在紧急情况下销毁密钥的措施。

K.3 密码技术应用要求

1）物理安全

物理安全基本技术要求在系统平台基础设施如电子门禁系统方面应当使用密码技术。在电子门禁系统中，应当使用密码技术的真实性服务来实现对进入重要区域人员的身份鉴别，并使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性。

2）网络安全

网络安全基本技术要求在安全访问路径、访问控制和身份鉴别方面应当使用密码技术。

在建立安全访问路径过程中，应当使用密码技术的真实性服务来保证通信主体身份鉴别信息的可靠，实现安全访问路径中通信主体身份的真实性应当使用密码技术的完整性服务来保证安全访问路径中路由控制信息的完整性。

在访问控制方面，应当使用密码技术的完整性服务来保证网络边界访问控制信息和数据敏感标记的完整性。

在审计记录方面，应当使用密码技术的完整性服务来对审计记录进行完整性保护。

在身份标识与鉴别方面，应当采用密码技术实现组合鉴别，使用密码技术的机密性和真实性服务来实现传输过程中鉴别信息防窃听、防假冒和防重用，保证网络设备用户身份的真实性。

3）主机安全

主机安全基本技术要求在身份鉴别、访问控制、安全信息传输路径、审计记录和程序安全方面可以使用密码技术。

在身份鉴别方面，应当采用密码技术来实现组合鉴别，使用密码技术的真实性服务来实现鉴别信息的防假冒和防重用，并在远程管理时使用密码技术的机密性服务来实现鉴别信息的防窃听。

在访问控制方面，应当使用密码技术的完整性服务来保证细粒度访问控制信息的完整性和所有主体和客体敏感标记的完整性。

在审计记录方面，应当使用密码技术的完整性服务来实现对审计记录和重要程序的完整性检测。

4）应用安全

应用安全基本技术要求在身份鉴别、访问控制、审计记录和通信安全方面应当使用密码技术。

在身份鉴别方面，应当采用密码技术来实现组合鉴别，使用密码技术的真实性和机密性服务来实现鉴别信息的防重用、防冒用、防泄露，保证应用系统用户身份的真实性在访问控制方面，应使用密码技术的完整性服务来保证主体对客体访问控制信息和敏感标记的完整性。

在建立安全的信息传输路径过程中，应当使用密码技术的真实性服务来实现通信主体身份鉴别，并综合使用密码技术的机密性和完整性服务来建立安全通道。

在审计记录方面，应使用密码技术的完整性服务来对审计记录进行完整性保护。

在通信安全方面，应当使用密码技术的完整性服务来保证通信过程中数据完整性；应当使用密码技术的真实性服务来实现通信双方会话初始化验证；应当使用密码技术的机密性服

务来实现对通信过程中整个报文或会话过程加密保护;应当使用密码技术的抗抵赖服务来提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

5）数据安全及备份恢复

数据安全及备份恢复基本技术要求在数据传输安全、数据存储安全和安全通信协议方面应当使用密码技术。

在数据传输安全方面，应使用密码技术的完整性服务来实现对系统管理数据、鉴别信息和重要业务数据在传输过程中完整性的检测;应使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的传输机密性。

在数据存储安全方面，应使用密码技术的完整性服务来实现对系统管理数据、鉴别信息和重要业务数据在存储过程中完整性的检测;应使用密码技术的机密性服务来实现系统管理数据、鉴别信息和重要业务数据的存储机密性。

