

DB11

北京市地方标准

DB 11/T XXXX—XXXX

重点单位安全防范要求 总则

Internal security management specifications: general requirements

(征求意见稿)

XXXX – XX – XX 发布

XXXX – XX – XX 实施

北京市市场监督管理局 发布

目次

目次 I

前言 III

引言 IV

1 范围 5

2 规范性引用文件 5

3 术语和定义 6

4 总体要求 9

 4.1 一般要求 9

 4.2 人员要求 9

 4.3 制度要求 10

 4.4 应急要求 10

 4.5 建设要求 10

5 常态防范要求 11

 5.1 一般要求 11

 5.2 人力防范要求 11

 5.3 实体防范要求 11

 5.4 电子防范要求 11

6 重点单位防范要求 12

 6.1 重点单位类别 12

 6.2 重点部位和区域 13

 6.3 风险等级和防范级别 13

 6.4 一般要求 13

 6.5 三级防范要求 14

 6.6 二级防范要求 16

 6.7 一级防范要求 17

7 非常态防范要求 18

 7.1 人力防范 18

 7.2 实体防范 18

 7.3 电子防范 19

8 系统技术要求 19

 8.1 基本要求 19

 8.2 入侵和紧急报警系统 19

 8.3 视频监控系统 19

 8.4 出入口控制系统 19

 8.5 电子巡查系统 20

8.6 停车库（场）安全管理系统 20

8.7 安全检查系统 20

8.8 实体防护系统 20

8.9 安全防范管理平台 21

9 监督检查要求 21

9.1 内部检查 21

9.2 外部监督 21

附录 A （资料性） 风险评估程序 23

附录 B （规范性） 单位内部安全防范管理工作职责 25

附录 C （规范性） 单位内部安全防范制度内容 26

附录 D （规范性） 常态防范设施配置 27

附录 E （资料性） 重点单位非限制区防护 28

附录 F （规范性） 重点单位常态防范设施配置 30

附录 G （规范性） 单位内部检查内容 33

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。

本文件由北京市公安局提出并归口。

本文件由北京市公安局组织实施。

本文件起草单位：

本文件主要起草人：

引言

为贯彻首都治安保卫工作方针，顺应单位内部治安形势发展，加强全市单位内部安全防范工作，建立长效管理机制，维护首都单位安全稳定，制定本文件。

根据重点单位安全防范工作需要，从基础、总体、共性原则提出适用于重点单位安全防范的通用要求。后续再根据需要，面向特定行业重点单位的具体管理要求提出行业要求，以进一步明确重点单位安全防范工作要求，提升重点单位安全防范的针对性、有效性和适用性。

重点单位安全防范要求 总则

1 范围

本文件规定了重点单位内部安全防范的总体要求、常态防范要求、非常态防范要求、系统技术要求和监督检查要求。

本文件适用于北京市行政区域机关、团体、企业、事业单位和民办非企业内部安全防范建设和管理工作，其他单位可参照执行。

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 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 9361 计算机场地安全要求

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 15208.2 微剂量 X 射线安全检查设备 第2部分：透射式行包安全检查设备

GB 15210 通过式金属探测门通用技术规范

GB 15603 危险化学品仓库储存通则

GB 17565-2022 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 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 32581 入侵和紧急报警系统技术要求

GB/T 33170 大型活动安全要求

GB 35114 公共安全视频监控联网信息安全技术要求

GB/T 37078 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 40248 人员密集场所消防安全管理

GB/T 41483 基于介电常数技术的液态危险化学品安全检查仪通用技术要求

GB 50174 数据中心设计规范

GB 50348 安全防范工程技术标准

GB 51309 消防应急照明和疏散指示系统技术标准
GB 55029 安全防范工程通用规范
GA 68 防刺服
GA 69 防爆毯
GA 294 防暴头盔
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 614 防割手套
GA/T 644 电子巡查系统技术要求
GA/T 761 停车库(场)安全管理系统技术要求
GA 872 防爆球
GA 844 防砸透明材料
GA 883 公安单警装备 强光手电
GA 1002 剧毒化学品、放射源存放场所治安防范要求
GA 1016 枪支(弹药)库室风险等级划分与安全防范要求
GA/T 1132 车辆出入口电动栏杆机技术要求
GA/T 1145 约束叉
GA/T 1336 车底成像安全检查系统通用技术要求
GA 1511 易制爆危险化学品储存场所治安防范要求
GA/T 1731 乘用车辆X射线安全检查系统技术要求
GA/T 1799 保安安全检查通用规范
DB11/T 855 安全防范系统运行与维护要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

单位 organization

机关、团体、企业、事业单位和民办非企业的简称。

3.2

治安保卫重点单位 key security and safeguard organization

关系国家安全、公共安全和国计民生，对国家或所在地区经济发展、社会稳定和人民生活具有重要影响的单位。

3.3

防范对象 **defensing object**

需要防范的、对单位及其内部构成安全威胁的对象。

[来源：GB 50348—2018，2.0.19，有修改]

3.4

安全防范 **security**

综合运用人力防范、实体防范、电子防范等多种手段,预防、延迟、阻止入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等事件发生的活动。

[来源：GB 50348—2018，2.0.1]

3.5

人力防范 **personal 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。

[来源：GB 50348—2018，2.0.2]

3.6

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。

[来源：GB 50348—2018，2.0.3]

