ICS 13.310
CCS A 90

DB4401

广　州　市　地　方　标　准

DB4401/ T 10.31—2024
代替 DB4401/T 10.31—2019

反恐怖防范管理　第31部分：电信互联网

Anti-terrorism precaution management—Part 31: Telecommunications Internet

征求意见稿

2024-XX-XX 发布　　2024-XX-XX 实施

广州市市场监督管理局　发布

目　　次

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。

本文件为DB4401/T 10《反恐怖防范管理》的第31部分。本文件替代DB4401/T 10.31-2019《反恐怖防范管理　第31部分：电信互联网》。第一次修订前DB4401/T 10已经发布以下部分，后续修订时按实际工作需要进行调整。

——第1部分：通则；
——第2部分：党政机关；
——第3部分：广电传媒；
——第4部分：涉外机构；
——第5部分：教育机构；
——第6部分：医疗卫生机构；
——第7部分：商场超市；
——第8部分：酒店宾馆；
——第10部分：园林公园；
——第11部分：旅游景区；
——第12部分：城市广场和步行街；
——第14部分：大型专业市场；
——第15部分：体育场馆；
——第16部分：影视剧院；
——第17部分：会展场馆；
——第18部分：宗教活动场所；
——第20部分：港口码头；
——第21部分：公交客运站场；
——第22部分：隧道桥梁；
——第24部分：城市轨道交通；
——第25部分：水务系统；
——第26部分：电力系统；
——第27部分：燃气系统；
——第29部分：粮食和物资储备仓库；
——第30部分：金融机构；
——第31部分：电信互联网；
——第32部分：邮政物流；
——第33部分：危险化学品；
——第34部分：民用爆炸物品；
——第35部分：核与放射性物品；
——第36部分：传染病病原体；
——第37部分：大型活动；
——第38部分：高层建筑。

本文件替代DB4401/T 10.31-2019《反恐怖防范管理　第31部分：电信互联网》，与DB4401/T 10.31-2019相比，除结构调整和编辑性改动外，主要技术变化如下：

a） 更改了文件的适用范围，增加了其它新型信息基础设施；

b） 更改了规范性引用文件；

c） 增加了术语和定义“新型信息基础设施”，修改了术语和定义“电信互联网机房（楼）”“周界”，删除了术语和定义“电信”“互联网”“电信互联网运行维护单位”“反恐怖防范重点目标的分目标”“互联网数据中心”；

d） 修改第4章“反恐怖防范原则”；

e） “防范分类和防范等级”由第5章更改为第6章，删除“非常态反恐怖防范等级”一节；

f） “重点分目标及其重要部位”更改为“重点目标和重要部位”，并由第6章更改为第5章，并更改了重点目标和重要部位的内容；

g） 增加第7章“总体要求”；

h） 原第7章第1节“人防”更改为“常态人力防范”，独立成为第8章，并对人力防范配置表进行修改；

i） 原第7章第2节“物防”更改为“常态实体防范”，独立成为第9章，修改实体防范配置表和实体防范设备设施要求；

j） 原第7章第3节“技防”更改为“常态电子防范”，独立成为第10章，修改电子防范配置表和各子系统的要求，增加授时安全保护系统和反无人机系统的内容；

k） 原第7章第4节“制度防”更改为“常态制度防范”独立成为第11章，根据DB4401/T 10.1-2024《反恐怖防范管理　第1部分：通则》修改管理制度配置的内容；

l） “非常态反恐怖防范”由第8章更改为第12章，删除“非常态反恐怖防范实施”和“非常态反恐怖防范措施”两节内容；

m） 不再规范性引用DB4401/T 10.1《反恐怖防范管理　第1部分：通则》内容，将相关条款直接引用在文本中。

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专利的责任。

本文件由广州市反恐怖工作领导小组办公室和广州市工业和信息化局共同提出。

本文件由广州市反恐怖工作领导小组办公室归口。

本文件起草单位：

本文件主要起草人：

本文件于2019年首次发布，本次为第一次修订。

引　言

广州市地方标准DB4401/T 10.31-2019《反恐怖防范管理 第31部分：电信互联网》(以下简称《电信互联网》)自发布以来，经过多年实施，取得良好的效果。以《电信互联网》为重要抓手开展电信互联网领域反恐怖防范工作，反恐怖防范管理标准宣传持续深入，社会面反恐怖防范意识、能力和参与程度大幅提升。

近年来，国家和省、市相继制定印发文件规范和有关标准，对电信互联网领域的反恐怖防范管理提出了新的要求，为进一步与各级文件规范、标准要求保持一致，完善电信互联网领域反恐怖防范管理标准，提高标准可行性、科学性，同时简化标准结构，提高标准可读性，按照市反恐怖工作领导小组的工作部署，市反恐办启动《电信互联网》修订工作。

本文件为DB4401/T 10《反恐怖防范管理》的第31部分。本文件在DB4401/T 10.1-2024《反恐怖防范管理 第1部分：通则》和DB4401/T 10.31-2019《反恐怖防范管理 第31部分：电信互联网》的基础上，根据行业的特点以及新的政策文件要求，明确了电信互联网领域的反恐怖防范要求，使其更有针对性、有效性和适用性。

反恐怖防范管理 第31部分：电信互联网

1 范围

本文件规定了电信互联网反恐怖防范管理的术语和定义、反恐怖防范原则、反恐怖防范重点目标和重要部位、防范分类和防范等级、总体要求、常态人力防范、常态实体防范、常态电子防范、常态制度防范、非常态防范要求、应急准备要求和监督、检查。

本文件适用于提供电信服务、互联网信息服务或政务信息服务的机房（楼）和其它新型信息基础设施等重点目标的反恐怖工作和管理，反恐怖防范一般目标可参照执行。

2 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,仅该日期对应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 2887 计算机场地通用规范

GB/T 2893.5 图形符号 安全色和安全标志 第5部分：安全标志使用原则与要求

GB 10408.1 入侵探测器 第1部分:通用要求

GB 12663 入侵和紧急报警系统 控制指示设备

GB 12664 便携式X射线安全检查设备通用规范

GB 12899 手持式金属探测器通用技术规范

GB 15208.1 微剂量X射线安全检查设备 第1部分：通用技术要求

GB 15210 通过式金属探测门通用技术规范

GB/T 15408 安全防范系统供电技术要求

GB 16796 安全防范报警设备 安全要求和试验方法

GB 17565 防盗安全门通用技术条件

GB 17945 消防应急照明和疏散指示系统

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25724 公共安全视频监控数字视音频编解码技术要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 31488 安全防范视频监控人脸识别系统技术要求

GB/T 32581 入侵和紧急报警系统技术要求

GB 35114 公共安全视频监控联网信息安全技术要求

GB/T 36546 入侵和紧急报警系统 告警装置技术要求

GB/T 37078 出入口控制系统技术要求

GB 37300 公共安全重点区域视频图像信息采集规范

GB 50198 民用闭路监视电视系统工程的技术要求

GB 50348 安全防范工程技术规范

GB 50394 入侵报警系统工程设计规范
GB 50395 视频安防监控系统工程设计规范
GB 50396 出入口控制系统工程设计规范
GB/T 50526 公共广播系统工程技术规范
GB 55029 安防工程通用规范
GA 68 警用防刺服
GA 69 防爆毯
GA 294 警用防暴头盔
GA/T 367 视频安防监控系统技术要求
GA/T 368 入侵和紧急报警系统技术要求
GA 422 警用防暴盾牌
GA/T 594 保安服务操作规程与质量控制
GA 614 警用防割手套
GA/T 644 电子巡查系统技术要求
GA/T 669.1 城市监控报警联网系统 技术标准 第1部分:通用技术要求
GA 872 防爆球
GA 883 公安单警装备 强光手电
GA 926 微剂量透射式X射线人体安全检查设备通用技术条件
GA/T 1126 近红外人脸识别设备技术要求
GA/T 1127 安全防范视频监控摄像机通用技术要求
GA/T 1132 车辆出入口电动栏杆机技术要求
GA/T 1145 警用约束叉
YD/T 1363 通信局（站）电源、空调及环境集中监控管理系统
YD/T 1666 远程视频监控系统的安全技术要求
YD/T 1806 基于IP的远程视频监控设备技术要求
YD/T 2883 电信网视频监控系统视音频编解码技术要求

3 术语和定义

DB4401/T 10.1—2024界定的以及下列术语和定义适用于本文件。

3.1

新型信息基础设施 new information infrastructure

5G网络、光纤宽带网络、骨干网络、国际通信网络、卫星互联网等网络基础设施，数据中心、通用算力中心、智能计算中心、超算中心等算力基础设施，人工智能、区块链、量子计算等新技术设施。

