

DB4401

广 州 市 地 方 标 准

DB4401/T 10.1—2024
代替 DB4401/T 10.1—2018

反恐怖防范管理 第1部分：通则

Anti-terrorism precaution management—Part 1: General

2024-04-30 发布

2024-05-30 实施

广州市市场监督管理局 发布

目 次

前言..... III

引言..... V

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 2

4 反恐怖防范原则..... 4

5 重点目标和重要部位..... 4

 5.1 重点目标..... 4

 5.2 重要部位..... 5

6 防范分类和防范等级..... 5

7 总体要求..... 5

8 常态人力防范..... 6

 8.1 人力防范组织..... 6

 8.2 人力防范配置..... 6

 8.3 人力防范管理..... 6

9 常态实体防范..... 7

 9.1 实体防范配置..... 7

 9.2 实体防护设备设施要求..... 8

10 常态电子防范..... 8

 10.1 电子防范配置..... 8

 10.2 电子防范设备设施要求..... 10

11 制度防范..... 11

 11.1 管理制度配置..... 11

 11.2 岗位标准配置..... 11

 11.3 操作规程配置..... 12

 11.4 制度防要求..... 12

12 非常态防范要求..... 12

 12.1 非常态防范启动..... 12

 12.2 人力防范要求..... 12

 12.3 实体防范要求..... 12

 12.4 电子防范要求..... 13

13 应急准备要求..... 13

14 监督、检查..... 13

14.1 监督职责.....13

14.2 检查.....14

附录 A（资料性） 部分重点目标的重要部位.....15

附录 B（规范性） 管理制度要求.....23

附录 C（规范性） 反恐怖防范系统自我检查及改进.....28

附录 D（规范性） 反恐怖防范工作检查实施.....30

参考文献.....33

前 言

本文件按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1部分。本文件代替DB4401/T 10.1—2018《反恐怖防范管理 第1部分：通则》。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。

本文件代替DB4401/T 10.1—2018《反恐怖防范管理 第1部分：通则》，与DB4401/T 10.1—2018相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 增加了术语和定义：反恐怖主义工作领导机构的办事机构、反恐怖防范重点目标管理单位、电子防范、管理制度、岗位标准、操作规程、关键信息基础设施；删除了术语和定义：反恐怖防

范重点目标责任主体、反恐怖主义工作领导小组及其办事机构、反恐怖防范一般目标、技术防范、管理标准、工作标准、技术标准、恐怖威胁预警和恐怖威胁预警响应；

- b) 调整了重点目标等级和分类表述，明确重点目标等级分三级，包括38个行业分类；
- c) 调整了重要部位划分的表述；
- d) 明确了常态反恐怖防范等级要求；
- e) 增加了总体要求；
- f) 增加网络安全管理员要求；
- g) 重新梳理了人防、物防、技防（电子防范）和制度防相关要求，人防、物防、技防配置要求分为三级，将重点目标日常经营业务相关要求删除；
- h) 删除了四级非常态反恐怖防范要求，重新梳理了非常态下人防、物防、技防相关要求；
- i) 优化了附录的检查表；
- j) 增加了附录A（资料性）部分重点目标的重要部位。

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提出并归口。

本文件起草单位：广州市公安局反恐怖支队、广州市标准化协会、广州计量检测技术研究院、广州市公安局科技通信处、广州市市公安局内部安全保卫支队、广州市公安局网络警察支队、广州市公安局治安管理支队、广州市公安局越秀区分局、广州市公安局天河区分局、广州市公共交通集团有限公司、广东粤海天河城商业管理有限公司、广州越秀怡城商业运营管理有限公司、广州市越秀公园。

本文件主要起草人：吴朝阳、吴志强、唐小军、廖章平、张晓军、殷秀梅、王同淇、陈淑宜、陈巧红、张卿勋、牛方勤、喻峰、杨伟洲、王念省、黄品乾、谢勇、刘军、高小章、倪青山、赵海军。

本文件于2018年首次发布，本次为第一次修订。

引 言

广州市地方标准DB4401/T 10.1—2018《反恐怖防范管理 第1部分：通则》（简称《通则》）自发布以来，经过多年实施，取得良好的效果。以《通则》为重要抓手开展反恐怖防范工作，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，对重点目标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，完善城市反恐怖防范管理标准体系，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《通则》修订工作。

本文件为DB4401/T 10《反恐怖防范管理》的第1部分。本文件明确了重点目标普遍适用的反恐怖防范要求。DB4401/T 10的其余部分在通则的基础上，根据行业的特点，增加行业反恐特殊要求、细化通则的有关内容，使其更有针对性、有效性和适用性。

反恐怖防范管理 第1部分：通则

1 范围

本文件规定了反恐怖防范管理的术语和定义、反恐怖防范原则、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、制度防范、非常态防范要求、应急准备要求和监督、检查。

本文件适用于广州市反恐怖防范重点目标的安全防范、应对准备和管理工作的，其他目标可参照执行，特定反恐怖防范重点目标的特殊要求按相应行业标准或具体分则执行。

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 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 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 37078—2018 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/T 39204 信息安全技术 关键信息基础设施安全保护要求
- GB 50348 安全防范工程技术标准
- 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/T 50526 公共广播系统工程技术标准

GA 68 警用防刺服
GA 69 防爆毯
GA 294 防暴头盔
GA/T 367 视频安防监控系统技术要求
GA 422 警用防暴盾牌
GA 576 防尾随联动互锁安全门通用技术条件
GA/T 594 保安服务操作规程与质量控制
GA 614 防割手套
GA/T 644 电子巡查系统技术要求
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要求
GA/T 1126 近红外人脸识别设备技术要求
GA/T 1127—2013 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 约束叉
DB4401/T 43 反恐怖防范管理 防冲撞设施

3 术语和定义

下列术语和定义适用于本文件。

3.1

反恐怖防范 anti-terrorism precaution

以维护公共安全为目的，为避免恐怖袭击（如爆炸、劫持、撞击、纵火、投毒、施放核与放射性物品、生物化学攻击、网络攻击等）或伤害，运用科技手段、防护硬件、软件，实施相关管理制度和措施等，以探测、延迟和应对恐怖威胁的行为。

3.2

反恐怖防范系统 anti-terrorism precaution system

针对常态和非常态形势下反恐怖防范需求，综合运用人力防范、实体防范、电子防范和制度防范手段而构成的反恐怖防范体系。

3.3

常态反恐怖防范 normal anti-terrorism precaution

在日常的安全管理工作中，采用常规性措施的反恐怖防范，简称常态防范。

3.4

非常态反恐怖防范 non-normal anti-terrorism precaution

在特殊时期（如重大活动期间、重要时段）或应对恐怖袭击时，采取特别措施的反恐怖防范，简称非常态防范。

3.5

反恐怖主义工作领导机构的办事机构 anti-terrorism work leading institution agency

市、区级反恐怖工作领导小组办公室。

注：除特殊声明，本文件所指的反恐怖主义工作领导机构的办事机构指广州市及各区反恐怖工作领导小组办公室。

3.6

反恐怖防范重点目标 the key target of anti-terrorism precaution

由公安机关会同有关部门确定，并经本级反恐怖主义工作领导机构备案的，存在遭受恐怖袭击的可能性较大以及遭受恐怖袭击可能造成重大人身伤亡、财产损失或者社会影响的单位、场所、活动和设施等，也称防范恐怖袭击的重点目标或反恐重点目标，简称为重点目标。

3.7

反恐怖防范重点目标重要部位 the major sections of key target for anti-terrorism

反恐怖防范重点目标的各个组成部分中对国家安全、公共安全和人民生命财产安全等有显著影响的部位，简称为重要部位。

3.8

反恐怖防范重点目标重要岗位人员 the important post staff of anti-terrorism key target major sections