3.7

电子防范 **electronic security**

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。

[来源：GB 50348—2018，2.0.4]

3.8

治安保卫机构 **security and protection agency**

单位内设的负责本单位内部治安保卫工作，配合公安机关打击处理违法犯罪活动的机构。

3.9

治安保卫人员 **security personnel**

单位内部从事维护治安秩序、开展安全防范、预防违法犯罪，保护单位内部人员和财产安全的人员。包括治安保卫管理人员和保卫执勤人员，其中保卫执勤人员由保安员和从事巡逻、值守、安检、值机等具体工作的单位人员组成。

3.10

治安保卫管理人员 **security management personnel**

履行单位内部治安保卫管理职责，组织实施单位内部安全防范工作的人员。

3.11

保安员 security guard

依照保安服务管理条例取得相关资格证，从事保安服务工作的人员。

3.12

限制区 restricted area

出于安全管理需求，只允许获得明确许可，方可进入的单位内部区域。

3.13

非限制区 non-restricted area

正常情况下不受出入限制的单位内部区域。

3.14

周界 perimeter

单位的区域边界。

3.15

治安保卫重点部位 important security and defense sections

位于治安保卫重点单位内部，对本单位生产、科研、经营、管理等活动起着关键作用和有着重要影响，需要实施重点保护的部位。

3.16

危险物品 dangerous goods

指具有易燃易爆、放射性、毒害性、传染性、杀伤性等特性，能够危及单位内部安全的物品，包括爆炸性物品、易燃性物品、放射性物品、毒害性物品、腐蚀性物品、传染病病原体、枪支弹药等。

3.17

最小应急单元 minimum emergency unit

单位组建的具备独立先期处置突发安全事件能力，由固定人员和标准装备构成的最小应急实体。

3.18

常态防范 regular protection

运用人力防范、实体防范、电子防范等多种手段和措施，常规性预防、延迟、阻止发生案事件的管理行为。

3.19

非常态防范 unusual protection

在重大会议、重大活动等重要时段以及获得涉暴恐、群体性事件、刑事治安警情等安全风险预警信息或发生上述案事件时，临时性加强防范手段和措施，提升安全防范能力的管理行为。

4 总体要求

4.1 一般要求

4.1.1 根据单位内部安全防范工作要求的不同，单位分为重点单位和一般单位。重点单位由区级以上公安机关根据相关法律法规确定，未列入重点单位的其他单位是一般单位。

4.1.2 单位内部安全防范分为常态防范和非常态防范。

4.1.3 单位是其内部安全防范工作的责任主体。单位应建立并落实治安保卫工作责任制，单位主要负责人是单位内部治安保卫工作第一责任人，对本单位内部治安保卫工作全面负责；单位其他责任人员对职责范围内的单位内部治安保卫工作负责。

4.1.4 单位安全防范工作应遵循预防为主的原则，建立健全安全防范风险评估预警工作机制，从源头预防风险案事件的发生，并与公安机关建立联防、联动工作机制。

4.1.5 单位应定期开展综合、全面的安全防范风险评估工作，宜参考附录 A 的要求开展，并根据评估结果落实各项安全防范措施。

4.1.6 单位应将安全防范工作纳入单位工作计划，保障内部安全防范工作必需的经费和装备。重点单位应建立内部安全防范工作专项经费保障制度，将内部安全防范涉及费用纳入预算、成本。

4.1.7 单位应建立健全内部安全防范工作档案。

4.1.8 单位应加强内部安全防范工作信息化、智能化建设，加强与公安机关等有关部门的数据共享。

4.1.9 单位应重视非常态防范，并根据公安机关、有关部门要求或实际工作需要及现实危害程度进入非常态防范状态。

4.1.10 单位应履行安全管理职责，落实网络安全、数据安全和个人信息保护义务。

4.1.11 单位内部安全防范工作除应满足本文件要求，还应满足相关国家标准、行业标准的规定。

4.1.12 重点单位应落实快速反应机制，建立“最小应急单元”，并在公安机关指导下加强人员选拔、培训、装备配备、演练等工作。

4.1.13 重点单位应针对外部监督和内部检查中发现的问题进行分析，制定纠正、整改措施并有效落实。

4.2 人员要求

4.2.1 单位的内部人员应熟悉单位内部安全防范管理制度、流程，并定期接受安全防范教育培训，提高个人安全防范意识。

4.2.2 单位应设置治安保卫机构或配备专（兼）职治安保卫人员。重点单位应设置与内部安全防范工作相适应的治安保卫机构，配备专职治安保卫人员，并将治安保卫机构设置和人员配备情况报公安机关备案。重点单位的治安保卫管理人员的数量应符合公安机关和行业主管部门的要求。