3.2

电信互联网重点目标管理单位 telecommunications Internet key prevention targets management unit

提供电信服务、互联网信息服务、政务信息服务以及其他信息服务的主体责任单位。

3.3

机房（楼） information technology equipment room（building）

为计算机设备、通信设备、服务器等设备提供稳定的运行环境的建筑物或场所。

3.4

周界 perimeter

保护对象的区域边界。

[来源：GB 50348-2018，2.0.30]

4 反恐怖防范原则

4.1 电信互联网的反恐怖防范应遵循“预防为主、突出重点、保障安全”，“谁运营、谁负责”的工作原则。

4.2 电信互联网的反恐怖防范工作应在反恐怖主义工作领导机构统一领导和指挥下开展，公安机关履行安全管理、监督和检查责任，行业指导部门履行指导责任。

4.3 电信互联网重点目标管理单位应按照反恐怖主义法等法律法规的相关要求履行职责，建立反恐怖防范系统，开展反恐怖防范工作。

5 重点目标和重要部位

5.1 重点目标

5.1.1 电信互联网反恐怖防范重点目标主要有：提供电信服务、互联网信息服务或政务信息服务的机房（楼）和其它新型信息基础设施。

5.1.2 重点目标的等级由低到高分别为三级、二级、一级。

5.2 重要部位

电信互联网反恐怖防范重要部位主要有：机房、主要出入口、周界、门卫室、保安装备存放室、储油库、配电房、蓄电池室、发电房、空调系统风柜房、网络管理监控室、安防监控中心、消防控制室等重要设施设备房间和人员密集场所。

6 防范分类和防范等级

6.1 反恐怖防范按防范管理性质分为常态反恐怖防范和非常态反恐怖防范两类，非常态防范应在常态防范要求基础上加强。

6.2 常态反恐怖防范等级对应重点目标等级分别为三级防范、二级防范、一级防范。

7 总体要求

7.1 电信互联网重点目标管理单位在新建、改建、扩建重点目标时，反恐怖防范系统应与主体工程同步规划、同步设计、同步建设、同步验收、同步运行。已建、在建的重点目标应按本文件要求补充完善反恐怖防范系统。

7.2 电信互联网重点目标管理单位应根据公安机关和有关部门的要求及时报告防范措施落实情况，提供重点目标的相关信息和重要动态。

7.3　电信互联网重点目标管理单位的网络与信息系统应按 GB/T 22240 明确安全保护等级，采取 GB/T 22239 中相应的安全保护等级的防护措施；并能在发生或可能发生网络入侵、网络攻击以及信息泄露、篡改、丢失等情况时立即采取补救措施。

7.4　电信互联网重点目标管理单位的安全防范系统中涉及公民个人信息的，应依法依规进行处理，包括收集、存储、使用、加工、传输、提供、公开、删除等。

7.5　电信互联网重点目标管理单位应满足人力防范配置、实体防范配置和电子防范配置等的要求或者以等同的防范措施实现其要求；若配置的设备设施已集成两种及以上的配置要求，不需要再配备单一的设备设施。

7.6　电信互联网重点目标管理单位应建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。

8　常态人力防范

8.1　人力防范组织

8.1.1　电信互联网重点目标管理单位应设立与防范任务相适应的反恐怖防范工作机构及责任部门。

8.1.2　电信互联网重点目标管理单位的主要负责人为反恐怖防范管理第一责任人，对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

8.1.3　配备专（兼）职工作人员，负责反恐怖防范的具体工作；并应指定反恐联络员 1 名，联络员应确保 24 小时通信畅通。主要负责人、联络员的配置和变更，应及时向行业主管部门、属地公安机关和反恐怖主义工作领导机构的办事机构备案。

8.1.4　电信互联网重点目标管理单位应明确反恐怖防范重要岗位，重要岗位人员主要包括：网络管理监控人员、网络安全管理人员、安防监控人员、技防系统管理人员、电力维护人员和消防值守人员等。

8.2　人力防范配置

电信互联网的人力防范配置应符合表1要求。

表 1　人力防范配置表

序号	配置项目		三级防范	二级防范	一级防范
1	安保力量		专/兼职	专职	专职
2	岗位要求	安防监控岗	24 小时值守	24 小时值守，每班不少于2人，每1小时轮巡一次。	24 小时值守，每班不少于2人，每30分钟轮巡一次。
3		周界出入口门岗	--	24 小时值守，对外来人员、车辆、物资登记核查	24 小时值守，对外来人员、车辆、物资登记核查
4		巡逻岗	配备与巡逻计划相适应的安保力量	配备与巡逻计划相适应的安保力量，重要部位巡逻间隔应不大于8小时，每组每班不少于2人	配备与巡逻计划相适应的安保力量，重要部位巡逻间隔应不大于2小时，每组每班不少于2人
5		网络安全管理岗	24小时值守	24小时值守	24小时值守

序号	配置项目	三级防范	二级防范	一级防范
6	反恐怖教育培训	每年至少组织1次	每半年至少组织1次	每半年至少组织1次
7	联动性综合演练	每年至少组织1次	每半年至少组织1次	每半年至少组织1次

8.3 人力防范要求

8.3.1 电信互联网重点目标管理单位应按照要求配备足够的安保力量，明确常态安保力量数量和相关工作岗位职责。

8.3.2 对重要岗位人员开展背景审查、考核、建立人员档案并备案，同时签订保密协议，确保用人安全。

8.3.3 电信互联网重点目标管理单位配置的安保力量应符合反恐怖防范工作的需要，并应符合以下要求：

a) 保安员应按 GA/T 594 的相关要求，承担安保职责；
b) 安保力量应了解国家有关法律、法规、规章、标准等规定，熟悉掌握本单位反恐怖防范职责、纪律制度等要求；
c) 安保力量应熟悉机房（楼）、数据中心等重点目标和重要部位的地理环境及主要设施布局，熟悉消防通道和各类疏散途径；
d) 安保力量应熟悉重点目标关键设备的操作规程或系统的作业指导书；
e) 具有应对电信互联网相关涉恐突发事件的能力，能协助、配合反恐怖主义工作领导机构、公安机关和行业指导部门开展应急处置工作；
f) 安保力量包括保安人员、巡查人员、机动人员、管理监控人员、电力维护人员和消防值守人员等。
g) 电信互联网重点目标管理单位应根据有关规定，结合目标规模、人员数量、重要部位分布等反恐怖防范工作实际需要，配备足够的安保力量，明确常态安保力量人数。
h) 其他需承担的反恐怖防范工作。

8.3.4 电信互联网重点目标管理单位应考虑网络安全威胁风险配备网络管理员。网络管理员应熟悉网站和信息系统的安全机制，按网络安全管理制度开展网络安全防范工作。重点目标中存在符合 GB/T 22240 中安全保护等级第二级网络系统的应设置专/兼职网络安全管理员，存在符合第三级及以上等级网络系统的应设置专职网络安全管理员。

8.3.5 电信企业应定期组织巡检人员进行反恐怖防范培训，包括但不限于反恐法律法规、应急处置流程、个人防护装备使用等内容，确保巡检人员具备应对突发恐怖事件的能力。