对重点目标的安全负有直接责任和管理责任的人员，简称为重要岗位人员。

3.9

反恐怖防范重点目标管理单位 the responsibility subject of anti-terrorism key target

反恐怖防范重点目标的主体责任单位，包括机关、企事业等单位，简称为重点目标管理单位。

3.10

人力防范 personnel protection

具有相应素质的人员有组织的防范、处置等安全管理行为，简称人防。

[来源：GB 50348—2018，2.0.2]

3.11

实体防范 physical protection

利用建（构）筑物、屏障、器具、设备或其组合，延迟或阻止风险事件发生的实体防护手段，又称物防。

[来源：GB 50348—2018，2.0.3]

3.12

电子防范 eletronic protection

利用传感、通信、计算机、信息处理及其控制、生物特征识别等技术，提高探测、延迟、反应能力的防护手段，又称技防。

[来源：GB 50348—2018，2.0.4]

3.13

制度防范 system protection

为确保人防、物防、技防的有效实施并达到预期目的而制定的各项规章制度，如管理制度、工作机制和操作规程等，简称为制度防。

3.14

管理制度 management system

对反恐怖防范工作中需要协调统一的管理事项所制定的文件。

注：管理事项主要指在反恐怖防范工作中，所涉及人防管理、物防管理、技防管理相关联的事项，如人防中安保人员管理、物防中安防设备设施管理、技防中视频监控信息管理等。

3.15

岗位标准 duty standard

对反恐怖防范工作中需要协调统一的工作事项所制定的文件。

注：工作事项主要指在执行相应管理制度和操作规程时与工作岗位的职责、岗位人员基本技能、工作内容、要求与方法、检查与考核等有关的重复性事物和概念。

3.16

操作规程 operating procedures

对反恐防范系统中涉及的设备设施的操作要求。

注：反恐防范系统涉及的设备设施指视频监控、出入口控制、防冲撞设施、防入侵系统等物防、技防设备。

3.17

安保力量 security forces

实施反恐防范系统的操作、管理、维护和反恐事件响应的专（兼）职人员和队伍。

3.18

保安员 security guard

专职承担门卫、巡逻、守护、安全检查、秩序维护、安全技术防范和安全风险评估等职能，并经专业培训取得资格证的安全保卫人员。

3.19

危险物品 dangerous goods

可能危及人身安全和财产安全的物品，如民用爆炸物品、易燃性物品、危险化学品、核与放射性物品、毒害性物品、腐蚀性物品、传染病病原体等。

3.20

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

4 反恐防范原则

- 4.1 反恐防范工作应遵循“属地负责，逐级监管”“谁主管，谁负责”“谁经营，谁负责”的原则。
- 4.2 反恐防范工作应在反恐主义工作领导小组统一领导和指挥下开展，公安机关、有关行业主管部门履行安全管理、指导、监督和检查责任。
- 4.3 重点目标管理单位应按照反恐主义法等法律法规的相关要求履行职责，建立并实施反恐防范系统。

5 重点目标和重要部位

5.1 重点目标

5.1.1 重点目标确定和等级

重点目标由公安机关会同有关部门确定，其等级根据遭受恐怖袭击的风险性和遭受恐怖袭击后的危害性由低到高可分为三级、二级、一级。

5.1.2 重点目标分类

重点目标的分类按目标的规模、性质及其遭受恐怖袭击后可能造成的人员伤亡、财产损失和社会影响等要素根据国家有关规定划分为38类。包括：

- a) 政治敏感：党政机关、外事外交机构（驻地）、国防军工单位；
- b) 人员密集：城市中心广场、学校幼儿园、旅游景区（园林公园）、旅游饭店、文体场馆、卫生健康、商业中心、会展场所、宗教活动场所；
- c) 基础设施：民用航空运输机场及部分民航设施、铁路、城市公共交通、汽车客运站、港口码头、

口岸、通信设施、传媒设施、发电供电、城市供水、城镇燃气、公路桥梁隧道、水利设施、粮食和物资储备仓库、货币发行及数据处理中心；

- d) 涉危涉爆：石油石化、枪支弹药库及生产厂、民用爆炸物品库及生产厂、烟花爆竹库及生产厂、危险化学品库及生产厂、核技术利用单位、危险化学品运输企业；
- e) 其他：大型活动、标志性建筑物、监狱公安监管场所、重点实验室等。

5.2 重要部位

5.2.1 确定原则

重点目标管理单位应根据相关标准结合自身实际情况按照应列尽列的原则，确认重点目标的重要部位，报行业主管部门、属地公安机关和反恐怖主义工作领导小组的办事机构备案，并接受监督、检查、指导。

5.2.2 重要部位划分

重要部位划分如下，部分重点目标的重要部位见附录A。

- a) 生产运营核心要害部位（重点目标主要职能或业务所对应的部位），包括：
 - 1) 人员密集区域：在一定时间段内聚集人数较多、密度较大的部位；
 - 2) 涉危险物品区域：生产、存储、使用、经营、运输危险物品的部位；
 - 3) 基础设施部位：关系国计民生的重要基础设施，如燃气、电力等能源设施、给排水设施、交通运输设施、邮政电信设施、关键信息基础设施、防灾设施等；
 - 4) 政治敏感、涉密部位：如机密档案室、信息中心、传媒设施等。
- b) 系统的关键部位：对生产、运营核心要害部位的安全有直接影响的部位，如重点目标的出入口、周界、监控中心、通往重要部位的道路和电梯出入口，供电、供水、供气、供油、通风、空调、网络通信等部位。
- c) 其他经风险评估应重点防范的部位。

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。

6.2 常态反恐怖防范等级由低到高分别为三级防范、二级防范、一级防范。

6.3 重点目标常态防范的等级应不低于重点目标的等级，非常态防范应在常态防范要求基础上加强。

7 总体要求

7.1 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 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 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信息泄露、篡改、丢失等情况时立即采取补救措施。

7.4 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 特定类别的重点目标相关条款有特殊规定的，从其规定。

8 常态人力防范

8.1 人力防范组织

- 8.1.1 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 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，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。

8.2 人力防范配置

常态防范人力配置及要求应符合表1要求，可根据重点目标的行业工作需求进行调整。

表 1 常态人力防范配置及要求表

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/兼职	专职
2	岗位要求	监控中心	24 小时值守	24 小时值守，每班不少于 2 人	24 小时值守，每班不少于 2 人
3		门卫室	24 小时值守	24 小时值守	24 小时值守
4		周界主要出入口	对外来人员、车辆登记核查	对外来人员、车辆、物资登记核查	对外来人员、车辆、物资登记核查
5		其他重要部位	配备与巡逻计划相适应的安保力量，巡逻间隔应不大于 16 小时	配备与巡逻计划相适应的安保力量，巡逻间隔应不大于 8 小时	配备与巡逻计划相适应的安保力量，巡逻间隔应不大于 4 小时
6	反恐怖教育培训		每年至少组织一次	每半年至少组织一次	每半年至少组织一次
7	联动性综合演练		每年至少组织一次	每半年至少组织一次	每半年至少组织一次

8.3 人力防范管理

- 8.3.1 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 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需要，并应符合以下要求：
- a) 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；
 - b) 保安员应按《保安服务管理条例》和 GA/T 594 的相关要求，承担保安职责；
 - c) 安保力量应熟悉重点目标内部和周边环境、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) 安保力量应熟悉重点目标反恐怖防范应急预案，包括处置流程、应对措施等；
 - f) 应对涉恐突发事件，配合反恐怖主义工作领导机构、公安机关、有关行业主管部门开展工作；
 - g) 其他需承担的反恐怖防范工作。

8.3.4 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的核心机制，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。

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 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 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 重点目标的实体防范应符合表2要求，可根据重点目标的行业工作需求进行调整。