4.2.3 单位的治安保卫人员应满足内部安全防范工作需求，并接受有关法律法规知识和治安保卫业务、技能以及相关专业知识的培训、考核。

4.2.4 单位的治安保卫管理人员应熟悉相关国家法律法规，全面掌握本单位内部安全防范工作内容，具备安全防范专业知识和技能，并定期接受相应的教育培训。

4.2.5 单位内部安全防范管理工作职责应按照附录 B 的要求执行。

4.2.6 单位内其他机构（部门）应根据工作实际履行单位内部安全防范职责。

4.2.7 单位聘请的保安服务组织应符合安保主体准入限制和国家保密管理的相关规定。

4.2.8 重点单位应根据风险评估情况，确定本单位的安全防范重要岗位。

4.2.9 重点单位应建立安全防范重要岗位人员甄选流程，并符合公安机关和行业主管部门有关规定。

4.3 制度要求

4.3.1 单位应建立与单位实际情况相适应的内部安全防范制度，制度应符合相关法律法规、规章、行政规范性文件的规定。

4.3.2 单位内部安全防范制度应按照附录 C 的要求执行。

4.3.3 重点单位应建立内部安全防范工作档案，对内部安全防范工作的机构设置、管理制度、监督检查等内容进行收集、整理。

4.3.4 重点单位的内部安全防范工作档案应包括单位基本情况、单位保卫责任制情况、重要岗位人员、重点部位和区域确认、内部安全防范制度、安全风险评估、安全防范措施情况、安全防范工程检验报告、安全防范系统效能评估、内部人员教育培训与奖惩记录、应急预案与演练记录、单位内部案事件记录等。

4.3.5 重点单位宜建立安全防范工作与生产经营管理等相结合的共享联动制度。

4.4 应急要求

4.4.1 单位应当建立由本单位主要领导负责、专职保卫人员分工、专兼职相结合的应急管理指挥体系和应急救援队伍。加强应急救援资金、物资的管理。

4.4.2 单位应结合自身特点，分级分类制定应急预案，应急预案应明确应急响应责任人、风险隐患监测、主要任务、信息报告、预警和应急响应、应急处置措施、人员避险疏散转移、应急资源调用等内容。

4.4.3 单位应定期开展应急演练，并做好事前方案制定、事中组织引导、事后总结点评。

4.4.4 单位应结合自身特点和应急能力，增加应急力量、强化安全防范措施，保障单位安全正常运行。

4.4.5 单位发生突发案事件，相应的治安保卫管理人员及最小应急单元应第一时间到达现场，采取必要的先期处置和救援措施，防止事件扩大升级，并积极配合公安机关进行处置。

4.5 建设要求

4.5.1 单位内部安全防范系统建设应纳入单位总体规划，新建、改建、扩建项目应与单位同步规划，宜同步建设、同步验收、同步运行。

4.5.2 重点单位的安全防范工程应进行工程检验。工程检验应由具有安全防范工程检验资质且检验能力在资质能力授权范围内的检验机构实施。

4.5.3 单位内部安全防范工程竣工移交后应开展安全防范系统的运行与维护工作，并符合 DB11/T 855 的规定。

4.5.4 重点单位应定期对安全防范系统的安全防范效能进行评估，建设管理、运行维护相关单位应根据评估意见进行改进。

4.5.5 重点单位的安全防范系统应明确安全保护等级，采取 GB/T 22239 中相应安全保护等级的防护措施。

5 常态防范要求

5.1 一般要求

5.1.1 多个单位处于同一周界内或共用同一建（构）筑物时，应明确各单位安全防范空间边界和治安保卫工作责任；应根据单位隶属关系或场地公用设施日常管理实际，确定一家单位作为牵头单位，负责统筹该场地安全防范管理工作。

5.1.2 多家单位共用周界、建（构）筑物出入口时，出入口各使用单位应明确访问控制负责人，负责管理本单位人员及访客的出入授权；宜确定出入口管理单位作为牵头单位，负责执行出入口管理工作。

5.1.3 单位宜根据治安保卫需求，参考重点单位对重点部位和区域的确定方法，确定单位内部安全防范的重点部位和区域。

5.1.4 人员密集区域的安全防范应符合 GB/T 40248、GB 51309 的防火和应急疏散相关标准要求。

5.1.5 涉及公共安全、个人隐私和个人信息的视频图像信息应采取严格保护措施。位于军事禁区、军事管理区以及涉密单位周边的单位，在安全防范设施设置前应当事先征得相关涉密单位的同意。

5.1.6 信息中心、数据中心应按照 GB 9361、GB 50174、GB/T 22239 安全物理环境的有关要求，采取安全防范措施。

5.1.7 枪支（弹药）库室应符合 GA 1016 的相关规定。

5.1.8 危险化学品仓库应符合 GB 15603 的相关规定。

5.1.9 易制爆危险化学品储存场所应符合 GA 1511 的相关规定。

5.1.10 剧毒化学品、放射源存放场应符合 GA 1002 的相关规定。

5.1.11 一般单位常态防范设施配置应符合附录 D 的规定。

5.2 人力防范要求

5.2.1 单位应配备专（兼）职治安保卫人员，宜配备必要的治安保卫防护装备。

5.2.2 治安保卫人员应对访客、车辆进行出入管理。

5.2.3 治安保卫人员应定期对单位内部进行巡视，维护单位内部治安秩序。

5.2.4 发生突发案事件时，单位应根据现场情况，采取制止、延阻、人员避险疏散等措施降低危害后果；涉嫌违法犯罪的应立即报警，并采取措施保护现场。

5.3 实体防范要求

5.3.1 单位周界宜设置实体屏障。

5.3.2 单位周界车辆出入口、人员密集部位周边宜设置车辆减速和防冲撞设施。

5.3.3 与外部相邻的建（构）筑物门窗应具有防撬、防砸、防拆卸等防护能力。

5.3.4 重要物品及其存放区域应根据防护需要合理设置实体防护装置。

5.4 电子防范要求

5.4.1 以下部位和区域应设置视频图像采集装置：

- a) 周界主要出入口；
- b) 机动车停车场（库）出入口；
- c) 对社会公共开放区域；
- d) 人员密集区域；
- e) 其他经评估需要防护的部位和区域。