9 常态实体防范

9.1 实体防范配置

9.1.1 应根据场地条件合理规划周界实体屏障的位置，周界实体屏障的防护面一侧的区域内不应有可供攀爬、钻入的物体或设施。

9.1.2 电信互联网重点目标出入口宜设置实体屏障:人员、车辆出入口宜分开设置；无人值守的出入口的防护能力应与周界实体屏障相当。

9.1.3 应在必要位置设置明显的警示标志，警示标志尺寸、颜色、文字、图像、标识应符合相关规定。

9.1.4　电信互联网重点目标重要部位建(构)筑物的洞口、管沟、管廊、吊顶、风管、桥架、管道等空间尺寸能够容纳人进入时，应有实体屏障封闭或阻挡。

9.1.5　穿越周界的河道、涵洞、管廊等孔洞，应有相应的实体防护措施。

9.1.6　电信互联网的实体防范应符合表2要求。

表2　实体防范配置表

序号	配置项目		安放区域或位置	设置要求		
				三级	二级	一级
1	实体防护设施	机动车阻挡装置	机房（楼）与外界相通的主要出入口或所在院落与外界相通的主要出入口	宜设	应设	应设
2		防暴阻车路障或隔离设施	机房（楼）或所在院落与外界相通且未做人车分流的主要出入口、受机动车冲击后容易受到重大伤害的部位	宜设	应设	应设
3		防盗安全门、金属防护门	机房、网络管理监控室、安防监控中心、储油库、配电房、空调系统风柜房等重要部位出入口	应设	应设	应设
4		围墙或栅栏等实体防护屏障	机房（楼）周界	应设	应设	应设
5		栅栏	直接与外界相通的一、二楼无人值守的机房窗户	应设	应设	应设
6			网络管理监控室、安防监控中心	应设	应设	应设
7		行李箱包寄存设施	机楼出入口	宜设	应设	应设
8		警示标志	机房、蓄电池室、配电房、储油库等重要设备场所、应急疏散通道	应设	应设	应设
9	个人应急防护装备	对讲机、强光手电、防护棍棒	安保力量、安防监控中心、门卫室、保安装备存放处	应设	应设	应设
10		防暴盾牌、钢叉	安防监控中心、门卫室（安保岗位）、保安装备存放处	宜设	应设	应设
11		防暴头盔、防割（防刺）手套、防刺服	安防监控中心、门卫室（安保岗位）、保安装备存放处	宜设	应设	应设
12	公共应急防护装备	防爆毯（含防爆围栏）	主要出入口、门卫室、值班室、保安装备存放处	宜设	应设	应设
13		防爆球（罐）	人员密集场所安检区	宜设	宜设	宜设
14		照明灯光	人员密集场所、应急疏散通道	宜设	应设	应设
15	消防设施设备	气体灭火系统	交换机房、配电房等通信、电力设备机房	宜设	应设	应设
16		灭火器	蓄电池室、配电房、储油库等重要设备场所、门卫室、安防监控中心	应设	应设	应设
17		防烟、排烟系统	机房、蓄电池室、配电房等重要设备场所、安防监控中心	宜设	应设	应设
18		防火分隔设施	机房、蓄电池室、配电房等重要设备场所、安防监控中心	宜设	应设	应设

9.1.7　出入口门卫室和设在建筑物二层以下的监控中心应配置防盗窗或护栏。

9.2　实体防护设备设施要求

实体防护配置的设备设施应符合以下要求：

a） 机动车阻挡装置宜采用电动可伸缩闸门或电动栏杆，电动栏杆应符合 GA/T 1132 的要求；

b） 防机动车冲撞或隔离设施应符合 DB4401/T 43 的要求；

c） 机房及监控室应采用金属防盗防火安全门；

d） 防盗安全门应符合 GB 17565 的要求；防尾随联动互锁安全门应符合 GA 576 的要求；

e） 围墙或栅栏等实体防护屏障应采用砖、石、混凝土或金属材料，并在其上方设置防攀爬、防翻越障碍物。周界实体屏障及附属封闭设施应能有效阻隔人员进入；

f） 警示标志应符合 GB/T 2893.5 的要求；

g） 应急报警器应符合 GB 16796 的要求；

h） 强光手电应符合 GA 883 的要求；

i） 防暴盾牌应符合 GA 422 的要求；

j） 防暴钢叉应符合 GA/T 1145 的要求；

k） 防暴头盔应符合 GA 294 的要求；

l） 防割（防刺）手套应符合 GA 614 的要求；

m） 防刺服应符合 GA 68 的要求；

n） 防爆毯应符合 GA 69 的要求；

o） 防爆球应符合 GA 872 的要求；

p） 应急照明应符合 GB 17945 的要求。

10 常态电子防范

10.1 电子防范配置

10.1.1 电信互联网重点目标的电子防范配置应符合表 3 要求。

表 3 电子防范配置表

序号	配置项目		安放区域或位置	配置要求		
				三级	二级	一级
1	视频监控系统	摄像机	重要部位全覆盖	应设	应设	应设
2		人脸识别装置	机楼出入口、安防监控中心出入口等主要出入口	应设	应设	应设
3		终端图形显示装置	安防监控中心	应设	应设	应设
4	入侵和紧急报警系统	入侵探测（报警）器	周界、与外界想通的重要部位或机房、电力室、储油库等无固定人员值守的重要部位	宜设	应设	应设
5		紧急报警装置	门卫室、机房、储油库、安防监控中心、消防控制室	宜设	应设	应设
6		控制指示设备	安防监控中心	宜设	应设	应设
7		报警控制器	安防监控中心、门卫室	宜设	应设	应设

序号	配置项目	安放区域或位置	配置要求		
			三级	二级	一级
8	出入口控制系统	机楼、配电房、空调系统风柜房、机房、电力室、高低压变配电室、变压器室、蓄电池室、发电房、冷冻机房、通风机房、水泵房、电缆充气控制室、电（光）缆进线室等设备房、储油库、安防监控中心	应设	应设	应设
9	电子巡查系统（巡更系统）	机楼周界、出入口、门厅、楼层出入口、主要通道、电梯轿厢内、核心机房、储油库、电力室、高低压变配电室、变压器室、蓄电池室、发电房、冷冻机房、通风机房、水泵房、电缆充气控制室、电（光）缆进线室等备机房、安防监控中心、消防控制室	应设	应设	应设
10	公共广播系统	重要部位全覆盖	宜设	宜设	应设
11	安防监控系统	安防监控中心	宜设	应设	应设
12	火灾自动报警系统	重要部位全覆盖	应设	应设	应设
13	授时安全防护系统	卫星授时信号接收装置	宜设	应设	应设
14	反无人机系统		宜设	宜设	宜设

10.1.2　应根据现场环境和反恐怖防范要求合理配置视频监控设备。

10.1.3　周界和出入口等部位应考虑视频图像智能分析技术的应用。

10.1.4　电信互联网重点目标管理单位宜根据反恐怖防范需要和防御非法入侵的能力，选用出入口控制系统的识读技术类型等。

10.1.5　电信互联网重点目标管理单位可根据安全检查的需求，增设X射线物品安检机、通过式金属探测门、爆炸物探测仪或液体检查设备。

10.1.6　电信互联网重点目标管理单位应结合防范的需求，增设反无人机系统。

10.1.7　电信互联网重点目标管理单位使用卫星时间同步装置的，应增设授时安全防护装置。装置宜具备常规电磁干扰信号入侵监测和实时告警能力、卫星信号拒止条件下高精度时间同步保持和干扰信号安全隔离能力，宜具备北斗信号原位加固授时防护与GPS信号安全隔离的能力。

10.1.8　授时安全防护装置直接串行接入时间同步装置/时间服务器与卫星天线之间；应在原有的授时设备上加装授时防火墙，卫星信号安全防护装置；通过加装时空防护装置，可以在不更换原有时间同步装置的前提下，实现预防卫星信号的干扰和欺骗。

10.2　电子防范设备设施要求

10.2.1　基本要求

电信互联网的反恐怖电子防范应满足以下要求：

a)　电子防范系统应满足GB 50348、GB 55029的要求；

b)　电子防范系统的供电应符合GB/T 15408的相关要求；

c)　监控中心应符合GB/T 2887的相关要求；

d)　应对电子防范系统内具有计时功能的设备进行校时，设备的时钟与北京时间误差应不大于5秒；

e） 电子防范系统的设备和材料应符合相关标准并检验合格。
f） 承载安防信息的信息系统应符合 GB/T 22239 和 GB/T 22240 中相应规定，一级和二级重点目标重要部位的承载安防信息的信息系统应符合 GB/T 22239 中第二级网络安全保护等级要求。
g） 备用电源应具备持续供电能力，持续供电时间应不低于 12h，选用满足相应技术条件的供电质量高的发电机组、动态储能不间断供电装置、静态储能装置或采用静态储能装置与发电机组的组合作为备用电源；备用电源的允许断电时间为毫秒级，应选用满足相应技术条件的静态储能不间断电源或动态不间断电源且采用自动切换功能。

10.2.2 建设应用要求

电子防范各子系统的建设和使用应符合以下要求：
a） 视频监控系统应符合 GB 50198、GB 50395、GB/T 25724、GB/T 28181、GA/T 367 和 GA/T 1127 的要求；
b） 人脸识别系统应符合 GB/T 31488 和 GA/T 1126 的要求；
c） 入侵报警系统应符合 GB 12663、GB/T 32581 和 GB 50394 的要求；
d） 出入口控制系统应符合 GB/T 37078 的要求；
e） 电子巡查系统应符合 GA/T 644 的要求；
f） 公共广播系统应符合 GB/T 50526 的要求；
g） 防爆安检系统应符合 GB 12664、GB 12899、GB 15208.1、GB 15210 和 GA 926 的要求。