表 2 实体防范配置表

序号	配置项目		三级防范	二级防范	一级防范
1	实体 防护 设施	机动车阻挡装置	车辆出入口（无实体防护屏障）	车辆出入口（无实体防护屏障）	车辆出入口（无实体防护屏障）
2		防暴阻车路障或隔离设施	主要出入口、受机动车冲击后容易受到重大伤害的重要部位配置隔离设施或防护装置	主要出入口、受机动车冲击后容易受到重大伤害的重要部位配置防暴阻车路障或隔离设施	主要出入口、受机动车冲击后容易受到重大伤害的重要部位配置防暴阻车路障
3		防盗安全门、金属防护门	生产运营核心要害部位出入口、监控中心出入口	生产运营核心要害部位出入口、监控中心出入口、网络通信等系统关键部位出入口	生产运营核心要害部位出入口；监控中心出入口；供电、供水、供气、供油、通风、空调、网络通信等系统关键部位出入口
4		围墙或栅栏等实体防护屏障	封闭式独立院落的周界，外沿高度（含防攀爬设施）大于 2.5 米	封闭式独立院落的周界、临道路和水域的周界，外沿高度（含防攀爬设施）大于 2.5 米	封闭式独立院落的周界、临道路和水域的周界，外沿高度（含防攀爬设施）大于 2.5 米
5		警示标志	生产运营核心要害部位、应急疏散通道	生产运营核心要害部位、应急疏散通道	生产运营核心要害部位、应急疏散通道
6	个人 应急 防护 装备	对讲机、强光手电、防护棍棒	安保力量、保安装备存放处	安保力量、保安装备存放处	安保力量、保安装备存放处
7		防暴盾牌、钢叉	安保力量、保安装备存放处	安保力量、保安装备存放处	安保力量、保安装备存放处
8		防暴头盔、防割（防刺）手套、防刺服	安保力量、保安装备存放处	安保力量、保安装备存放处	安保力量、保安装备存放处

表 2 实体防范配置表（续）

序号	配置项目		三级防范	二级防范	一级防范
9	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	主要出入口、门卫室、值班室、保安装备存放处	主要出入口、门卫室、值班室、保安装备存放处
10		防爆球	/	人员密集场所安检区	党政机关主要出入口、人员密集场所安检区
11		照明灯光	应急疏散通道	人员密集区域、应急疏散通道	人员密集区域、应急疏散通道

- 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。
- 9.1.8 涉危险物品的重点目标应配置相应的防护装备，如防护口罩和消洗喷剂等。

9.2 实体防护设备设施要求

- 9.2.1 车辆出入口的电动栏杆应符合GA/T 1132的要求。
- 9.2.2 防机动车冲撞或隔离设施应符合DB4401/T 43的要求。
- 9.2.3 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。
- 9.2.4 警示标志应符合 GB/T 2893.5 的要求。
- 9.2.5 强光手电应符合 GA 883 的要求；防暴盾牌应符合 GA 422 的要求；防暴钢叉应符合 GA/T 1145 的要求；防暴头盔应符合 GA 294 的要求；防割（防刺）手套应符合 GA 614 的要求；防刺服应符合 GA 68 的要求。
- 9.2.6 防爆毯应符合 GA 69 的要求；防爆球应符合 GA 872 的要求。
- 9.2.7 应急照明应符合 GB 17945 的要求。
- 9.2.8 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。

10 常态电子防范

10.1 电子防范配置

- 10.1.1 重点目标的电子防范配置应符合表3要求，可根据重点目标的行业工作需求进行调整。

表 3 电子防范配置表

序号	项目		三级防范	二级防范	一级防范
1	安防监控中心		应设	应设	应设
2	视频图像采集装置（视频监控设备）		周界、出入口、安防监控中心；人员密集区域、涉危险物品区域等生产运营核心要害部位	周界、出入口、安防监控中心；人员密集区域、涉危险物品区域等生产运营核心要害部位；供电、供水、供气、供油、通风、空调和网络通信等系统关键部位	周界、出入口、安防监控中心；人员密集区域、涉危险物品区域等生产运营核心要害部位；供电、供水、供气、供油、通风、空调和网络通信等部位以及通往重要部位的电梯、通道和出入口等系统关键部位
3	入侵报警系统	入侵探测（报警）器	封闭式独立院落的周界	封闭式独立院落的周界、危险物品存放处、涉密部位等生产运营核心要害部位	封闭式独立院落的周界；危险物品存放处、涉密部位等生产运营核心要害部位；网络通信等系统的关键部位

表3 电子防范配置表（续）

序号	项目		三级防范	二级防范	一级防范
4	入侵报警系统	入侵探测（报警）器	紧急报警装置（一键报警）	门卫室、值班室、安防监控中心	门卫室、值班室、安防监控中心
5	出入口控制系统		封闭式独立院落的主要出入口、安防监控中心、危险物品存放处、涉密部位	封闭式独立院落的主要出入口、安防监控中心、危险物品存放处、涉密部位、重要建筑物出入口、网络通信等系统的关键部位	封闭式独立院落的主要出入口、安防监控中心、危险物品存放处、涉密部位、供电、供水、供气、供油、通风、空调和网络通信等部位以及通往重要部位的电梯等系统的关键部位
6	电子巡查系统		周界及重要部位	周界及重要部位	周界及重要部位
7	公共广播系统		区域全覆盖	区域全覆盖	区域全覆盖
8	防爆安检系统	X射线物品安检机（或/和便携式）	有禁止、限制携带物品进入的入口	有禁止、限制携带物品进入的入口	有禁止、限制携带物品进入的入口
9		通过式金属探测门	/	/	有禁止、限制携带物品进入的入口
10		手持式金属探测器	安检入口	安检入口	安检入口
11	信息隔离控制系统（网络防火墙、授时安全防护装置）		/	网络通讯控制区域	网络通讯控制区域
注：不同行业对禁止、限制携带物品有不同要求。					

10.1.2 应根据现场环境和反恐怖防范要求合理配置视频图像采集装置（视频监控设备）：

- 对周界的监视效果至少应能看清周界环境中人员的活动情况；
- 对出入口的监视效果应能清晰辨别出人员的面部特征和出入车辆的号牌；
- 对通道和公共区域的监视效果应能看清监控区域内人员、物品、车辆的通行情况；
- 对室内区域的监控效果应能清晰显示其内人员出入及活动情况。

10.1.3 人员密集区域应考虑视频图像采集装置（视频监控设备）的全覆盖。

10.1.4 周界和出入口等部位应考虑视频图像智能分析技术、人面识别技术的应用。

10.1.5 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，如IC卡识别、指纹识别、虹膜识别、人脸图像识别等。

10.1.6 重点目标管理单位应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。

10.1.7 重点目标管理单位应结合防范无人机袭击的需求，增设符合国家法律法规和有关要求的反无人机防御系统。

10.1.8 重点目标管理单位使用卫星时间同步装置的,应增设符合国家法律法规和有关要求的授时安全防护装置。装置应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。

注:授时安全防护装置即保护卫星时间同步装置免受干扰、攻击和欺骗的时空安全防护设备。

10.2 电子防范设备设施要求

10.2.1 基本要求

电子防范应符合以下要求:

- a) 电子防范系统各子系统应符合 GB 50348 的相关要求;
- 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。

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 50395、GB/T 25724、GB/T 28181、GA/T 367 和 GA/T 1127—2013 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—2018 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 视频监控设施要求

10.2.3.1 重要部位应设置视频图像采集装置,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,视频信息应能与公安机联网。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。