5.4.2 以下部位和区域宜设置视频图像采集装置：

- a) 单位周界；
- b) 单位内部主要道路；
- c) 建（构）筑物内主要通道；
- d) 电梯轿厢、电梯厅；
- e) 非机动车集中停放处。

5.4.3 以下部位和区域宜设置紧急报警装置：

- a) 门卫室（传达室）；
- b) 安防监控中心（室）；
- c) 易发生安全威胁事件的区域；
- d) 其他经评估需要防护的部位和区域。

5.4.4 以下部位和区域宜设置出入口控制装置：

- a) 周界、建（构）筑物主要出入口；
- b) 集中存放重要物品的部位；
- c) 其他经评估需要防护的部位和区域。

5.4.5 单位周界车辆出入口宜设置机动车识别装置。

6 重点单位防范要求

6.1 重点单位类别

下列单位确定为安全防范的重点单位：

- a) 党政机关、社会团体；
- b) 广播电台、电视台、通讯社等重要新闻单位；
- c) 国防科技工业重要产品的科研、生产、存储、试验单位；
- d) 大型能源动力、水利设施运营单位，城市水、电、油、气、热力等生产、输送、供应单位；
- e) 银行、保险、证券等金融单位；
- f) 重要教育、科研、医疗单位；
- g) 重要博物馆、档案馆、图书馆、展览馆和文物保护单位；
- h) 重要物资储备单位；
- i) 通信、邮政单位；
- j) 大型文化、体育场所和商贸中心；
- k) 研制、生产、销售、存储危险物品或者实验、保藏传染性菌种、毒种的单位；
- l) 国家重点建设工程单位；
- m) 重要高新技术领域企业；
- n) 其他需要列为治安保卫重点的单位。

6.2 重点部位和区域

6.2.1 重点部位

下列部位确定为重点单位安全防范的重点部位：

- a) 涉密部位：单位内部涉及国家秘密、单位重要商业秘密或者其他内部重要事项的部位，如档案室、机要室、文件库、涉密物品存放地等；
- b) 关键决策部位：单位指挥调度、首脑决策、规划、设计部位，如：核心人员办公区、指令调度室、计算机网络中心、业务监控中心等；
- c) 关键生产部位：对单位业务活动起关键作用，一旦发生事故或遭受破坏，会使单位生产、科研等活动瘫痪或者局部瘫痪或者将使其生产的产品产量受到影响的部位，如研发中心、实验室、金融单位的数据处理中心、工厂的总装车间等；
- d) 危险物品部位：生产、使用、保管易燃、易爆、剧毒、放射性化学危险物品、毒害、传染类物品部位，以及存放枪支、弹药和管制刀具等物品的部位，如危险化学品储存仓库等；
- e) 供给保障部位：确保单位业务活动正常运转而所必需的后勤保障供给部位，如内部变（配）电站、热力锅炉房、热力泵房、暖通空调机房、可燃气体泵房、水源泵房、油库、加油站等；
- f) 重要设备部位：贵重、稀有、关键设备所在部位，即经济价值高、国内稀有或在生产科研活动中起决定作用的机器、仪器等设备所在部位；
- g) 财物集中部位：单位内部集中储存钱财物资的部位，如各单位内部掌管钱款票证的财务部门；工厂的重要原材料库和成品、半成品库；商业部门的物资仓库；金融机构的金库；文博单位的展厅、展室、文物库房等；
- h) 承担安全保卫任务的部位，如值班室、门卫室（传达室）、安防监控中心（室）、安保设备存放处等；
- i) 其他经评估应重点防范的部位。

6.2.2 重点区域

下列区域确定为重点单位安全防范的重点区域：

- a) 周界
- b) 周界出入口；
- c) 重点部位所在建（构）筑物；
- d) 人员密集区域：单位内部人员集中或者人员流动性大的部位，如业务大厅、礼堂、图书馆、教室、操场、售票窗口等；
- e) 其他经评估应重点防范的区域。

6.3 风险等级和防范级别

6.3.1 重点单位的安全风险等级由公安机关会同行业主管部门确定，重点单位安全风险等级分为三级，按风险由小到大定义为三级风险、二级风险、一级风险。

6.3.2 重点单位的防范级别分为三级，由低到高分别是三级防范、二级防范、一级防范，防范级别应与单位的风险等级相适应。

6.3.3 常态三级防范要求为重点单位应达到的最低标准，常态二级防范要求应在常态三级防范要求基础上执行，常态一级防范要求应在常态二级防范要求基础上执行。

6.4 一般要求

6.4.1 重点单位的一般要求应在 5.1 的要求基础上执行。

6.4.2 重点单位应根据治安保卫需求以及公安机关或行业主管部门的相关要求，参照 6.2 的确定方法，识别确定单位内部安全防范的重点部位和区域，并确定重点部位和区域的责任部门。