10.2.3 安防监控中心要求

安防监控中心应符合以下要求：
a） 安防监控中心应符合 GB/T 2887、GB 50348、YD/T 1363 的相关要求；
b） 安防监控中心应有控制、记录、显示装置；
c） 视频监控系统、入侵和紧急报警系统、出入口控制系统、电子巡查系统等各子系统设备终端均应设在监控中心，能实现对各子系统的操作、记录和打印；
d） 配置能与报警同步的终端图形显示装置，能准确地识别报警区域，实时显示发生警情的区域、日期、时间及报警类型等信息；
e） 主要出入口监控系统应接入管辖公安机关指挥部门、辖区派出所；
f） 安防监控中心疏散门应采用外开方式，且应自动关闭，并应保证在任何情况下均能从室内开启。

10.2.4 视频监控系统要求

视频监控系统应符合以下要求：
a） 电信互联网重点目标的重要部位应设置视频监控装置，监视及回放图像的水平像素数应不小于 1920，垂直像素数应不小于 1080，视频图像帧率应不小于 25 帧每秒，且能清晰显示区域内人员活动情况、车辆通行情况。配置的视频图像采集装置应满足 GA/T 1127-2013 中规定的 C 类高清晰度及以上要求，具有宽动态、低照度、强光抑制等功能的机型，视频信息系统应能与公安机关联网；
b） 周界部署的视频图像采集装置宜有入侵探测(报警)布防功能；
c） 视频录像保存时间应不少于 90 日；
d） 视频监控系统的备用电源应满足至少 4h 正常工作的需要。
e） 视频监控系统应留有与公共安全视频图像信息共享交换平台联网的接口，联网信息传输、交换、控制协议应符合 GB/T 28181 的相关规定，联网信息安全应符合 GB 35114 的相关规定。
f） 涉及公共区域的视频图像信息的采集要求应符合 GB 37300 的相关规定；

g) 视频监控系统应具有对图像信号的采集、传输、切换控制、显示、分配、记录和重放等基本功能。系统应集成声音复核装置、视频智能分析系统、人脸识别系统等功能。视频监控系统应同时满足 GB 50198、GB 50395、GA/T 367、GA/T 669.1、YD/T 1666、YD/T 1806、YD/T 2883 的要求；
h) 视频监控系统应采用数字系统；
i) 视频监控范围内的报警系统发生报警时，应与该视频系统联动。辅助照明灯光应满足视频系统正常摄取图像的照度要求；
j) 宜支持 H.264、H.265 或 MPEG-4 视频编码格式和文件格式进行图像存储，宜支持 G.711、G.723.1、G729 等音频编解码标准实现音频同步存储，新建、改建、扩建视频监控系统的视音频编解码宜优先采用 GB/T 25724 对监控数字视音频编解码技术的要求。

10.2.5 入侵和紧急报警系统要求

入侵和紧急报警系统应符合以下要求：

a) 入侵和紧急报警系统应符合 GB 12663、GB 16796、GB/T 32581、GB/T 36546、GB 50394、GA/T 368、GB 50348 等入侵和紧急报警系统相关标准的要求；
b) 入侵探测器应符合 GB 10408.1 和相应的国家标准要求；
c) 室内报警声压不宜低于 80dB，室外报警声压不宜低于 100dB；
d) 入侵和紧急报警系统应能探测报警区域内的入侵事件，系统报警后，安防监控中心(室)应能有声、光指示，并能准确指示发出报警的位置，报警信号保持至人工操作复位；
e) 入侵和紧急报警系统应具备防拆、开路、短路报警功能；
f) 入侵和紧急报警系统应具备自检功能和故障报警、断电报警功能；
g) 视频监控范围内的报警系统发生报警时，应与该视频系统联动，报警响应时间应不大于 2 秒，辅助照明灯光应满足视频系统正常摄取图像的照度要求；
h) 入侵和紧急报警系统布防、撤防、故障和报警信息存储时间应不少于 180 日，并具备与公安机关联动的接口；
i) 入侵报警装置应有明显的警告标志；
j) 入侵和紧急报警系统备用电源应满足至少 24h 正常工作的需要。

10.2.6 出入口控制系统要求

出入口控制系统应符合以下要求：

a) 出入口控制系统应满足 GB/T 37078、GB 50396 等出入口控制系统相关标准的要求；
b) 出入口控制系统备用电源应满足至少 48h 正常工作的需要；
c) 出入口控制系统应能对强行破坏、非法进入的行为发出报警信号，报警信号应与相关出入口的视频图像联动；
d) 出入口控制系统宜具备在线巡查管理功能，门禁读卡器可作为巡查信息装置；
e) 出入口控制系统应满足紧急逃生时人员疏散的相关要求；
f) 出入口控制系统信息存储时间应不少于 180 日；
g) 出入口控制系统宜具备对重要部位防火门开关状态的监测功能，并具备远程开锁控制功能；
h) 出入口控制系统授权等级宜根据电信互联网重点目标管理单位对安全防范的总体要求进行设定。

10.2.7 电子巡查系统要求

电子巡查系统应符合以下要求：

a) 电子巡查系统应满足 GA/T 644 的相关要求；
b) 电子巡查系统应具备巡查路线偏离报警、规定时间无位移报警等功能；
c) 电子巡查系统的巡查路线、巡查时间应能根据安全管理需要进行设定和修改，并覆盖重要部位；
d) 电子巡查系统可独立设置，也可基于出入口控制系统组合设置。

10.2.8 公共广播系统要求

公共广播系统应符合以下要求：
a） 公共广播系统应符合 GB/T 50526 相应规定；
b） 当发生安全事件时，公共广播系统应能根据应急预案中确定的处置流程，进行公共安全信息播报与发布，并能有效指引各岗位人员处置突发状况；
c） 广播系统（含音频和视频）应常态化开展反恐怖防范安全教育。

10.2.9 无线通信对讲指挥调度系统要求

无线通信对讲指挥调度系统应符合以下要求：
a） 无线通信对讲指挥调度系统覆盖的时间地点概率不应小于 90%，并覆盖重要部位；
b） 无线通信对讲指挥调度系统应提供在岗的安保人员、网络管理监控人员、安防监控人员、电子防范系统管理人员、巡查岗位人员、机动岗位人员、电力维护人员和消防岗位人员等用户之间的通信手段。

10.2.10 授时安全防护系统

授时安全防护系统应符合以下要求：
a） 在能够接收到授时所必需的卫星信号条件下，受到欺骗或干扰时，不应输出异常的时间信号；
b） 检测到欺骗信号时，应输出告警信息；
c） 当干扰会导致接收卫星信号中断时，应输出告警信息。

10.2.11 反无人机系统

反无人机系统应符合以下要求：
a) 系统应能自动 24h 持续工作，无需人员值守；
b) 系统不应对周边重要设施产生有害干扰；
c) 系统不应对电信互联网授时产生影响。

11 制度防范

11.1 管理制度配置

重点目标的管理制度配置应符合表 4 要求。

表 4 管理制度配置

序号	项目		配置要求
1	人力防范	教育培训及考核制度	按附录 A 中的 A.3.1
2		人员背景审查制度	按附录 A 中的 A.3.2
3		人员档案及备案制度	按附录 A 中的 A.3.3
4		门卫与寄递物品管理制度	按附录 A 中的 A.3.4

序号	项目		配置要求
5		巡查制度	按附录A中的A.3.5
6		安全检查制度	按附录A中的A.3.6
7		值班监看和运维制度	按附录A中的A.3.7
8		训练演练制度	按附录A中的A.3.8
9		检查督导制度	按附录A中的A.3.9
10		人防增援配置制度	按附录A中的A.3.10
11	实体防范、电子技防	采购管理制度	按附录A中的A.3.11
12		设备设施档案制度	按附录A中的A.3.12
13		技防系统管理制度	按附录A中的A.3.13
14	综合	工作报告制度	按附录A中的A.3.14
15		网络安全管理制度	按附录A中的A.3.15
16		专项经费保障制度	按附录A中的A.3.16
17		情报信息管理制度	按附录A中的A.3.17
18		恐怖威胁风险评估制度	按附录A中的A.3.18
19		联动配合机制	按附录A中的A.3.19
20		应急管理制度	按附录A中的A.3.20
21		应急预案管理制度	按附录A中的A.3.21
22		保密制度	按附录A中的A.3.22

11.2 岗位标准配置

11.2.1 制定重点目标管理单位责任领导、责任部门的正（副）职、联络员等岗位标准，应包括反恐怖防范工作职责和权限。

11.2.2 在安保、网络管理监控、网络安全管理、安防监控、技防系统管理、巡查岗位、机动岗位、电力、消防等工作岗位的标准中，要明确人员的配置标准、资质条件、操作规范和权限等，细化每个岗位工作细节及与其他岗位人员协调、配合、交接的操作流程。