在安全通信协议方面，应综合使用密码技术的真实性、完整性和机密性服务来建立安全通信协议。

参考文献

[1] GB/T 25069-2010 《信息安全技术 术语》
[2] GB/T 31167-2014 《信息安全技术 云计算服务安全指南》
[3] GB/T 31168-2014 《信息安全技术 云计算服务安全能力要求》
[4] GB/T31495.1-2015 《信息安全技术 信息安全保障指标体系及评价方法 第1部分：概念和模型》
[5] GB/T31495.2-2015 《信息安全技术 信息安全保障指标体系及评价方法 第2部分：指标体系》
[6] GB/T31495.3-2015 《信息安全技术 信息安全保障指标体系及评价方法 第3部分：实施指南》
[7] GB/T 17964-2008 《信息安全技术 分组密码算法的工作模式》
[8] GB/T 25056-2010 《信息安全技术 证书认证系统密码及其相关安全技术规范》
[9] GB/T 29827-2013 《信息安全技术 可信计算规范 可信平台主板功能接口》
[10] GB/T 29828-2013 《信息安全技术 可信计算规范 可信连接架构》
[11] GB/T 29829-2013 《信息安全技术 可信计算密码支撑平台功能与接口规范》
[12] GB/T 15843.5-2005 《信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制》
[13] GB/T 16264.8-2005 《信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架》
[14] GB/T 17902.2-2005 《信息技术 安全技术 带附录的数字签名 第2部分：基于身份的机制》
[15] GB/T 17902.3-2005 《信息技术 安全技术 带附录的数字签名 第3部分：基于证书的机制》
[16] GB/T 19713-2005 《信息技术 安全技术 公钥基础设施 在线证书状态协议》
[17] GB/T 19714-2005 《信息技术 安全技术 公钥基础设施 证书管理协议》
[18] GB/Z 19717-2005 《基于多用途互联网邮件扩展（MIME）的安全报文交换》
[19] GB/T 19771-2005 《信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范》
[20] GB/T 20518-2006 《信息安全技术 公钥基础设施 数字证书格式》
[21] GB/T 20519-2006 《信息安全技术 公钥基础设施 特定权限管理中心技术规范》
[22] GB/T 20520-2006 《信息安全技术 公钥基础设施 时间戳规范》
[23] GB/T 21053-2007 《信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求》
[24] GB/T 21054-2007 《信息安全技术 公钥基础设施 PKI 系统安全等级保护评估准则》
[25] GB/T 15843.1-2008 《信息技术 安全技术 实体鉴别 第1部分：概述》
[26] GB/T 15843.2-2008 《信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制》
[27] GB/T 15843.3-2008 《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》
[28] GB/T 15843.4-2008 《信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制》
[29] GB/T 15852.1-2008 《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的

机制》
[30] GB/T 15852.2-2008 《信息技术 安全技术 消息鉴别码 第 2 部分：采用专用杂凑函数的机制》
[31] GB/T 17710-2008 《信息技术 安全技术 校验字符系统》
[32] GB/T 17903.1-2008 《信息技术 安全技术 抗抵赖 第 1 部分：概述》
[33] GB/T 17903.2-2008 《信息技术 安全技术 抗抵赖 第 2 部分：采用对称技术的机制》
[34] GB/T 17903.3-2008 《信息技术 安全技术 抗抵赖 第 3 部分：采用非对称技术的机制》
[35] GB/T 25055-2010 《信息安全技术 公钥基础设施安全支撑平台技术框架》
[36] GB/T 25057-2010 《信息安全技术 公钥基础设施 电子签名卡应用接口基本要求》
[37] GB/T 25059-2010 《信息安全技术 公钥基础设施 简易在线证书状态协议》
[38] GB/T 25060-2010 《信息安全技术 公钥基础设施 X.509 数字证书应用接口规范》
[39] GB/T 25061-2010 《信息安全技术 公钥基础设施 XML 数字签名语法与处理规范》
[40] GB/T 25062-2010 《信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范》
[41] GB/T 25064-2010 《信息安全技术 公钥基础设施 电子签名格式规范》
[42] GB/T 25065-2010 《信息安全技术 公钥基础设施 签名生成应用程序的安全要求》
[43] GB/T 26855-2011 《信息安全技术 公钥基础设施 证书策略与认证业务声明框架》
[44] GB/T 28455-2012 《信息安全技术 引入可信第三方的实体鉴别及接入架构规范》
[45] GB/T 29241-2012 《信息安全技术 公钥基础设施 PKI 互操作性评估准则》
[46] GB/T 29242-2012 《信息安全技术 鉴别与授权 安全断言标记语言》
[47] GB/T 29243-2012 《信息安全技术 数字证书代理认证路径构造和代理验证规范》
[48] GB/T 29767-2013 《信息安全技术 公钥基础设施 桥 CA 体系证书分级规范》
[49] GB/T 30272-2013 《信息安全技术 公钥基础设施 标准一致性测试评价指南》
[50] GB/T 30274-2013 《信息安全技术 公钥基础设施 电子签名卡应用接口测试规范》
[51] GB/T 30275-2013 《信息安全技术 鉴别与授权 认证中间件框架与接口规范》
[52] GB/T 30277-2013 《信息安全技术 公钥基础设施 电子认证机构标识编码规范》
[53] GB/T 30280-2013 《信息安全技术 鉴别与授权 地理空间可扩展访问控制置标语言》
[54] GB/T 30281-2013 《信息安全技术 鉴别与授权 可扩展访问控制标记语言》
[55] GB/T 31501-2015 《信息安全技术 鉴别与授权 授权应用程序判定接口规范》
[56] GB/T 31503-2015 《信息安全技术 电子文档加密与签名消息语法》
[57] GB/T 31504-2015 《信息安全技术 鉴别与授权 数字身份信息服务框架规范》
[58] GB/T 31508-2015 《信息安全技术 公钥基础设施 数字证书策略分类分级规范》
[59] GB/T 32213-2015 《信息安全技术 公钥基础设施 远程口令鉴别与密钥建立规范》
[60] GB 17859-1999 《计算机信息系统 安全保护等级划分准则》
[61] GB/T 20008-2005 《信息安全技术 操作系统安全评估准则》
[62] GB/T 20009-2005 《信息安全技术 数据库管理系统安全评估准则》
[63] GB/T 20010-2005 《信息安全技术 包过滤防火墙安全评估准则》
[64] GB/T 20011-2005 《信息安全技术 路由器安全评估准则》
[65] GB/T 20270-2006 《信息安全技术 网络基础安全技术要求》
[66] GB/T 20271-2006 《信息安全技术 信息系统通用安全技术要求》
[67] GB/T 20272-2006 《信息安全技术 操作系统安全技术要求》
[68] GB/T 20273-2006 《信息安全技术 数据库管理系统安全技术要求》