6.4.3 重点单位应针对需要防范的具体风险，对重点部位和区域进行有效的防护设计。

6.4.4 重点单位应综合运用人力防范、实体防范、电子防范等手段科学规划、合理设计，建设安全、可靠、有效的安全防范系统。

6.4.5 重点单位应根据重点部位和区域的风险不同，合理选择具备相应防范能力的安全防范设施，具备预防、延迟、阻止相关威胁事件的能力。

6.4.6 重点单位应根据单位面向公众开放情况，将单位划分为限制区和非限制区。

6.4.7 重点单位应按照周界、缓冲区域、重点部位和区域的纵深防护原则，对限制区采取逐层深入的防范措施，建立整体与局部相结合的纵深防护体系，对非限制区的防护应参考附录 E 的要求执行。

6.4.8 重点单位使用一般单位部分场地办公时，应对相关的公用设施、共用场地进行安全评估，并对本单位工作场地独立分区，加强信息保密、隔离等安全防范措施。

6.4.9 重点单位应配备满足防范管理、值守巡逻、应急处置、系统运维等需要的治安保卫人员，并应满足以下要求：

- a) 治安保卫人员应身心健康、品行良好，无刑事犯罪记录、无社区戒毒或强制隔离戒毒记录的中华人民共和国公民；
- b) 治安保卫管理人員和从事巡逻、值守、安检、值机等具体工作的单位人员应达到相应国家保卫管理员专业能力；
- c) 安检、值机等专业性強的人员应通过专业培训。

6.4.10 重点单位应制定重点部位和区域的人员、交通工具访问控制程序，并根据安全管理需要，对非授权出入风险设置相应的防范措施。访客、机动车登记记录保存期限不少于 180d。

6.4.11 访客进入重点单位的重点部位时，应有单位内部人员陪同。

6.4.12 重点单位应制定重点部位和区域的重要物品仓储盘点、出入控制等程序，并根据安全管理需要，确定禁限带物品、单位管控物资等物品清单，设置相应的防范措施。

6.4.13 重点单位应根据安全管理需要，并满足行业要求，对通行人员、物品、交通工具进行安全检查。

6.4.14 重点单位发生危险物品丢失时，应依照预案采取处置措施、做好相关记录，并向公安机关和行业主管部门报告。

6.4.15 重点单位应设置安防监控中心（室），并符合 GB 50348 的规定。

6.4.16 重点单位常态防范设施配置应符合附录 F 的规定。

6.5 三级防范要求

6.5.1 人力防范要求

6.5.1.1 应配备符合单位安保需求的治安保卫人员，其中专职治安保卫管理人员不低于单位总人数的 2%，保卫执勤人员应配备棍棒、钢叉、防暴盾牌、头盔、防刺背心等防护装备及对讲机等通信工具。

6.5.1.2 治安保卫人员每年至少组织 1 次安全防范教育培训和 1 次应急预案演练。

6.5.1.3 周界主要出入口应配置保卫执勤人员值守，对出入人员、通行车辆进行审核、登记。其他出入口在开启时应有人值守。

6.5.1.4 保卫执勤人员应定期对重点部位和区域巡逻，周期间隔应不大于 24h，巡逻人数不少于 2 人。

6.5.1.5 人员、车辆高峰时期的主要路口（路段）、人员密集区域等重点区域，应配置保卫执勤人员。

6.5.1.6 重点部位所在建（构）筑物的主要出入口和应急出入口开启时，宜有保卫执勤人员值守，核验进入人员身份，登记、检查携带物品。

6.5.2 实体防范要求

6.5.2.1 单位周界应设置不间断实体屏障，其外侧无可供攀爬的物体或设施，高度不低于 2.2m（含防攀爬设施）。

6.5.2.2 单位周界应设置“未经允许禁止入内”等警示标志；宜设置满足巡查、警戒、视频图像采集需求的照明装置。

6.5.2.3 穿越周界的河道、涵洞等地下空间应采取实体封堵等防护设施。

6.5.2.4 周界主要出入口应满足以下要求：

- a) 设置防车辆冲撞设施；
- b) 分别设置人员、车辆出入口；
- c) 人员出入口设置人行通道闸，防止尾随进入；
- d) 车辆出入口设置车辆减速限速装置；
- e) 出入口位置避免直对单位内部的重点部位；
- f) 配备防爆毯等安全处置设施。

6.5.2.5 通向重点部位和人员密集区域的道路，应设置减速降速设施。

6.5.2.6 室外人员密集区域周边应设置防车辆冲撞设施。

6.5.2.7 重点部位所在建（构）筑物应采取相应的实体防护设施，并满足以下要求：

- a) 外立面、窗户具有防攀爬、防盗措施；
- b) 无人值守出入口设置防盗安全门；
- c) 应急疏散出入口具有紧急开启功能；
- d) 直通室外的通道、管口等设置实体防护设施。

6.5.2.8 重点部位应根据具体用途，合理选择设置防盗、防砸的防护设施。

6.5.2.9 信访接待场所应设置在限制区外。

6.5.3 电子防范要求

6.5.3.1 单位周界应设置视频图像采集装置，宜设置入侵探测装置和电子巡查装置，并满足以下要求：

- a) 视频监视和回放图像应能清晰显示周界区域人员活动情况，宜具有智能视频分析功能，可对区域内入侵等行为检测、识别、报警；
- b) 电子巡查装置应沿周界巡逻路线设置，巡查点宜在视频图像采集范围内；
- c) 周界入侵探测不应存在盲区。

6.5.3.2 周界主要出入口应设置视频图像采集装置和车辆出入控制装置，视频监视及回放图像应能清晰显示出入人员的面部及体貌特征，能对进出车辆号牌、颜色等进行识别、比对、放行。