11.2.3 制定考核条件和奖惩办法，明确检查、考核部门、时间要求，明确考核程序和考核办法，应有考核记录。

11.3 操作规程配置

11.3.1 配备反恐怖安全防范系统中有关设备设施涉及到国家、行业、地方的标准及文件。

11.3.2 配备反恐怖防范工作中关键设备的操作规程或系统的作业指导书。

11.4 制度防范要求

11.4.1 重点目标管理单位应制定反恐怖防范管理组织制度，明确责任领导的管理职责和责任部门的工作职责。配置专人负责反恐怖防范制度管理工作，所有制度文件应受控，确保制度的宣贯、实施与持续改进。

11.4.2 重点目标管理单位建立健全包括值守、巡逻、培训、检查、考核、反恐怖防范系统运行与维护等制度。

11.4.3 重点目标管理单位应建立反恐怖防范系统建设、运行与维护的保障体系和长效机制。

11.4.4　重点目标管理单位应建立反恐怖工作专项经费保障制度，将反恐怖防范涉及费用纳入企业预算、成本，保障反恐怖防范工作机制运转正常。
11.4.5　重点目标管理单位应与属地公安机关等有关部门和单位建立联防、联动、联治工作机制。
11.4.6　重点目标管理单位应建立反恐怖与安全生产等有关信息的共享和联动机制。
11.4.7　重点目标管理单位应定期开展反恐怖风险评估工作，根据评估结果，针对常态防范与非常态防范的不同要求，落实各项反恐怖防范措施。
11.4.8　重点目标管理单位应建立健全反恐怖防范管理档案和台账，包括重点目标的名称、地址或位置、目标等级、防范级别、重点目标管理单位负责人、保卫部门负责人，现有人力防范、实体防范、电子防范、制度防范相关材料，平面布置图、结构图、重要部位分布图等。

12　非常态反恐怖防范

12.1　非常态防范启动

12.1.1　根据恐怖威胁预警，进入非常态反恐怖防范。
12.1.2　根据反恐怖主义工作领导机构、有关职能部门的要求进入非常态防范。
12.1.3　电信互联网重点目标管理单位可根据实际工作需要或现实危害进入非常态反恐怖防范。

12.2　人力防范要求

12.2.1　电信互联网重点目标管理单位应启动反恐应急响应机制，组织开展反恐饰动员，负责人应24h带班组织防范工作，在常态防范基础上加强保卫力量。
12.2.2　应加强对出入人员、车辆及所携带物品的安全检查。
12.2.3　应加强对重要部位的执勤巡逻。

12.3　实体防范要求

12.3.1　应加强电信互联网设施的防护器具、救援器材、应急物资及门、窗、锁、防冲撞设施等设施的有效性检查。
12.3.2　应关闭部分周界出入口，减少周界出入口的开放数量。
12.3.3　周界主要出入口的防冲撞设施应设置为阻截状态。

12.4　电子防范要求

12.4.1　应加强电子防范设施、通信设备的检查和维护，确保反恐怖防范系统正常运行和通信设备的正常使用。
12.4.2　根据需要更新相关电子防范设施以满足不断变化的应急防范需要。

13　应急准备要求

13.1　应急处理总体要求

13.1.1　重点目标管理单位应针对恐怖事件的规律、特点和可能造成的社会危害，分级分类制定并实施应急预案，应对可能遭受的恐怖袭击或危害等紧急情况，并对本单位的应急准备和应急能力进行评估。
13.1.2　应急预案应规定恐怖事件应对处置的组织指挥体系、恐怖事件安全防范、应对处置程序以及事后社会秩序恢复等内容：

a) 应包括目标概况、应急基本原则、组织机构、应急联动、信息报告、应急指挥、应急措施、保障、应急解除等内容；
b) 根据情况应提供基本情况说明、工作人员信息详表、应急联络通讯表、实景照片、地理位置标示图、周边环境图、单位平面图、重要部位分布图、应急疏散通道(路线)图、应急装备(设备)分布图、消防设施分布图、防范设施标示图；
c) 宜提供电路设施网分布图、自来水管网分布图、地下管网分布图、信息系统网络分布图及相应的视频资料或三维建模(配合 3D 地图采集建模)等。

13.1.3 宜建立相应的数据库和应急指挥系统。

13.1.4 宜组建具有组织人员疏散、保护重要部位、控制损失和准确反馈现场情况等能力的应急作战队伍。

13.1.5 电信互联网重点目标管理单位应定期按照应急预案开展演练，按规定修订和完善应急预案。

13.1.6 电信互联网重点目标管理单位应建立高效的反恐防范处置工作机制，应主动强化与各方联动、联巡、联勤机制建设，强化电信互联网安全管理能力。

13.2 反恐应急

13.2.1 电信互联网重点目标管理单位应组建应急处置队伍，制定完善反恐怖应急处置总体预案和专项预案等，细化流程，明确各部门、重要部位、关键岗位及相关人员的任务职责等要求。

13.2.2 在反恐防范工作中，电信互联网重点目标管理单位应做好综合信息收集和报告工作，强化风险管控，及时联动，根据预案有序开展监控和应对工作，实现对反恐和突发事件“网上与网下”、“硬件与软件”、“院内与院外”一体化处置。

13.2.3 电信互联网重点目标管理单位应按照上级指挥机构的应急指令，配合做好反恐应急处置力量、物资、通信信息等保障任务，快速处置恐怖突发事件。具备组织人员疏散、保护重要部位、控制损失和准确反馈现场情况等能力。

13.3 反恐应急演练

13.3.1 电信互联网重点目标管理单位应根据各机楼实际情况，因地制宜，建立应急“一楼一预案”。

13.3.2 电信互联网重点目标管理单位每年应至少组织一次反恐应急综合演练，对重要部位每半年应组织一次反恐应急演练。重点加强重要岗位人员的培训和实操演练，确保重要岗位员工熟练掌握各类应急业务技能，保证工作安全、有序、可控。

13.3.3 电信企业应定期组织反恐应急演练，可在安全演练中合并进行，重点演练基站设施被破坏、通信网络中断等情景下的应急处置流程，包括紧急修复、数据备份与恢复、通信保障等关键环节。

14 监督、检查

14.1 监督职责

14.1.1 反恐怖主义工作领导机构的办事机构

反恐怖主义工作领导机构的办事机构应设置与公安机关、行业主管部门、重点目标管理单位对接的岗位人员，负责全市、区各重点目标的备案、日常指导和监督检查工作。

14.1.2 公安机关

公安机关应掌握重点目标的基本信息和重要动态，指导、监督重点目标管理单位履行防范恐怖袭击的各项职责，应当依照有关规定对重点目标进行警戒、巡逻、检查。

14.1.3 行业主管部门

电信互联网行业主管部门应掌握主管领域内重点目标的基本信息和重要动态，指导、监督重点目标管理单位履行防范恐怖袭击的各项职责。

应由反恐怖主义工作领导机构的办事机构和电信互联网行业主管部门配合，共同指导重点目标。

14.2 检查

14.2.1 自我检查

14.2.1.1 电信互联网重点目标管理单位应定期和不定期地开展自我检查，定期检查每季度应不少于1次，不定期检查根据实际工作需要开展。

14.2.1.2 电信互联网重点目标管理单位每年应对其反恐怖防范系统开展至少1次的自我评价，对反恐怖防范工作中存在的问题实施持续改进，不断完善人防、物防、技防和制度防，提高其反恐怖防范能力。自我评价可结合定期的自我检查一起开展。电信互联网重点目标管理单位应及时向公安机关递交自我评价报告。

14.2.1.3 自我检查及改进按附录B的要求进行。

14.2.1.4 应及时向电信互联网主管部门递交自我检查报告。

14.2.2 督导检查

由公安机关对电信互联网反恐怖防范进行监督及相关检查工作，年度检查报告由公安机关负责向反恐怖主义工作领导机构提交。

14.2.3 检查的实施

反恐怖防范工作检查实施按附录C规定进行。

附录 A
（规范性）
管理制度要求

A.1 范围

本附录规定了各项管理制度的管理内容要求，可视实际工作需要整合设置。

A.2 制度的基本框架

制度的基本框架至少应包括以下内容：

a） 制的管理目的（或适用范围）；
b） 制度的引用文件；
c） 制度的管理职责，如制定、维护、落实责任部门或岗位；
d） 管理内容与实施方法；
e） 制度实施报告和记录；
f） 制度的编号、版本号、实施时效、制定人、审核人和批准实施人。