[69] GB/T 20274.1-2006 《信息安全技术 信息系统安全保障评估框架 第1部分:简介和一般模型》
[70] GB/T 20276-2006 《信息安全技术 智能卡嵌入式软件安全技术要求（EAL4 增强级）》
[71] GB/T 20280-2006 《信息安全技术 网络脆弱性扫描产品测试评价方法》
[72] GB/Z 20283-2006 《信息安全技术 保护轮廓和安全目标的产生指南》
[73] GB/T 20987-2007 《信息安全技术 网上证券交易系统信息安全保障评估准则》
[74] GB/T 18018-2007 《信息安全技术 路由器安全技术要求》
[75] GB/T 20979-2007 《信息安全技术 虹膜识别系统技术要求》
[76] GB/T 20983-2007 《信息安全技术 网上银行系统信息安全保障评估准则》
[77] GB/T 21028-2007 《信息安全技术 服务器安全技术要求》
[78] GB/T 21050-2007 《信息安全技术 网络交换机安全技术要求（评估保证级3）》
[79] GB/T 21052-2007 《信息安全技术 信息系统物理安全技术要求》
[80] GB/T 20274.2-2008 《信息安全技术 信息系统安全保障评估框架 第2部分:技术保障》
[81] GB/T 20274.3-2008 《信息安全技术 信息系统安全保障评估框架 第3部分:管理保障》
[82] GB/T 20274.4-2008 《信息安全技术 信息系统安全保障评估框架 第4部分:工程保障》
[83] GB/T 22186-2008 《信息安全技术 具有中央处理器的集成电路（IC）卡芯片安全技术要求(评估保证级4增强级)》
[84] GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》
[85] GB/T 22240-2008 《信息安全技术 信息系统安全保护等级定级指南》
[86] GB/T 25058-2010 《信息安全技术 信息系统安全等级保护实施指南》
[87] GB/T 25063-2010 《信息安全技术 服务器安全测评要求》
[88] GB/T 25066-2010 《信息安全技术 信息安全产品类别与代码》
[89] GB/T 25070-2010 《信息安全技术 信息系统等级保护安全设计技术要求》
[90] GB/T 28448-2012 《信息安全技术 信息系统安全等级保护测评要求》
[91] GB/T 28449-2012 《信息安全技术 信息系统安全等级保护测评过程指南》
[92] GB/T 28452-2012 《信息安全技术 应用软件系统通用安全技术要求》
[93] GB/T 28451-2012 《信息安全技术 网络型入侵防御产品技术要求和测试评价方法》
[94] GB/T 28456-2012 《IPsec协议应用测试规范》
[95] GB/T 28457-2012 《SSL协议应用测试规范》
[96] GB/T 28458-2012 《信息安全技术 安全漏洞标识与描述规范》
[97] GB/T 29240-2012 《信息安全技术 终端计算机通用安全技术要求与测试评价方法》
[98] GB/T 29244-2012 《信息安全技术 办公设备基本安全要求》
[99] GB/T 29765-2013 《信息安全技术 数据备份与恢复产品技术要求与测试评价方法》
[100] GB/T 29766-2013 《信息安全技术 网站数据恢复产品技术要求与测试评价方法》
[101] GB/Z 29830.1-2013 《信息技术 安全技术 信息技术安全保障框架 第1部分:综述和框架》
[102] GB/Z 29830.2-2013 《信息技术 安全技术 信息技术安全保障框架 第2部分:保障方法》
[103] GB/Z 29830.3-2013 《信息技术 安全技术 信息技术安全保障框架 第3部分:保障方法分析》