10.2.3.2 视频录像保存时间应不少于 90 日。

10.2.3.3 视频监控系统的备用电源应满足至少 4 小时正常工作的需要;入侵报警系统备用电源应满足至少 24 小时正常工作的需要。

10.2.3.4 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。

10.2.3.5 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。

10.2.4 入侵和紧急报警系统要求

10.2.4.1 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。

10.2.4.2 入侵和紧急报警系统应具备防拆、开路、短路报警功能。

10.2.4.3 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。

10.2.4.4 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。

10.2.4.5 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 90 日。

10.2.5 出入口控制系统要求

10.2.5.1 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。

10.2.5.2 出入口控制系统应满足紧急逃生时人员疏散的相关要求。

10.2.5.3 出入口控制系统信息存储时间应不少于 180 日。

10.2.5.4 出入口控制系统的安全等级应不低于 GB/T 37078—2018 中规定的 2 级要求。

10.2.6 电子巡查系统要求

10.2.6.1 电子巡查系统的巡查路线、巡查时间应根据安全管理需要进行设定和修改。

10.2.6.2 电子巡查系统巡查记录保存时间应不少于 90 日。

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。可视工作需要整合设置。

表 4 管理制度配置

序号	项目		配设要求
1	人防	教育培训及考核制度	按附录 B. 3. 1
2		人员背景审查制度	按附录 B. 3. 2
3		人员档案及备案制度	按附录 B. 3. 3
4		门卫与寄递物品管理制度	按附录 B. 3. 4
5		巡查制度	按附录 B. 3. 5
6		安全检查制度	按附录 B. 3. 6
7		值班监看和运维制度	按附录 B. 3. 7
8		训练演练制度	按附录 B. 3. 8
9		检查督导制度	按附录 B. 3. 9
10		人防增援配置制度	按附录 B. 3. 10
11	物防、技防	采购管理制度	按附录 B. 3. 11
12		设备设施档案制度	按附录 B. 3. 12
13		技防系统管理制度	按附录 B. 3. 13
14	综合	工作报告制度	按附录 B. 3. 14
15		网络安全管理制度	按附录 B. 3. 15
16		专项经费保障制度	按附录 B. 3. 16
17		情报信息管理制度	按附录 B. 3. 17
18		恐怖威胁风险评估制度	按附录 B. 3. 18
19		联动配合机制	按附录 B. 3. 19
20		应急管理制度	按附录 B. 3. 20
21		应急预案管理制度	按附录 B. 3. 21
22		保密制度	按附录 B. 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 制定技防、值守、巡查、网管、机动等岗位标准，每个岗位按作业流程列出工作细节，明确与其他工作接口相互协调要求。

11.2.3 有定额的岗位应明确定额，有数量和时间方面要求的，应量化。

11.2.4 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 非常态防范要求

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 重点目标管理单位可以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 重点目标管理单位应启动反恐应急响应机制，组织开展反恐怖动员，负责人应24小时带班组织防范工作，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 应加强重点目标的防护器具、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 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。

13.2 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。

13.3 宜建立相应的数据库和应急指挥系统。

13.4 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。

13.5 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。

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

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。

重点目标仅涉及一个行业主管部门的，应由该行业主管部门领导班子成员分管反恐怖防范工作，并应设置专职工作人员指导重点目标。

重点目标涉及多个行业主管部门的，应由反恐怖主义工作领导机构指定一个牵头部门负责，其他行业主管部门配合，共同指导重点目标。牵头部门应设置专职工作人员。

14.2 检查

14.2.1 自我检查

14.2.1.1 重点目标管理单位每年应对其反恐怖防范系统开展至少一次的自我检查，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。

14.2.1.2 自我检查及改进按附录C的要求进行。

14.2.1.3 应及时向行业主管部门递交自我检查报告。

14.2.2 督导检查

反恐怖主义工作领导机构的办事机构、公安机关、行业主管部门应定期、不定期地开展反恐怖防范的工作检查。公安机关、行业主管部门每半年应向反恐怖主义工作领导机构提交检查报告，报告内容包括：

- a) 本行业反恐怖防范概况及重点目标增减情况；
- b) 本阶段部门检查情况及整改情况；
- c) 存在的问题及原因分析；
- d) 下一阶段的部门检查计划。

14.2.3 检查的实施

自我检查、部门检查和督导检查的实施按附录D。

附 录 A
（资料性）
部分重点目标的重要部位

A.1 党政机关

党政机关反恐怖防范重要部位：机关大院（大楼）出入口、重要办公区域、档案室、机要室、保密室、财务室、案件管理中心、接访场所、公文交换中心、数据信息中心、文印中心、会议场所、配电站、通信系统、通风系统、空调系统、安防监控中心、枪支弹药存放场所、餐厅、停车库（场）等。

A.2 外事外交机构（驻地）

外事外交机构（驻地）反恐怖防范重要部位：对外缓冲区（包括馆舍外等候区）、主要出入口、电梯等候区、配电房、通风系统、电梯、监控中心、外国机构的馆舍、国际组织办公场所、楼顶、二次供水设施、地下停车场等。

A.3 城市中心广场

城市中心广场反恐怖防范重要部位：广场区域；周界；周界出入口（含无障碍通道），包括进出广场区域的地面出入口、地下停车场、地下商业区的地面出入口、地下通道、过街通道的出入口、地铁的出入口；国旗区；标志性建（构）筑物；供电设施；安防监控中心（室）；其他重要部位，包括制高点、配电室、喷泉控制室、广场内部道路、广场景观水体；其他经风险评估应防范的部位。

A.4 学校幼儿园

A.4.1 高等院校反恐怖防范重要部位：主要出入口（大门、宿舍、食堂餐厅、教学楼、办公大楼、实验大楼）、门卫室、安防监控中心、主要通道、广播（电视）室、配电房、锅炉房、燃气设施、水池及水泵房、重大活动时的场馆、危化物品储藏室、食堂操作间和储存间、重点实验室、档案室、专用试卷保密室、网络中心、校（院）长室、财务室、图书馆、停车场（库）、周界等。

A.4.2 中小学反恐怖防范重要部位：主要出入口、门卫室、安防监控中心、主要通道、广播（电视）室、配电房、水池及水泵房、运动场馆、危化物品储藏室、食堂操作间和储存间、重点实验室、档案室、专用试卷保密室、校（院）长室、网络中心、财务室、周界等。

A.4.3 幼儿园反恐怖防范重要部位：主要出入口、门卫室、安防监控中心、主要通道、广播（电视）室、午休房、配电房、水池及水泵房、操场、游泳池、食堂操作间和储存间、档案室、校（园）长室、财务室、周界等。

A.5 旅游景区（园林公园）

A.5.1 自然景观类景区：包括但不限于主要出入口、游客中心、集散中心、文娱表演场所、标志性建筑物、陈列展览厅（馆）、藏品库房、售票处、安防监控中心、游乐设施、索道、控制机房、危化品储存室、变配电房、大型显示屏，其中安防监控中心、藏品库房、控制机房、危化品储存室、变配电房为限制区域。

A.5.2 文博景区：包括但不限于周界、主要出入口、安防监控中心、贵重文物陈列展览厅（馆）、藏品保护技术区、藏品库房、藏/展品卸运交接区、公共服务区（包括公共活动区、服务设施、教育用房）、新风口（室内密闭景区适用）、变配电房，其中藏品保护技术区、藏品库房、藏/展品卸运交接区为限制区域。

A.5.3 主题公园景区：包括但不限于主要出入口、游客中心、集散中心、文娱表演场所、售票处、安

防监控中心、游乐设施、大型显示屏、危化品储存室、控制机房、新风口（室内密闭景区适用）、变配电房，其中安防监控中心、控制机房、变配电房为限制区域。

A.5.4 城市文化景区、宗教景区、建筑类景区的反恐怖防范重要部位分别按 A.3、A.11 和 A.33 的规定。

A.6 旅游饭店

旅游饭店反恐怖防范重要部位：主要出入口、主要通道、监控中心、高压配电房、锅炉房、食用水泵房、燃气总阀、中央空调控制机房、电话总机房、信息设备机房、电梯机房、驻店涉外机构周界、前台、厨房、停车库（场）（包括货物装卸区）、防范目标高空瞭望处、内部码头等区域。

A.7 文体场馆

A.7.1 体育场馆反恐怖防范重要部位：包括但不限于主要出入口、观众席、主席台、贵宾室、安全疏散通道、安防监控中心、消防中心、强弱电房、空调机房、水泵房、音视频控制室、停车库（场）。