6.5.3.3 信访接待场所应设置视频图像采集、紧急报警、声音采集、有线/无线通信等装置。监视及回放图像应能清晰显示出入人员面部和携带物品特征。

6.5.3.4 单位内部主要道路、高风险车辆行驶路线、人员密集区域和室外重要部位应设置视频图像采集装置，监视及回放图像应能清晰显示人员、车辆活动情况。

6.5.3.5 单位内部易发生安全威胁事件的区域应设置紧急报警装置。

6.5.3.6 机动车停车场（库）出入口应设置视频图像采集装置和电子巡查等装置，监视及回放图像应能清晰显示出入车辆的颜色、号牌等信息；宜设置停车场（库）安全管理装置，对出入车辆进行验证和控制。

6.5.3.7 非机动车集中存放处应设置视频图像采集装置和电子巡查等装置，监视及回放图像应能清晰显示人员活动情况。

6.5.3.8 重点部位所在的建（构）筑物设置电子防护设施，并满足以下要求：

- a) 出入口、大厅、主要通道、楼顶、电梯轿厢、电梯厅、楼梯间应设置视频图像采集装置，视频监视和回放图像应能清晰显示人员体貌特征，其中车辆出入口的视频监视和回放图像应能清晰显示车辆颜色和号牌；
- b) 多个单位共用同一建（构）筑物时，应根据管理边界设置出入口控制装置；
- c) 无人值守出入口宜设置入侵探测装置；
- d) 重点部位所在楼层宜设置出入口控制装置。

6.5.3.9 重点部位应根据安全防范需要合理设置电子防护设施，并满足以下要求：

- a) 应设置电子巡查装置；
- b) 其出入口应设置视频图像采集装置，宜设置出入口控制装置；
- c) 其内部主要通道应设置视频图像采集装置；
- d) 其内部宜设置入侵探测装置。

6.6 二级防范要求

6.6.1 人力防范要求

6.6.1.1 应配备符合单位安保需求的治安保卫人员，其中专职治安保卫管理人员不低于单位总人数的3‰。

6.6.1.2 治安保卫人员每半年至少组织 1 次安全防范教育培训和 1 次应急预案演练。

6.6.1.3 保卫执勤人员定期巡逻的周期间隔应不大于 12h。

6.6.1.4 周界主要出入口应设置独立的门卫室（传达室），配置保卫执勤人员值守，核验进入人员身份，登记或检查携带物品。单位运营时段值守数量不少于 2 人。

6.6.1.5 主要路口（路段）、人员密集区域等重点区域，应配置保卫执勤人员。

6.6.1.6 重点部位所在建（构）筑物的主要出入口和应急出入口开启时，应有保卫执勤人员值守。

6.6.1.7 安防监控中心（室）值机人员应定期利用安全防范系统进行电子巡查，发现异常情况时，记录并及时报告。

6.6.1.8 重点部位应有专人负责出入人员身份、携带物品核验；保密性强或危险性大的重点部位，还应采取双人验证或异地复核方式对出入进行授权管理。发生异常事件和突发情况时应及时报告。

6.6.2 实体防范要求

6.6.2.1 周界实体屏障其外侧高度应不低于 2.5m（含防攀爬设施）。

6.6.2.2 周界主要出入口应设置安检区。

6.6.2.3 门卫室（传达室）与外界相通的窗户应安装金属防护窗或符合 GA 844 要求的防砸透明玻璃，与外界相通的出入口应设置防盗安全等级不低于 GB 17565-2022 中 3 级要求的防盗安全门。

6.6.2.4 重点部位所在的建（构）筑物应设置实体防护设施，并满足以下要求：

- a) 当建（构）筑物的室外空气进气口低于 2.5m 时，设置安全隔离设施；
- b) 无人值守出入口设置具有自动锁闭功能的防盗安全门。

6.6.3 电子防范要求

6.6.3.1 周界应设置入侵报警探测装置和电子巡查装置，巡查点应在视频图像采集范围内。

6.6.3.2 周界主要出入口应设置出入口控制装置，对出入人员进行验证和控制。应设置手持式金属探测器或通过式金属探测门等安全检查装置。

6.6.3.3 门卫室（传达室）设置电子防护设施，并满足以下要求：

- a) 应设置紧急报警、视频图像采集、有线/无线通信等装置，视频监视和回放图像应能清晰显示室内人员活动情况；
- b) 应能实时显示周界（含出入口）的视频图像、接收显示周界入侵报警信息；
- c) 应能显示车辆识别比对结果，能够手动控制放行车辆；
- d) 根据安全管理需要宜设置符合 GB 12899 要求的手持式金属探测器等安全检查装置，对来访人员及携带物品进行安全检查。

6.6.3.4 重点部位所在的建（构）筑物应设置电子防护设施，并满足以下要求：

- a) 建（构）筑物周边、无人值守的出入口设置入侵探测装置；
- b) 保卫执勤岗设置视频图像采集装置，视频监视和回放图像能清晰显示值班活动情况；
- c) 重点部位所在楼层设置出入口控制装置，并具有梯控功能。