[104] GB/T 20275-2013 《信息安全技术 网络入侵检测系统技术要求和测试评价方法》
[105] GB/T 20278-2013 《信息安全技术 网络脆弱性扫描产品安全技术要求》
[106] GB/T 20945-2013 《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》
[107] GB/T 30270-2013 《信息技术 安全技术 信息技术安全性评估方法》
[108] GB/T 30273-2013 《信息安全技术 信息系统安全保障通用评估指南》
[109] GB/T 30276-2013 《信息安全技术 信息安全漏洞管理规范》
[110] GB/T 30278-2013 《信息安全技术 政务计算机终端核心配置规范》
[111] GB/T 30279-2013 《信息安全技术 安全漏洞等级划分指南》
[112] GB/T 30282-2013 《信息安全技术 反垃圾邮件产品技术要求和测试评价方法》
[113] GB/Z 30286-2013 《信息安全技术 信息系统保护轮廓和信息系统安全目标产生指南》
[114] GB/T 18336.1-2015 《信息技术 安全技术 信息技术安全评估准则 第 1 部分：简介和一般模型》
[115] GB/T 18336.2-2015 《信息技术 安全技术 信息技术安全评估准则 第 2 部分：安全功能组件》
[116] GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第 3 部分：安全保障组件
[117] GB/T 20277-2015 信息安全技术 网络和终端隔离产品测试评价方法
[118] GB/T 20279-2015 信息安全技术 网络和终端隔离产品安全技术要求
[119] GB/T 20281-2015 信息安全技术 防火墙安全技术要求和测试评价方法
[120] GB/T 31499-2015 信息安全技术 统一威胁管理产品技术要求和测试评价方法
[121] GB/T 31502-2015 信息安全技术 电子支付系统安全保护框架
[122] GB/T 31505-2015 信息安全技术 主机型防火墙安全技术要求和测试评价方法
[123] GB/T 31506-2015 信息安全技术 政府门户网站系统安全技术指南
[124] GB/T 31507-2015 信息安全技术 智能卡通用安全检测指南
[125] GB/T 30284-2013 《信息安全技术 移动通信智能终端操作系统安全技术要求（EAL2 级）》
[126] GB/T 19715.1-2005 《信息技术 信息技术安全管理指南 第 1 部分:信息技术安全概念和模型》
[127] GB/T 19715.2-2005 《信息技术 信息技术安全管理指南 第 2 部分:管理和规划信息技术安全》
[128] GB/T 20269-2006 《信息安全技术 信息系统安全管理要求》
[129] GB/T 20282-2006 《信息安全技术 信息系统安全工程管理要求》
[130] GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》
[131] GB/Z 20985-2007 《信息技术 安全技术 信息安全事件管理指南》
[132] GB/Z 20986-2007 《信息安全技术 信息安全事件分类分级指南》
[133] GB/T 20988-2007 《信息安全技术 信息系统灾难恢复规范》
[134] GB/T 22080-2008 《信息技术 安全技术 信息安全管理体系 要求》
[135] GB/T 22081-2008 《信息技术 安全技术 信息安全管理实用规则》
[136] GB/T 24363-2009 《信息安全技术 信息安全应急响应计划规范》
[137] GB/Z 24364-2009 《信息安全技术 信息安全风险管理指南》
[138] GB/Z 24294-2009 《信息安全技术 基于互联网电子政务信息安全实施指南》
[139] GB/T 25067-2010 《信息技术 安全技术 信息安全管理体系审核认证机构的要求》

[140] GB/T 25068.3-2010 《信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护》
[141] GB/T 25068.4-2010 《信息技术 安全技术 IT网络安全 第4部分：远程接入的安全保护》
[142] GB/T 25068.5-2010 《信息技术 安全技术 IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护》
[143] GB/T 28447-2012 《信息安全技术 电子认证服务机构运营管理规范》
[144] GB/T 28450-2012 《信息安全技术 信息安全管理体系审核指南》
[145] GB/T 25068.1-2012《信息技术 安全技术 IT网络安全 第1部分：网络安全管理》
[146] GB/T 25068.2-2012 《信息技术 安全技术 IT网络安全 第2部分：网络安全体系结构》
[147] GB/T 28454-2012 《信息技术 安全技术 入侵检测系统的选择、部署和操作》
[148] GB/T 28453-2012 《信息安全技术 信息系统安全管理评估要求》
[149] GB/Z 28828-2012 《信息安全技术 公共及商用服务信息系统个人信息保护指南》
[150] GB/T 29245-2012 《信息安全技术 政府部门信息安全管理基本要求》
[151] GB/T 29246-2012 《信息技术 安全技术 信息安全管理体系 概述和词汇》
[152] GB/T 30271-2013 《信息安全技术 信息安全服务能力评估准则》
[153] GB/T 30283-2013 《信息安全技术 信息安全服务 分类》
[154] 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》
[155] GB/T 31496-2015 《信息技术 安全技术 信息安全管理体系实施指南》
[156] GB/T 31497-2015 《信息技术 安全技术 信息安全管理 测量》
[157] GB/T 31500-2015 《信息安全技术 存储介质数据恢复服务要求》
[158] GB/T 31509-2015 《信息安全技术 信息安全风险评估实施指南》
[159] GB/T 31722-2015 《信息技术 安全技术 信息安全风险管理》