A.7.2 影视剧院反恐怖防范重要部位：包括但不限于主要出入口、大堂、观众厅、贵宾室、多媒体显示屏、演出及放映设备控制室、变配电房、安防监控中心、空调机房及新风口、停车库（场）。

A.8 卫生健康

A.8.1 医疗机构反恐怖防范重要部位：主要进出通道、门诊大厅、急诊大厅、生物安全实验室、监控中心、网络与信息中心机房、配电间、发电机房、危险化学品库、危险药品库、易燃易爆物品存放库房、停车场、气体室（站）、消防控制室、食堂、放射源与设备、医疗废弃物暂存间、储水池、污水处理站、救护车等。

A.8.2 疾病预防控制机构反恐怖防范重要部位：实验菌（毒）种（株）、菌（毒）种库、实验室、疫苗冷库、传染病档案室、监控中心、网络与信息中心机房、配电间、发电机房、危险药品库、易燃易爆物品存放库房、气体室（站）、消防控制室、放射源与设备、医疗废弃物暂存间、储水池等。

A.8.3 血液中心反恐怖防范重要部位：主要进出门口、血库、配电间、发电机房等。

A.8.4 120 急救中心反恐怖防范重要部位：120 急救指挥系统的控制中心、配电间、发电机房等。

A.8.5 高等级病原微生物实验室反恐怖防范重要部位：实验室设立单位和（或）实验室所在建筑物的周界；实验室设立单位和（或）实验室所在建筑物的周界出入口；实验室所在建筑物出入口；门卫值班室；通往实验室的电梯、电梯厅、通道（楼道、楼梯）；实验室设立单位的安防监控中心（室）；实验室出入口；核心工作间；保存菌（毒）种及样本的房间；中控室；设备机房；其他经风险评估应防范的部位。

A.8.6 病原微生物菌（毒）种保藏中心反恐怖防范重要部位：保藏中心设立单位和（或）保藏中心所在建筑物的周界；保藏中心设立单位和（或）保藏中心所在建筑物的周界出入口；保藏中心所在建筑物的出入口；门卫值班室；通往保藏中心的电梯、电梯厅、通道（楼道、楼梯）；高致病性病原微生物保藏区、接收区、发放区；保藏中心配套高等级病原微生物实验室；保密数据存储场所；安防监控中心（室）；其他经风险评估需要防范的部位。

A.8.7 高生物安全风险疫苗生产单位反恐怖防范重要部位：园区周界；园区周界出入口；园区门卫值班室；园区内主要道路；安防监控中心（室）；生产车间周界；生产车间周界出入口；通往防护区的电梯、电梯厅、通道（楼道、楼梯）；生产车间防护区；生产车间核心工作区；生产车间中控室；成品库房；设备机房；其他经风险评估应防范的部位。

A.9 商业中心

A.9.1 商场超市反恐怖防范重要部位：主要出入口、主要通道、重大活动区域、监控中心、高压配电房、中央空调控制机房、电梯机房、食用水泵房、燃气总阀、财务出纳室、物资储存仓库、贵重商品存

放区、寄递物品存放区、停车库（场）（包括货物装卸区、临时车辆停靠区）、装修施工现场、天台等。

A. 9.2 大型专业市场反恐怖防范重要部位：包括但不限于主要出入口、主要通道、大型活动区域、安防监控中心、高低压配电房、中央空调控制机房及新风口、水泵房、二次供水池（箱）、公共广播控制室、大型显示屏控制室、易燃易爆仓库、信息中心、停车库（场）。

A. 10 会展场所

会展场所反恐怖防范重要部位：主要出入口、主要通道、活动场地、展会重要展示区域、安防监控中心、办证中心、配电房、中央空调控制机房、大型显示屏控制室、公共广播控制室、水泵房、二次供水池（箱）、燃气总阀、信息中心、停车库（场）。

A. 11 宗教活动场所

宗教活动场所反恐怖防范重要部位：主要出入口、主要通道、殿堂、标志性建筑、视频监控室、电房、燃香烛处、停车场、周界等。

A. 12 城市公共交通

A. 12.1 公交站场反恐怖防范重要部位：乘客上车区、落客区、站场主要出入口、远程监控中心等。

A. 12.2 城市轨道交通反恐怖防范重要部位：人员密集区域，包括车站、运营列车等；关键区域，包括主变电所（站）、运营控制中心、风亭、车辆段、停车场、地面区间沿线、隧道口（含过渡段）等。

A. 13 汽车客运站

汽车客运站反恐怖防范重要部位：售票厅（室）、候车厅（室）、站场出入口、安检区域、站内人行通道、安防监控中心（室）、发车卡位、落客区、行包托运寄存处等。

A. 14 港口码头

A. 14.1 货运码头反恐怖防范重要部位：外界出入口（人员出入口、机动车出入口、火车出入口）、安防监控中心、限制区域、安检区域、生产调度指挥中心、机房、保密档案室、消防控制室、配电站、加油站（加油车）、生产用燃料油储存库、码头前沿及水域、储罐区、含油管（道）线、码头装卸泊位、引桥、船岸通道、危险货物的仓库或集装箱堆场。

A. 14.2 涉外客运码头反恐怖防范重要部位：人员密集类重要部位，包括但不限于客车停车区、外界出入口、安检区域、候船厅、出入境联检区域、旅客主要通道、电梯；其他部位，包括：限制区域、安防监控中心、消防控制室、配电站、广播（媒体）控制室，保密档案室、码头前沿及水域、泊位等。

A. 14.3 国内客运码头反恐怖防范重要部位：人员密集类重要部位，包括：外界出入口、售票处、验（检）票处、安检区域、候船室（区）、登（离）船通道；其他部位，包括：安防监控中心、广播（媒体）控制室、泊位、码头前沿及水域。

A. 15 口岸

A. 15.1 水路口岸反恐怖防范重要部位：外界出入口（人员出入口、机动车出入口、火车出入口）、安防监控中心、限制区域、安检区域、生产调度指挥中心、码头前沿及水域、含油管（道）线、码头装卸泊位、引桥、船岸通道、危险货物的仓库或集装箱堆场。

A. 15.2 陆路口岸反恐怖防范公共区域的重要部位：旅检大厅、旅检通道、旅检区广场、货检区域、交通运输工具公共查验场地（客运车道、货运车道）、与地铁（高铁）接驳区域、公交车（出租车）站、停车库（场）、联勤联动办公室、监控中心等。

注：口岸查验单位内部区域的重要部位由各单位自行确定。

A. 16 通信设施

通信设施反恐怖防范重要部位：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、空调主机室、网络管理监控室、安防监控室、消防监控室等。

A.17 传媒设施

A.17.1 媒体机构反恐怖防范重要部位：院落周界；院落周界出入口；门卫室；重要办公建筑出入口；重要机房，包括广播电视台数据中心机房、播出机房、主控机房、新媒体机房、通讯社数据中心机房、无线收发站机房、报刊社数据中心机房、采编业务机房、卫星传版机房、网站和新媒体的数据中心机房、发布系统机房；重要区域，包括广播电视台技术区、直播间、演播厅、通讯社技术指挥中心、发稿区、报刊社全媒体指挥中心、核心编发区、网站和新媒体直播间；安防监控中心；其他经风险评估需要防范的部位。

A.17.2 广播电视发射台、卫星地球站、微波站、监测台反恐怖防范重要部位：院落周界；院落周界出入口；门卫室；技术区主要出入口；重要机房，包括中控机房、发射机房、节传机房、监测机房、电力（电源）室、天线调配室、天线交换室；安防监控中心；其他经风险评估需要防范的部位。

A.17.3 有线电视网络枢纽设施和卫星直播枢纽设施反恐怖防范重要部位：重要办公建筑出入口；重要机房，包括前端播出机房、数据中心机房、网管中心机房、传输机房、电源室、卫星直播节目集控平台机房；安防监控中心；其他经风险评估需要防范的部位。