6.6.3.5 重点部位出入口应设置出入口控制装置，宜具有防尾随、防反传功能。

6.6.3.6 重点部位内部应设置入侵探测装置。

6.7 一级防范要求

6.7.1 人力防范要求

6.7.1.1 应设置独立的治安保卫机构。

6.7.1.2 周界主要出入口应配置不少于 2 名保卫执勤人员 24h 值守，宜对通行车辆进行安全检查。

6.7.1.3 保卫执勤人员定期巡逻的周期间隔应不大于 6h。

6.7.1.4 建（构）筑物内重点部位楼层宜有保卫执勤人员值守，核心生产区、工艺区等重点部位应 24h 值守。

6.7.1.5 安防监控中心(室)应有值机人员 24h 在岗值守, 每班不少于 2 人。

6.7.2 实体防范要求

6.7.2.1 周界实体屏障内、外侧高度应不低于 2.5m (含防攀爬设施), 实体屏障两侧无可供攀爬的物体或设施。

6.7.2.2 周界易发生误侵入位置, 宜设置广播警示装置, 对该区域进行警告驱离。

6.7.2.3 应设置独立的外来车辆停放区、寄递物品处理区, 并远离重点部位。

6.7.2.4 室外重点部位和重点部位所在的建(构)筑物周边应设置实体屏障。

6.7.3 电子防范要求

6.7.3.1 重点部位和区域设置的视频图像采集装置宜符合 GB/T 25724 的规定。

6.7.3.2 应设置安全防范管理平台。

6.7.3.3 周界主要出入口应设置具有人员身份识别的出入口控制装置, 宜设置车底成像或乘用车辆 X 射线等安全检查装置。

6.7.3.4 单位内部制高点宜设置视频图像采集装置, 视频监视和回放图像应清晰显示区域内人员活动和车辆行驶情况。

6.7.3.5 重点部位所在的建(构)筑物设置电子防护设施, 并满足以下要求:

- a) 人员、车辆通道应设置出入口控制装置, 宜具有防尾随、防反传功能;
- b) 保卫执勤岗应设置紧急报警装置;
- c) 重点部位所在楼层应设置出入口控制装置。

6.7.3.6 重点部位出入口应设置安检区, 并设置符合 GB 12899 要求的手持式金属探测器等安全检查装置, 对来访人员及携带物品进行安全检查。

7 非常态防范要求

7.1 人力防范

7.1.1 单位应根据事态发展情势, 启动应急响应机制, 组织开展动员, 单位负责人或其授权人员应 24h 带班组织防范工作, 在常态防范的基础上加强保卫力量。

7.1.2 单位应设置警戒区域, 限制人员、交通工具进出, 应加强对周界出入口的人员、交通工具及所携带物品的安全检查, 应对人员携带的物品进行开包检查。

7.1.3 单位应加强重点部位和区域的执勤巡逻, 缩短巡逻周期间隔。

7.2 实体防范

7.2.1 应关闭部分周界出入口, 减少周界出入口的开放数量。

7.2.2 周界主要出入口的车辆阻挡装置应设置为阻截状态。

7.2.3 应加强重点部位和区域的防护器具、救援器材、应急物资以及门、窗、锁、车辆阻挡装置等实体防范设施的有效性检查。

7.3 电子防范

7.3.1 应加强电子防范设施、通信设备的检查和维护，确保安全防范系统正常运行及通信设备的正常使用。

8 系统技术要求

8.1 基本要求

8.1.1 安全防范系统使用的设备和材料应符合相关标准并检验或认证合格。

8.1.2 系统应具有权限管理功能和网络安全防护措施，各子系统宜有效集成并集中管理。

8.1.3 系统内具有计时功能的设备应进行校时，设备的时钟与北京时间误差应不大于 5s。

8.1.4 系统和设备登录密码不应为弱口令，不应存在网络安全漏洞和隐患。当基于不同传输网络的系统和设备联网时，应采取相应的安全管理措施。

8.1.5 系统的其他要求应符合 GB 55029 的相关规定。

8.2 入侵和紧急报警系统

8.2.1 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，监控中心（室）应能有声、光指示，准确指示发出报警的位置。

8.2.2 紧急报警信号应根据行业实际要求接入属地公安机关、上级主管部门。

8.2.3 系统应具备防拆、开路、短路报警功能。

8.2.4 系统应具备自检功能和故障报警、断电报警功能。

8.2.5 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。

8.2.6 系统布防、撤防、故障和报警信息存储时间应不少于 90d。

8.2.7 系统的其他要求应符合 GB/T 32581 的相关规定。

8.3 视频监控系统

8.3.1 视频图像信息应实时记录，存储时间应不少于 30d，反恐重点目标存储时间应不少于 90d。

8.3.2 系统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 25fps。

8.3.3 系统应能与入侵和紧急报警系统、出入口控制系统联动。

8.3.4 重点目标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。

8.3.5 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。视频监控联网信息传输、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。