A.3 管理制度

A.3.1 教育培训和考核制度

重点目标管理单位应制定教育培训制度，持续提升人防技能，至少应包括：

a）保安员：应经专业装备使用技能培训并取得相应专业资格证书，除应熟悉服务单位地理环境、消防通道和各类出入口外，还应熟悉应急处突装备的放置区域，并管理好个人所配备的防护和应急装备，严防被不法分子所用；
b）全员培训：每年至少应组织一次反恐怖防范与应急知识的全员教育培训；
c）责任部门培训：每个季度至少应组织一次重要岗位反恐怖防范与应急知识的部门教育培训；
d）宣传教育：协助各有关部门开展反恐怖主义宣传教育；
e）考核：应包括反恐知识考核和技能考核。

A.3.2 人员背景审查制度

重点目标管理单位应当对重要岗位人员进行安全背景审查，对有不适合情形的人员，应当调整工作岗位，并将有关情况通报公安机关。

重要岗位人员至少应包括：

a）责任领导；
b）责任部门负责人；
c）保卫管理人员；
d）联络员；
e）保安员；
f）技防岗位人员。

人员背景审查的内容至少应包括：

a） 个人资料，身份信息和户口信息；

b） 个人经历，教育、就业履历和出入境记录；

c） 无犯罪记录；

d） 本人及亲属是否有涉及极端主义，恐怖主义活动或关联的有关信息。

A.3.3 人员档案及备案制度

重点目标管理单位应建立人员档案并及时向有关部门备案，人员档案至少应包括以下内容。

a）基本信息；

b）背景审查情况；

c）反恐怖防范继续教育情况；

d）证件（身份证、保安员证书等复印件）；

e）岗位聘用情况；

f）备案信息，至少包括：

1） 备案日期；

2） 备案人相关信息；

3） 备案部门。

A.3.4 门卫与寄递物品管理制度

重点目标管理单位应对出入口人员、车辆进行登记检查；加强寄递物品验视、签收和登记管理。

安全检查中发现违禁品和管制物品，应当予以扣留并立即向公安机关报告；发现涉嫌违法犯罪人员，应当立即向公安机关报告。

A.3.5 巡查制度

重点目标管理单位应确定出入口、周界、重要部位的巡查路径和方式，明确值守、巡查的要求和措施。

A.3.6 安全检查制度

重点目标管理单位应确定出入口、重要部位的安检形式，明确安检设备的使用位置和使用规范。

A.3.7 值班监看和运维制度

重点目标管理单位应做好视频监控系统的值班监看、信息保存使用制度，定期开展电子防范各系统的运行维护检查，保障各系统的正常运行。

A.3.8 训练演练制度

重点目标管理单位应结合工作实际，制定训练演练大纲，有计划地定期组织开展应急技能训练和应急处突演练，应急技能训练每周至少一次，应急演练每季度至少一次，不断提升应对恐袭的应急能力。

训练演练制度应明确：

a） 安保力量的训练演练要求；

b） 训练演练计划的要求；

c） 训练大纲，包括训练的目的、类型及对应的内容、训练效果评价方法；

d） 演练大纲，包括演练的目的、类型及对应的内容、演练效果评价方法。

A.3.9 检查督导制度

重点目标管理单位应定期开展反恐怖防范督导、检查、考核工作，落实反恐怖防范措施。

A.3.10 人防增援配置制度

重点目标管理单位应具备当启动非常态反恐怖防范时增派安保力量的保障能力，包括：

a） 建立后备的安保力量；
b） 与安保企事业单位签订临派安保力量的服务合同；
c） 通过联动配合机制获得安保力量；
d） 其他途径获取的可靠安保力量。

A.3.11 采购管理制度

重点目标管理单位应对采购活动进行控制，制定采购管理制度。

a） 供方应提供其具备合格供方能力的证据，包括：
   1） 供方的产品、程序、过程、设备、人员的概况；
   2） 供方的产品安全认证（必要时）；
   3） 供方的质量管理等体系的认证。
b） 根据供方提供产品的能力，进行评价和选择。
c） 制定选择评价和重新评价合格供方的准则。
d） 保存评价结果及评价记录。

重点目标管理单位应建立并实施验收标准，包括提供合格证明文件、现场验证等方式，以确保采购的产品满足规定的物防、技防要求。

A.3.12 设备设施档案制度

重点目标的设备设施应有台账管理，并建立档案，档案内容至少应包括：

a） 物品名称、型号、编号；
b） 物品管理编号，领用人或保管人；
c） 物品使用说明书，合格证、保修证、检验报告、验收报告及相关发票（原件或复印件）；
d） 物品的使用状态，包括在用、停用和报废；
e） 操作手册（使用、维护和保养）；
f） 维护保养记录。

A.3.13 技防系统管理制度

重点目标应有技防系统的总台账、各系统的设备设施台账、系统操作手册（包括使用、维护和保养），并建立系统管理档案。

技防系统的总台账至少应包括以下内容：

a） 系统名称、型号；
b） 工程提供和建设方名称；
c） 系统责任人；
d） 维护保养周期。

系统管理档案至少包括以下内容：

a） 采购有关资料；
b） 建设工程有关的资料，包括设计、验收报告等；

c） 所有设备设施的使用说明书，合格证、检验报告和验收资料；
d） 操作手册（使用、维护和保养）；
e） 维护保养记录。

A.3.14 工作报告制度

重点目标管理单位应定期向反恐怖主义工作领导机构的办事机构、属地公安机关和相关行业主管部门提交工作报告，每半年至少一次，内容至少应包括：

a） 人防配置及实施情况；
b） 防配置及实施情况；
c） 技防配置及实施情况；
d） 制度防配置及实施情况；
e） 自我检查报告。

存在下列情况时应提交工作报告：

a） 非常态反恐怖防范的响应及实施总结；
b） 特殊活动安全防范总结；
c） 人防、物防、技防、制度防的重大变化；
d） 其他重要情况。

A.3.15 网络安全管理制度

对重点目标的网站、业务管理等信息系统，应依法落实网络安全等级保护制度和数据安全保护制度，严格按照国家标准和规定落实网络定级、网络备案、等级保护测评等法定要求，强化主体责任意识，加强网络安全监测和隐患排查、整改。在发生安全案件时，应及时上报属地公安机关。属于关键信息基础设施的应按GB/T 39204 实施重点保护。

A.3.16 专项经费保障制度

重点目标管理单位应建立反恐怖主义工作专项经费保障制度，做好年度经费预算，确保：

a） 人防配置及奖励制度有效落实；
b） 物防配备、更新防范和处置设备设施；
c） 技防系统正常运维；
d） 各项制度实施经费保障，如教育培训、物防设施设备验收、技防委托验收、人防增援配置等经费。

A.3.17 情报信息管理制度

重点目标管理单位应建立快速高效的情报信息工作机制，主动收集重点目标范围内的情报信息，对收集到的有关线索、人员、活动等情报信息应及时分析整理，及时向责任领导、责任部门汇报。

发现恐怖活动嫌疑或者恐怖活动嫌疑人员的信息应及时向行业主管部门和属地公安机关报送，必要时经责任领导批准后提升内部的反恐怖防范等级。

联络员接到上级部门或属地公安机关情报信息，应立即向责任领导报告并落实相应工作措施。

A.3.18 恐怖威胁风险评估制度

重点目标实行风险评估制度，实时监测安全威胁，编写恐怖威胁风险评估报告。每年至少要开展一次恐怖威胁风险评估，评估内容包括但不限于：

a） 可识别性：重点目标可以被了解和熟悉、关注和重视的程度；

b） 可接近性：重点目标可以被靠近、进入的难易程度；
c） 内在危险性：重点目标是否存在可以被作为攻击手段目标，该目标的容易破坏的程度；
d） 标志性和轰动性：重点目标敏感度、关注度、社会影响的程度；
e） 后果严重性：重点目标受到袭击后会造成的人员伤亡、经济损失、社会影响程度。

A.3.19 联动配合机制

重点目标管理单位应与公安机关、应急管理、街道等有关政府职能部门建立联动机制，实现资源共享，信息互通。

A.3.20 应急管理制度

A.3.20.1 反恐怖袭击专项应急预案

重要部位的责任主体应制定反恐怖袭击专项应急预案，至少应包括：
a） 恐怖事件按照其性质、严重程度、可控性和影响范围等因素进行分类或分级；
b） 恐怖事件发生时的应急报告，包括报告程序、报告内容；
c） 报告内容应包括恐怖袭击的时间、地点、目标、人员伤亡情况、已采取的措施等内容；
d） 恐怖事件发生时的应急准备，包括组织架构、工作职责；
e） 设置反恐怖袭击应急指挥小组和反恐怖应急指挥办公室的组织架构；
f） 应急指挥小组、应急指挥办公室和责任主体各部门应对恐怖袭击的工作职责；
g） 恐怖事件发生时的应急处置，包括预案启动、应急上报、应急行动、应急要点；
h） 应急处置后的应急终止；
i） 事后处置，包括保险理赔、工作简报、新闻稿、总结会、奖惩等。