A.18 发电供电

A.18.1 电力调度机构反恐怖防范重要部位：周界；周界出入口、门卫室；调度楼出入口；通往调度控制中心（室）、信息通信机房、通信调度中心（室）的电梯、电梯厅及通道；调度控制中心（室）、信息通信机房、通信调度中心（室）出入口；调度控制中心（室）与信息通信机房以及配电室相连的强弱电设备间；供电电缆、通信电缆、光缆等线缆通道；与外界相通的窗口、通风口、管道口（沟、渠等）；安防监控中心（室）；其他经评估应防范的重要部位。

A.18.2 变电站、换流站（含接地极址）反恐怖防范重要部位：周界；周界出入口、门卫室；与站外相通的窗口、通风口、管道口（沟、渠等）；安防监控中心（室）/安防设备间；主控楼出入口；主控室、二次设备机房出入口。

A.18.3 直接为重要用户供电的变电站反恐怖防范重要部位：周界；周界出入口；与站外相通的窗口、通风口、管道口（沟、渠等）。

A.18.4 直接为重要用户供电的开关站反恐怖防范重要部位：与站外相通的门；与站外相通的窗口、通风口、管道口（沟、渠等）。

A.18.5 火力发电站（厂）反恐怖防范重要部位：站（厂）周界；站（厂）周界出入口；生产区出入口；运煤铁路和公路的进（出）厂道口；站（厂）内主要道路；汽轮机房、锅炉区域；液氨贮存区、燃油设施区、制（供）氢站、天然气调压站；主变压器和升压站区域；危险化学品库；集中控制室；安防监控中心（室）；供水设施区域；其他经评估应防范的重要部位。

A.18.6 水电站（厂）反恐怖防范重要部位：周界及主要出入口；大坝区域；厂房区域；大坝区域和厂房区域之外的建筑物；水电站（厂）运行管理的通航设施；安防监控中心（室）；其他经评估应防范的重要部位。

A.18.7 风电场反恐怖防范重要部位：升压变电站（或开关站）；换流站；集控中心；其他经评估需要防范的部位。

A.18.8 光伏电站反恐怖防范重要部位：升压变电站（或开关站）；集控中心（安防监控中心）。

A.18.9 光热发电站反恐怖防范重要部位：周界及主要出入口；站内主要道路；发电区周界；汽轮机房、启动锅炉房；燃油、燃气设施区；制（供）氢区；升压变电站（或开关站）；化学药品库；集控中心（安防监控中心）。

A. 18.10 核电站（厂）的反恐怖防范重要部位：周界，包括管理区周界、控制区周界、保护区周界和要害区周界；周界出入口，包括管理区周界出入口、控制区周界出入口、保护区周界出入口和要害区周界出入口；主要道路，包括管理区主要道路，控制区、保护区和要害区主要道路；管理区主要建（构）筑物；管理区安防监控中心（室）；保卫控制中心；其他重要部位，包括反应堆厂房、核燃料厂房、主控室、汽轮机房、主变压器、开关站区域、危险化学品库、放射源库、冷却水泵房、核材料数据库机房；其他经评估需要防范的部位。

A. 19 城市供水

城市供水系统反恐怖防范重要部位：周界；周界主要出入口；清水池；变配电室；中央控制室（调度室）；泵房；危化品储藏室（库）；加药间；地表水取水设施、水源井、补压井；安防监控中心（室）；列为重点目标的调蓄水池（箱）；其他经评估应防范的部位。

A. 20 城镇燃气

城镇燃气系统防范恐怖重要部位：燃气厂站周界、出入口、门卫（值班）室；燃气厂站核心生产区、工艺区；燃气厂站控制室；城市主要燃气调度中心出入口、调度大厅、信息通信机房；其他经评估应防范的部位。

A. 21 公路桥梁隧道

A. 21.1 公路、桥梁的反恐怖防范重要部位：包括但不限于桥梁承载结构（梁、墩、台、索、杆、塔、拱）、安防监控中心、配电房、重要内部结构（如箱梁、桥塔、锚室等）。

A. 21.2 隧道反恐怖防范重要部位：包括但不限于隧道承载结构（衬砌、接缝）、隧道出入口、隧道通道、安防监控中心、配电房、通风设施、隧道范围水面。

A. 22 水利设施

A. 22.1 水库工程反恐怖防范重要部位：主要出入口、大坝、泄洪设施、取（进）水口、廊道出入口、水电厂房、调度中控室（监控中心）、启闭机房。

A. 22.2 引调水工程反恐怖防范重要部位：主要出入口、取水口、重点渠段、重要节制闸、启闭机房、泵站（房）、配电房、调度中控室（监控中心）、重要涵洞。

A. 22.3 拦河闸工程反恐怖防范重要部位：主要出入口、水闸主体结构、启闭机房、调度中控室（监控中心）。

A. 23 粮食和物资储备仓库

A. 23.1 粮食和物资储备仓库反恐怖防范重要部位：粮食和物资储备仓库出入口；仓库；生产车间；配（变）电室；集中控制室；粮食仓库工作塔；安防监控中心；门卫处；重要技防系统设施；储粮药剂室；实验室；周界；粮食码头；消防泵房；应急物资器材存放室和微型消防站等。

A. 23.2 通用仓库的反恐怖防范重要部位：库区周界；库区周界出入口；库房；装卸区域；内部道路；行政楼主出入口；安防监控室；信息机房、档案室；其他经评估应防范的重要部位。

A. 24 货币发行及数据处理中心

A. 24.1 金库反恐怖防范重要部位：包括但不限于与外界相连的出入口、守库室、出入库通道、出入库交接场地、票币清分场地、金库库体、供电房、安防监控中心、周界。

A. 24.2 综合办公大楼反恐怖防范重要部位：包括但不限于主要出入口、服务大厅、现金服务区、现金交接区域、现金清分场所、保管箱库、档案库、供电房、安防监控中心、贵金属展示区、银行自助设备处。

A. 24.3 数据中心、清算中心反恐怖防范重要部位：包括但不限于出入口、机房、供电房、监控室、通风系统。

A. 25 石油石化

A. 25.1 油气田企业反恐怖防范重要部位：周界、周界出入口、门卫值班室、安防监控中心、油气处理核心装置区。

A. 25.2 炼油与化工企业反恐怖防范重要部位：厂区周界、厂区周界出入口、核心生产装置区、储油（气）罐区、集中管理的全厂性生产控制中心。

A. 25.3 加油（气）站反恐怖防范重要部位：站区出入口、油（气）操作区、油（气）储罐区、监控设备存放区、收银处。

A. 25.4 储油（气）库反恐怖防范重要部位：库区周界出入口；库区周界；油（气）储罐区；接卸油（气）作业区；油（气）发货作业区；监控中心（控制室）；内部道路；装卸区；门卫值班室；内部道路；铁路装卸区；公路装卸区；水运装卸区；油泵房等；行政区，包括内部道路、信息机房、档案室等；辅助作业区，包括内部道路、变配电间、化验室等；库外输油管道；其他经评估应防范的重要部位。

A. 25.5 工程技术服务企业反恐怖防范重要部位，包括但不限于：周界、周界出入口、装卸区域、安防监控室或保卫值班室。

A. 25.6 运输企业反恐怖防范重要部位，包括但不限于：周界、周界出入口、门卫值班室、安防监控室、主要通道、运输车辆停放区、危险化学品道路运输车辆。

A. 25.7 石油天然气管道企业反恐怖防范重要部位，包括但不限于：周界；周界出入口值班室；安防监控中心（室）；输油泵房/棚；输油气管道系统跨越或隧道穿越大型河流管段；输油气管道系统地处治安复杂、人口密集区部位；输油管道系统地处水源地（饮用水水源保护区）部位。

A. 25.8 石油储备库反恐怖防范重要部位：石油储备库周界及出入口；内部道路；储油区（设施），包括储罐（含地下水封洞罐）、储油附属设施、油泵房；安防监控中心；调度运行中心；消防控制中心；重要运行保障设施，包括水、气、电、通信、消防等系统的核心设备；其他经评估需要防范的部位。

A. 26 枪支弹药库及生产厂

枪支弹药库及生产厂反恐怖防范重要部位：库区，包括周界、出入口、门卫值班室、内部道路、库房、取样间；转运站，包括周界、出入口、门卫值班室、装卸区；行政区，包括门卫值班室、安防监控中心、钥匙管理室、档案室；重要运行保障设施，包括水、电、通信、消防等系统的核心设备；其他经评估应防范的重要部位。

A. 27 民用爆炸物品库及生产厂

A. 27.1 生产企业的反恐怖防范重要部位：安防监控中心、出入口、周界、停车场、生产车间、存储场所、试验场、销毁场、民用爆炸物品运输车辆、现场混装炸药车。

A. 27.2 销售企业的反恐怖防范重要部位：安防监控中心、出入口、周界、存储场所、装卸区。

A. 27.3 运输企业的反恐怖防范重要部位：监控室、停车场、民用爆炸物品运输车辆。

A. 27.4 使用企业（爆破作业）的反恐怖防范重要部位：使用场所、存储场所。

A. 27.5 火炸药库反恐怖防范重要部位：库区，包括周界、出入口、门卫值班室、内部道路、库房、取样间；转运站，包括周界、出入口、门卫值班室、装卸区；行政区，包括门卫值班室、安防监控中心、钥匙管理室、档案室；重要运行保障设施，包括水、电、通信、消防等系统的核心设备；其他经评估应

防范的重要部位。

A.28 烟花爆竹库及生产厂

烟花爆竹库及生产厂反恐怖防范重要部位：库区，包括周界、出入口、门卫值班室、内部道路、库房、取样间；转运站，包括周界、出入口、门卫值班室、装卸区；行政区，包括门卫值班室、安防监控中心、钥匙管理室、档案室；重要运行保障设施，包括水、电、通信、消防等系统的核心设备；其他经评估应防范的重要部位。

A.29 危险化学品库及生产厂

A.29.1 危险化学品生产企业反恐怖防范重要部位：厂区周界、厂区出入口、保卫值班室、安防监控中心（室）、生产控制中心（室）、核心生产装置区、储罐区、危险化学品库房、危险化学品装卸区、其他经评估需要防范的部位。

A.29.2 危险化学品经营企业反恐怖防范重要部位：企业周界；企业出入口；通往仓库、罐组的道路；仓库；罐组；装卸作业区；安防监控中心；其他需要防范的重要部位。

A.30 核技术利用单位

A.30.1 核设施单位反恐怖防范重要部位：周界，包括控制区周界、保护区周界和要害区周界；周界出入口，包括控制区周界出入口、保护区周界出入口和要害区周界出入口；保卫控制中心、保卫值班室和安防监控室；其他重要部位，包括反应堆、临界装置、带有放射性和/或使用核材料的辅助实验装置、核材料生产工艺厂房、核燃料元件制造工艺厂房、乏燃料后处理主工艺厂房、核材料库、乏燃料存放场所、高中低放废液及高中放固体废物处理与暂存厂房、高中放废物处置单元、涉及核材料的分析实验室、核材料数据库机房、中央控制室、危险化学品库、放射源库、保障安全生产必需的能源动力装置；其他经评估应防范的重要部位。

A.30.2 城市放射性废物库反恐怖防范重要部位：库区周界、周界出入口、库区主要道路、库房、安防监控室。

A.30.3 放射源生产场所反恐怖防范重要部位：生产场所出入口、放射源生产区和存放区、放射性物品存放区、安防监控室。

A.30.4 放射源使用场所反恐怖防范重要部位：辐照室、控制室及辐照货物装卸区；探伤源和石油测井源库房；安防监控室。

A.31 危险化学品运输企业

危险化学品运输企业反恐怖防范重要部位：包括但不限于危险化学品运输车辆（重车）。

A.32 大型活动

A.32.1 封闭式固定场所活动反恐怖防范重要部位：包括但不限于主要出入口，主要通道，安全疏散通道，主要流线，舞台、看台、观众席等固定及临时搭建物，指挥中心，安防监控中心，转播直播室，新风口，供水，供电，供气，通信，电子显示屏，广播设备。

A.32.2 开放式固定场所活动反恐怖防范重要部位：包括但不限于主要出入口，主要通道，主要流线，广场，舞台、展台、展架等临时搭建物，指挥中心，安防监控中心，转播直播室，供水，供电，通信，电子显示屏，广播设备。

A.32.3 其他临时性场所活动反恐怖防范重要部位：包括但不限于活动起终点，主要流线，广场，舞台、展台、展架等临时搭建物，指挥中心，供水，供电，通信，电子显示屏，广播设备，治安缓冲区域。

A.33 标志性建筑物

标志性建筑物反恐怖防范重要部位：主要出入口、大堂、观光层、观光电梯、候梯厅、建筑结构关键构件及节点、新风入口、新风机房、生活水箱、消防水池、高低压变压器房、燃气调压柜、发电机房及其储油间、锅炉房、信息中心机房、垂直运输系统（消防电梯）、室外宣传屏幕及控制端、安防监控中心、公共广播系统控制室、避难层、屋面层、直升机停机坪和停车库（场）。

A.34 监狱公安监管场所

A.34.1 监狱类反恐怖防范重要部位，包括但不限于：各监区监舍、监狱医院、多功能大厅、劳动现场、监狱燃气燃油储存室、伙房、变电室、危化品仓库、管教谈话室、图书阅览室、医务室、收押中心、物料间、晾衣间、监狱枪弹库、保密室、监狱大门、AB门区域、监管区（含各监区内部）各通道、监狱周界围墙、武警岗哨、指挥中心、监控室、监狱综合服务大厅（接待、会见大厅等）、提审室、会见室等。

A.34.2 看守所类反恐怖防范重要部位，包括但不限于：监所内监室、拘室、监所内燃气燃油储存室伙房、变电室、管教谈话室、医务室、收押室、监所枪弹库、保密室、监所外大门、AB门区域、监区内各通道、监所周界围墙、武警岗哨、监控室、监所接待大厅、顾送室、提讯室、会见室。

A.34.3 其他监管场所类反恐怖防范重要部位，包括但不限于：监所内监室、拘室、监所内燃气燃油储存室伙房、变电室、管教谈话室、医务室、收押室、监所枪弹库、保密室、监所外大门、AB门区域、监区内各通道、监所周界围墙、武警岗哨、监控室、监所接待大厅、顾送室、提讯室、会见室。

A.35 其他

反恐怖防范重要部位参照 5.2.2 重要部位划分根据实际确定。

附录 B (规范性) 管理制度要求

B.1 概述

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。

B.2 制度的基本框架

制度的基本框架至少应包括以下内容：

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

B.3 管理制度

B.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：

- 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；
- 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；
- 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；
- 宣传教育：协助各有关部门开展反恐怖主义宣传教育；
- 考核：应包括反恐知识考核和技能考核。

B.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：

- 责任领导；
- 部门负责人；
- 保卫管理人员；
- 联络员；
- 保安员；
- 技防岗位人员。

人员背景审查的内容至少应包括：

- 个人资料，身份信息和户口信息；
- 个人经历，教育、就业履历和出入境记录；

- 无犯罪记录；
- 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。

B.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。

B.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。

B.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。

B.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。

B.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，定期开展技防各系统的运行维护检查，保障各系统的正常运行。

B.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：

- 安保力量的训练演练要求；
- 训练演练计划的要求；
- 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；
- 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。

B.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。

B.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：

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

B.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。

B.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：

- 物品名称、型号、编号；
- 物品管理编号，领用人或保管人；
- 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）；
- 物品的使用状态，包括在用、停用和报废；
- 操作手册（使用、维护和保养）；
- 维护保养记录。