A.3.20.2 反恐通信保障专项预案

重要部位的责任主体应制定反恐通信保障专项预案，至少应包括：
a） 恐怖事件按照移动通信网络直接损失程度、本地网通信受影响程度、本地网网间接通率等因素进行分类或分级；
b） 不同级别的恐怖事件对应不同程度的网络保障响应工作；
c） 通信保障机制，包括常设保障机制、流程制度保障、资源保障等；
d） 反恐应急通信保障内容应包括网络保障、应急发电、应急传输、应急会议电话、视频监控、数据业务等内容；
e） 设置反恐通信保障应急指挥小组和反恐通信保障应急指挥办公室的组织架构；
f） 应急方案启动索引，包含通信故障场景、应急保障方案、启动条件、责任部门、责任人、操作实施人、联系方式等；
g） 反恐通信保障应急指挥小组、反恐通信保障应急指挥办公室和责任主体各部门应对恐怖袭击的工作职责；
h） 通信保障应急处置后的应急终止；
i） 事后处置，包括保险理赔、工作简报、新闻稿、总结会、奖惩等。

A.3.21 应急预案管理制度

A.3.21.1 通信网络和设施安全管理制度

重要部位的责任主体应制定通信网络和设施安全管理制度，应包括：
a） 网络安全岗位人员的工作职责和工作保密要求；

b） 操作维护规范，包括网络系统操作维护要求、网络系统防病毒和防攻击入侵要求、系统接入的安全规范要求、服务的安全规范要求、数据的安全规范要求、网络设备的安全规范要求、终端的安全规范要求等；
c） 网管网的建设、维护及接入管理，包括物理环境安全管理要求、设备安全管理要求、系统安全管理要求等；
d） 通信网络安全事件处理流程及应急预案。

A.3.21.2 信息安全保护管理制度

重要部位的责任主体应制定信息安全保护管理制度，应包括：
a） 信息安全岗位人员的工作职责和工作保密要求；
b） 信息泄漏安全防范技术手段，包括帐号口令、文件加密、访问控制、数据传输保护机制、违规紧急封停等；
c） 信息安全保护管理要求，包括安全通信网络要求、安全区域边界要求、安全计算环境要求、安全管理中心要求、安全管理制度要求、安全管理机构要求、安全管理人员要求、安全建设管理要求、安全运维管理要求等；
d） 信息安全维护作业计划；
e） 信息安全事件应急预案。

A.3.22 保密制度

重点目标管理单位应制定保密制度，明确保密范围、密级确定、保密要求、保密管理等内容。

附录 B
（资料性）
反恐怖防范系统自我检查及改进

B.1 自我检查

B.1.1 自我检查的目的

确定其建立和实施的人防、物防、技防及制度防反恐怖防范系统与反恐怖防范目标的适宜性、充分性和有效性。

B.1.2 自我检查的时间

重点目标管理单位建立了反恐怖防范系统所需的人防、物防、技防及制度防并有效实施三个月后方可开展首次自我检查。

后续检查时间间隔不宜大于半年，每年应至少一次。

B.1.3 自我检查的组织

成立包括责任领导、责任部门负责人在内的自我检查小组，并确定一名组长，成员包括各岗位的负责人数名，必要时可外聘反恐专家协助。

B.1.4 检查方法

自我检查一般采用整体检查的方法，由重点目标管理单位所在单位组成检查小组，对建立、实施和开展反恐怖防范全过程进行检查。具体方法主要通过检查人员的现场核查、观察、提问、对方陈述、检查、比对、验证等获取客观证据的方式进行。根据检查结果，对不符合标准要求的项目制定纠正和预防措施，并跟踪实施和改进。

B.1.5 检查程序

检查活动应按以下程序进行:

a) 成立检查小组；
b) 制定检查计划；
c) 检查准备；
d) 检查实施；
e) 编写自我检查报告和不合格报告；
f) 检查结果处置；
g) 考核奖惩。

B.1.6 自我检查的内容

覆盖人防、物防、技防和制度防等所有要素。

B.1.7 自我检查结果处置

自我检查后，应编写自我检查报告。对检查结果，特别是对发现的问题、不合格项产生的原因要进行分析研究，制定纠正和预防措施。

B.2 改进

B.2.1 改进的目的

持续改进是重点目标管理单位一项长期工作，是不断完善管理、实现最终反恐怖防范目标的有效办法，持续改进应按照PDCA(计划一实施一检查一改进)管理模式进行。

B.2.2 改进的实施及依据

B.2.2.1 收集有关不符合反恐怖防范要求的信息，明确信息来源，组织有关人员对信息进行分析，确定现有的和潜在的问题根源。

B.2.2.2 根据信息分析的结果，督导责任部门会同有关人员共同制定纠正和预防措施，对制度、程序、人员或管理部门进行调整，并报责任领导批准，避免不符合情况再次发生。

B.2.2.3 实施改进的依据包括：

a) 公众反馈安全防范漏洞的意见；
b) 物防中所涉及安防产品日常检查、技防工程的验收、周期检验的报告；
c) 各项制度落实的记录、报表中反映的数据；
d) 有关部门检查发现的问题；
e) 安保人员等有关人员的建议。

B.2.3 持续改进

重点目标管理单位通过实施纠正措施,对标准、制度文件或岗位人员进行调整,直至达到预期效果。

B.2.4 改进后检查

重点目标管理单位责任领导组织对改进的有效性进行跟踪检查。

附录 C
（资料性）
反恐怖防范工作检查实施

C.1 检查方式

反恐怖防范工作检查包括自我检查、部门检查和督导检查。

C.2 检查基本信息

检查基本信息至少应包括：
——管理单位的名称、地址；
——检查执行机构名称，检查人员签名（不少于2人）；
——检查的时间。

C.3 检查的实施机构

自我检查由重点目标管理单位自行组织实施。
部门检查由公安机关、行业主管部门组织实施。
督导检查由反恐怖主义工作领导机构的办事机构组织实施。

C.4 检查内容

检查内容见表C.1。

C.5 检查结果及处置

C.5.1 自我检查的结果及处置

自我检查中应做好书面记录，并应根据自我检查的结果进行整改，由责任领导检查整改情况，确保整改措施落实。

C.5.2 部门检查和督导检查的结果及处置

公安机关、行业主管部门的检查应做好书面记录，将检查情况现场通报被检查单位，及时督促整改。发现有重大涉恐隐患的，应及时向反恐怖主义工作领导机构的办事机构汇报。

反恐怖主义工作领导机构的办事机构的检查应做好书面记录，将检查情况现场通报被检查单位，视检查情况出具限期整改通知书或通报相关部门进行行政处罚。

C.3 检查表格

检查表格应包括检查的项目、内容概要、检查情况记录和结论。格式参见表C.1。

表C.1　检查表格

序号	标准条款		内容概要	检查记录	项目结论
1	5 重点目标和重要部位		重点目标的重要部位分布图/列表是否清晰、完整，是否及时报备		
2	8 常态人力防范	8.1	是否按要求设立与防范任务相适应的反恐怖防范工作机构及责任部门		
3			是否配备专（兼）职工作人员，负责反恐怖防范的具体工作		
4			主要负责人、联络员的配置和变更是否及时向行业主管部门、属地公安机关和反恐怖主义工作领导机构的办事机构备案		
5			是否明确反恐怖防范重要岗位，如：网络管理监控人员、网络安全管理人员、安防监控人员、技防系统管理人员、电力维护人员和消防值守人员等		
6		8.2	是否按照要求配置安防监控岗、门岗、巡逻岗、网络安全管理岗等岗位		
7			是否定期开展反恐怖教育培训和联动性综合演练		
8		8.3	是否按照要求配备足够的安保力量		
9			是否对重要岗位人员开展背景审查、考核、建立人员档案并备案，并签订保密协议		
10			反恐怖防范专（兼）职工作人员是否熟悉本重点目标反恐怖防范工作情况及相关规章制度、应急预案等		
11			保安员承担保安职责，是否满足《保安服务管理条例》和GA/T 594的相关要求并持证上岗		
12			反恐怖防范专（兼）职工作人员是否熟悉重点目标内部和周边环境、消防通道和各类疏散途径		
13			应对涉恐突发事件，年内是否存在不配合反恐怖主义工作领导机构、公安机关、有关行业指导部门开展工作的情况		
14			是否设置专职网络安全管理员		
15			是否应定期组织巡检人员进行反恐怖防范培训		
16	9 常态实体防范	9.1	周界实体屏障是否符合要求		
17			出入口宜设置实体屏障是否符合要求		
18			是否按照要求设置警示标志		
19			洞口、管沟、管廊、吊顶、风管、桥架、管道等空间尺寸能够容纳人进入时，是否有实体屏障封闭或阻挡		
20			穿越周界的河道、涵洞、管廊等孔洞，是否有相应的实体防护措施		
21			机房（楼）与外界相通的主要出入口或所在院落与外界相通的主要出入口是否设置机动车阻挡装置		
22			机房（楼）或所在院落与外界相通且未做人车分流的主要出入口、受机动车冲击后容易受到重大伤害的部位是否设置防暴阻车路障或隔离设施		
23			机房、网络管理监控室、安防监控中心、储油库、配电房、空调系统风柜房等重要部位出入口是否设置防盗安全门、金属防护门		
24			机房（楼）周界是否设置围墙或栅栏等实体防护屏障		
25			直接与外界相通的一、二楼无人值守的机房窗户、网络管理监控室、安防监控中心是否安装栅栏		
26			机楼出入口是否设置行李箱包寄存设施		
27			机房、蓄电池室、配电房、储油库等重要设备场所、应急疏散通道是否设置警示标志		
28			安保力量、安防监控中心、门卫室、保安装备存放处是否配备对讲机、强光手电、防护棍棒、防暴盾牌、钢叉、防暴头盔、防割（防刺）手套、防刺服		
29			主要出入口、门卫室、值班室、保安装备存放处是否配备防爆毯（含防爆围栏）		
30			人员密集场所安检区是否配备防爆球		