B.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：

- 系统名称、型号；
- 工程提供和建设方名称；
- 系统责任人；
- 维护保养周期。

系统管理档案至少应包括以下内容：

- 采购有关资料；
- 建设工程有关的资料，包括设计、验收报告等；
- 所有设备设施的使用说明书，合格证、检验报告和验收资料；
- 操作手册（使用、维护和保养）；
- 维护保养记录。

B.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：

- 人防配置及实施情况；
- 物防配置及实施情况；
- 技防配置及实施情况；
- 制度防配置及实施情况；
- 自我检查报告。

存在下列情况时应提交工作报告：

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

B.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。

B.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：

- 人防配置及奖励制度有效落实；
- 物防配备、更新防范和处置设备设施；
- 技防系统正常运维；
- 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。

B.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。

B.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：

- 可识别性：重点目标可以被了解和熟悉、关注和重视的程度；
- 可接近性：重点目标可以被靠近、进入的难易程度；
- 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；
- 标志性和轰动性：重点目标敏感度、关注度、社会影响的程度；

——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。

B.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。

B.3.20 应急管理制度

重点目标管理单位应制定应急管理制度，针对暴力破坏、袭击事件的规律、特点和可能造成的社会危害，制定并实施反恐怖应急预案。

B.3.21 应急预案管理制度

重点目标管理单位应制定应急预案管理制度，增强应急预案的科学性、针对性、实效性。明确应急预案的编制和管理，定期对应急预案开展学习培训，定期对预案的适用性进行评价。

B.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 C

（规范性）

反恐怖防范系统自我检查及改进

C.1 自我检查

C.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。

C.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。

C.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。

C.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。

C.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 and 不合格报告；
- f) 检查结果处置；
- g) 考核奖惩。

C.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。

C.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进行分析研究，制定纠正和预防措施。

C.2 改进

C.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—实施—检查—改进）管理模式进行。

C.2.2 改进的实施及依据

C.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。

C.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。

C.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。

C.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。

C.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 D
（规范性）
反恐怖防范工作检查实施

D.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。

D.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。

D.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。

D.4 检查内容

检查内容见表D.1、表D.2。

D.5 检查结果及处置

D.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。

D.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。

D.6 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。格式见表D.1、表D.2。

表 D.1 台账检查表格

序号	项目	内容概要	检查情况记录	项目结论
1	基础情况	重点目标类别及等级、确立时间，查看重点目标确认资料		
2		重点目标平面图、重要部位分布图/列表是否清晰、完整，是否及时报备		
3		反恐怖防范工作组织结构图、第一负责人、责任领导、责任部门情况及相关信息，查看资料		
4		反恐联络员信息及与公安机关、反恐怖工作领导机构联系的记录		
5	人力防范	重点目标安保力量配置表（包括安保力量持证上岗证明材料）		
6		是否建立重要岗位人员名录、背景审查及备案记录，查看档案资料及备案回执		
7		是否对出入口人员、车辆进行登记检查，检查记录		
8		是否对寄递物品进行验视、签收和登记管理，检查记录		
9		是否按有效的路径和方式开展巡查，检查记录		
10		视频监控系统的值班监看是否到位，检查值班记录		
11		检查教育培训记录，是否按教育计划开展		
12		检查训练记录，是否按训练计划开展		
13		检查演练记录，是否按演练计划开展		
14	实体防范	物防设备设施清单及使用位置		
15		防冲撞设施建设情况，查看技术资料及验收报告		
16		物防设备设施维护，检查记录		
17	电子防范	安防监控中心建设情况（位置及平面布局图，包括门窗位置；设备情况，包括显示屏数量；视频保存时间等）		
18		技防系统清单及使用区域		
19		摄像机安装平面图		
20		入侵报警器、紧急报警装置（一键报警）安装平面图		
21		出入口控制系统安装平面图		
22		信息隔离控制系统配置情况		
23		技防系统运行维护保养相关资料（维护保养台账等）		
24		相关工作记录		
25	制度防	反恐怖防范责任管理制度		
26		管理制度清单及标准文本		
27		重要岗位标准清单及标准文本		
28		使用的技防、物防设备操作规程清单及文本		
29		应急处置预案		
30		是否开展自我检查督导和反恐怖防范体系自我检查工作，查看相关记录		
31		对反恐怖防范工作中存在的问题实施持续改进的相关记录		
32		网络安全等级保护测评报告		

表D.2 现场检查表格

序号	内容概要		检查情况记录	项目结论
1	实体 防范	机动车阻挡装置设置是否已覆盖无实体防护屏障的主要出入口		
2		防机动车冲撞或隔离设施是否已覆盖主要出入口和受机动车冲击后容易受到重大伤害的重要部位		
3		生产运营核心要害部门、监控中心等重要部位出入口有否设立防盗安全门等实体防护设施		
4		设置的围墙或栅栏外侧高度是否大于2.5米		
5		是否设置警示标志		
6		是否按实际需要配备了对讲机、强光手电、防护棍棒、防暴盾牌、钢叉、防暴头盔、防割（防刺）手套、防刺服等个人应急防护装备		
7		是否按实际需要配备了防爆毯（防爆围栏）、防爆球等公共应急防护装备		
8		是否设置了应急照明灯光		
9		门卫室对外窗口和建筑物二层以下的监控中心是否有防盗窗或护栏		
10		涉危险物品的重点目标是否配置了相应的防护装备，如防护口罩和消洗喷剂		
11	电子 防范	摄像机是否已覆盖周界、出入口、安防监控中心；人员密集区域、涉危险物品区域等生产运营核心要害部位（三级及以上）；供电、供水、供气、供油、通风、空调和网络通信等系统关键部位（二级及以上）；通往重要部位的电梯、通道和出入口等系统关键部位（一级）		
12		与外界相通的出入口等重要部位配置的摄像机是否满足GA/T 1127—2013中规定的C类高清晰度及以上要求，视频信息是否与公安机关联网，查看录像参数		
13		视频录像保存时间是否不少于90日，查看90日前任意视频		
14		视频监控范围内的报警系统发生报警时，是否能与该视频系统联动。辅助照明灯光是否满足视频系统正常摄取图像的照度要求		
15		视频监控系统的备用电源是否满足至少4小时正常工作的需要；入侵报警系统备用电源是否满足至少24小时正常工作的需要		
16		入侵探测（报警）器是否已覆盖封闭式独立院落的周界（三级及以上）；危险物品存放处、涉密部位等生产运营核心要害部位（二级及以上）；网络通信等系统的关键部位（一级）		
17		报警系统信息本地保存时间是否不少于180日，并具备与公安机关联动的接口		
18		紧急报警装置（一键报警）是否已设置在门卫室、值班室、安防监控中心		
19		出入口控制系统是否已设置在封闭式独立院落的主要出入口、安防监控中心、危险物品存放处（三级及以上）；重要建筑物出入口、网络通信等系统的关键部位（二级及以上）；供电、供水、供气、供油、通风、空调以及通往重要部位的电梯等系统的关键部位（一级及以上）		
20		周界及重要部位是否设置了电子巡查系统		
21		公共广播系统是否已区域全覆盖		
22		安检入口是否设置了手持式金属探测器		
23		有禁止、限制携带物品进入的区域是否设置了通过式金属探测门、X射线物品安检机（或/和便携式）等安检设备		
24		是否设置信息隔离控制系统（网络防火墙、授时安全保护装置）		

参 考 文 献

- [1] GB/T 32555—2016 城市基础设施管理
 - [2] GA 1801—2022（所有部分） 国家战略储备库反恐怖防范要求
 - [3] GA 1802—2022（所有部分） 生物安全领域反恐怖防范要求
 - [4] GA 1803—2022 城市中心广场反恐怖防范要求
 - [5] 中华人民共和国主席令第三十六号 中华人民共和国反恐怖主义法
 - [6] 中华人民共和国主席令第六十九号 中华人民共和国突发事件应对法
 - [7] 中华人民共和国国务院令 第 421 号 企业事业单位内部治安保卫条例
 - [8] 中华人民共和国国务院令 第 564 号 保安服务管理条例
-