序号	标准条款		内容概要	检查记录	项目结论
31			人员密集场所、应急疏散通道是否设置照明灯光		
32			交换机房、配电房等通信、电力设备房是否设置气体灭火系统		
33			蓄电池室、配电房、储油库等重要设备场所、门卫室、安防监控中心是否配备灭火器		
34			机房、蓄电池室、配电房等重要设备场所、安防监控中心是否设置防烟、排烟系统		
35			机房、蓄电池室、配电房等重要设备场所、安防监控中心是否设置防火分隔设施		
36			出入口门卫室和设在建筑物二层以下的监控中心是否配置防盗窗或护栏		
37		9.2	实体防护配置的设备设施是否符合相关要求		
38	10 常态电子防范	10.1	摄像机是否覆盖全部重要部位		
39			机楼出入口、安防监控中心出入口等主要出入口是否安装人脸识别装置		
40			安防监控中心是否设置终端图形显示装置		
41			周界、与外界相通的重要部位或机房、电力室、储油库等无固定人员值守的重要部位是否配备入侵探测（报警）器		
42			门卫室、机房、储油库、安防监控中心、消防控制室是否配备紧急报警装置		
43			安防监控中心是否配备控制指示设备		
44			安防监控中心、门卫室是否配备报警控制器		
45			机楼、配电房、空调系统风柜房、机房、电力室、高低压变配电室、变压器室、蓄电池室、发电房、冷冻机房、通风机房、水泵房、电缆充气控制室、电（光）缆进线室等设备房、储油库、安防监控中心是否配备出入口控制系统		
46			机楼周界、出入口、门厅、楼层出入口、主要通道、电梯轿厢内、核心机房、储油库、电力室、高低压变配电室、变压器室、蓄电池室、发电房、冷冻机房、通风机房、水泵房、电缆充气控制室、电（光）缆进线室等备机房、安防监控中心、消防控制室是否配备电子巡查系统（巡更系统）		
47			公共广播系统是否覆盖全部重要部位		
48			安防监控中心是否配备安防监控系统		
49			火灾自动报警系统是否覆盖全部重要部位		
50			卫星授时信号接收装置是否配备授时安全防护系统		
51			重点目标是否配备无人机防御系统		
52		10.2	备用电源是否符合要求		
53			监控中心是否配备视频监控系统、入侵和紧急报警系统、出入口控制系统、电子巡查系统等各子系统设备终端		
54			监控中心是否配置能与报警同步的终端图形显示装置，并能准确地识别报警区域，实时显示发生警情的区域、 日期、时间及报警类型等信息		
55			主要出入口监控系统是否接入管辖公安机关指挥部门、辖区派出所		
56			安防监控中心疏散门是否采用外开方式，能自动关闭，并在任何情况下均能从室内开启		
57			视频图像采集装置是否满足 GA/T 1127-2013 中规定的 C 类高清晰度及以上要求		
58			视频录像保存时间是否不少于 90 日		
59			频监控系统的备用电源是否满足至少 4 h 正常工作的需要		
60			室内报警声压是否不低于 80dB，室外报警声压是否不低于 100dB		
61			视频监控范围内的报警系统发生报警时，是否与该视频系统联动，报警响应时间是否不大于 2 秒		
62			入侵和紧急报警系统布防、撤防、故障和报警信息存储时间是否不少于 180 日		
63			入侵报警系统备用电源是否满足至少 24h 正常工作的需要		

序号	标准条款		内容概要	检查记录	项目结论
64			出入口控制系统备用电源是否满足至少 48h 正常工作的需要		
65			出入口控制系统信息存储时间是否不少于 180 日		
66			电子巡查系统是否具备巡查路线偏离报警、规定时间无位移报警等功能		
67			电子巡查系统的巡查路线、巡查时间是否能根据安全管理需要进行设定和修改，并覆盖重要部位		
68			公共广播系统是否符合 GB/T 50526 相应规定		
69			无线通信对讲指挥调度系统覆盖的时间地点概率是否不小于 90%，并覆盖重要部位		
70			无线通信对讲指挥调度系统是否提供在岗的安保人员、网络管理监控人员、安防监控人员、电子防范系统管理人员、巡查岗位人员、机动岗位人员、电力维护人员和消防岗位人员等用户之间的通信手段		
71			授时安全防护系统是否满足安全防范要求		
72			无人机防御系统是否能自动 24 小时持续工作，无需人员值守		
73	11 制度防范	11.1	是否按要求按照要求配置了相关管理制度，包括教育培训及考核制度、人员背景审查制度、人员档案及备案制度、门卫与寄递物品管理制度、巡查制度、安全检查制度、值班监看和运维制度、训练演练制度、检查督导制度、人防增援配置制度、采购管理制度、设备设施档案制度、技防系统管理制度、工作报告制度、网络安全管理制度、专项经费保障制度、情报信息管理制度、恐怖威胁风险评估制度、联动配合机制、应急管理制度、应急预案管理制度、保密制度		
74		11.2	是否制定重点目标管理单位责任领导、责任部门的正（副）职、联络员等岗位标准，应包括反恐怖防范工作职责和权限		
75			在安保、网络管理监控、网络安全管理、安防监控、技防系统管理、巡查岗位、机动岗位、电力、消防等工作岗位的标准中，是否明确人员的配置标准、资质条件、操作规范和权限等，细化每个岗位工作细节及与其他岗位人员协调、配合、交接的操作流程		
76			是否制定考核条件和奖惩办法，明确检查、考核部门、时间要求，明确考核程序和考核办法，是否有考核记录		
77		11.3	操作规程配置是否符合要求		
78		11.4	是否制定反恐怖防范管理组织制度，明确责任领导的管理职责和责任部门的工作职责		
79			是否建立健全包括值守、巡逻、培训、检查、考核、反恐怖防范系统运行与维护等制度		
80			是否建立反恐怖防范系统建设、运行与维护的保障体系和长效机制		
81			是否建立反恐怖工作专项经费保障制度，将反恐怖防范涉及费用纳入企业预算、成本		
82			是否与属地公安机关等有关部门和单位建立联防、联动、联治工作机制		
83			是否建立反恐怖与安全生产等有关信息的共享和联动机制		
84			是否定期开展反恐怖风险评估工作		
85			是否建立健全反恐怖防范管理档案和台账		
86	其它防范管理	12	是否按要求制定了非常态反恐怖防范应对措施		
87		13	是否制定了应急预案		
88			应急预案的内容是否全面		
89			是否有组建应急处置队伍并建立有效增援保障措施		
90			是否按规定开展应急预案的演练		
91		14	是否定期开展自我评价并向公安机关递交自我评价报告		
92			是否对反恐怖防范工作中存在的问题实施持续改进		
93		附录 A.3	专项经费是否符合实际防范工作需要		
94			情报信息管理是否符合要求		
95			恐怖威胁预警是否得到快速有效响应		
96			是否开展恐怖威胁风险评估工作		

序号	标准条款		内容概要	检查记录	项目结论
97			是否建立有效联动配合机制		