8.4 出入口控制系统

8.4.1 出入口控制系统应能对强制开启、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。

8.4.2 系统应满足人员逃生疏散时的相关要求，当需要紧急疏散时，各闭锁通道应开启，保障人员迅速安全通过。

8.4.3 系统的操作、故障、配置、通行等信息存储时间应不少于 180d。

8.4.4 系统的其他要求应符合 GB/T 37078 的相关规定。

8.5 电子巡查系统

8.5.1 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。

8.5.2 系统巡查记录保存时间应不少于 90d。

8.5.3 系统的其他要求应符合 GA/T 644 的相关规定

8.6 停车库（场）安全管理系统

8.6.1 停车库（场）安全管理系统应具有驾驶员面部抓拍功能的，应能在同一界面同时显示出入车辆号牌和驾驶员的面部抓拍图像。

8.6.2 系统应具有出入车辆信息、日志等的记录和管理功能。

8.6.3 系统应具有对无牌车辆的出入授权功能。

8.6.4 系统应具有防止非授权钥匙遥控开启功能。

8.6.5 系统的其他要求应符合 GA/T 761 的相关规定。

8.7 安全检查系统

8.7.1 微剂量 X 射线安全检查设备应符合 GB 15208.1 和 GB 15208.2 的相关规定。

8.7.2 通过式金属探测门、手持式金属探测器应分别符合 GB 15210、GB 12899 的相关规定。

8.7.3 车底成像安全检查系统、乘用车辆 X 射线安全检查系统应分别符合 GA/T 1336、GA/T 1731 的相关要求。

8.7.4 液态危险化学品安全检查仪应符合 GB/T 41483 的相关规定。

8.7.5 防爆毯应符合 GA 69 的相关规定。

8.7.6 防爆球应符合 GA 872 的要求。

8.8 实体防护系统

8.8.1 车辆电动栏杆机应符合 GA/T 1132 的要求。

8.8.2 防机动车冲撞或隔离设施应符合北京市相关文件要求。

8.8.3 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。

8.8.4 警示标志应符合 GB/T 2893.5 的要求。

8.8.5 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。

8.8.6 应急照明应符合 GB 17945 的要求。

8.9 安全防范管理平台

8.9.1 安全防范管理平台应具有集成管理、信息管理、用户权限管理、存储管理、检索与回放、设备管理、联动控制、日志管理、系统校时等功能。

8.9.2 平台的故障不应影响各子系统的正常运行。某一系统的故障不应影响安全防范管理平台和其他系统的正常运行。

8.9.3 平台的人员角色分级授权管理功能应具有严格限定信息的访问、下载权限和使用范围，对人员操作过程进行记录并采取技术措施确保记录不可修改、删除。

8.9.4 平台应预留与有关部门信息化系统联网的接口，宜预留与物业管理等信息化系统联网的接口。

8.9.5 平台通过互联网传输人员和车辆等信息,应通过国家相关机构检测认证的密码算法对信息进行加密;通过专用传输网络传输信息时，应符合有关部门关于专用传输网络的网络安全规定和安全技术要求。

8.9.6 平台的其它功能应符合 GB 50348 的规定。

9 监督检查要求

9.1 内部检查

9.1.1 单位内部检查应包括安全巡查和治安保卫安全检查。

9.1.2 单位应定期对内部治安隐患开展安全巡查，及时发现可能导致治安案件、刑事案件、治安灾害事故发生或产生严重后果的隐患。重点单位应每日开展至少 1 次安全巡查。

9.1.3 单位应定期对单位管理制度、防范措施的适用性和落实情况开展治安保卫安全检查，全面排查深层次、系统性隐患。重点单位应每季度开展至少 1 次治安保卫安全检查，安全检查内容应包括附录 G 的内容。

9.1.4 重点单位在以下情况时，应及时组织开展治安保卫安全检查：

- a) 单位保卫责任制发生重大变化时；
- b) 治安保卫机构或治安保卫管理人员发生重大调整时；
- c) 确定、变更本单位重点部位或修改相关内部安全防范制度后的 15d 内；
- d) 进入或可能进入非常态防范状态前；
- e) 出现恶劣天气时；
- f) 其他可能对现有安全防范措施造成重大影响时。

9.1.5 单位应制定内部安全检查表，检查结果和治安隐患整改记录应定档留存。

9.1.6 单位应鼓励内部人员积极发现内部治安隐患，并向单位治安保卫机构或治安保卫人员报告。

9.1.7 重点单位应针对外部监督和内部检查中发现的问题进行分析，制定纠正、整改措施并有效落实。整改期间应当采取有效的防范措施。由于客观原因致使治安隐患整改情况难以达到规定要求，并严重威胁公民人身安全、公私财产安全或者公共安全的，应及时向上一级主管部门或公安机关报告。

9.2 外部监督

- 9.2.1 单位应接受公安机关、行业主管部门定期、不定期地对单位保卫制度、人力防范、实体防范、电子防范等安全防范工作情况的指导、监督。
- 9.2.2 单位应接受公安机关、行业主管部门定期、不定期地对单位内部治安突发事件处置预案及组织演练情况进行的指导、监督。
- 9.2.3 重点单位应接受公安机关、行业主管部门定期、不定期地对单位保卫责任制、治安保卫机构设置和人员配备报主管公安机关备案、重点部位确定、重要岗位甄选、治安隐患排查、整改等情况进行的指导、监督。
- 9.2.4 重点单位应接受公安机关、行业主管部门定期、不定期地对单位重点部位和区域实施重点保护情况进行的指导、监督。

附录 A
(资料性)
风险评估程序

A.1 风险识别

A.1.1 识别目的：以保护单位内部人员和重点部位安全为核心，识别本单位所面临的潜在安全威胁行为。

A.1.2 识别方式：通过现场观察、交流访谈、事件记录等多种方式开展识别工作。

A.1.3 潜在威胁行为类型（含内部威胁、外部威胁）：非法侵入、盗窃、窃密、蓄意破坏、群体性事件、暴力袭击、邮寄/放置可疑物品、诈骗、威胁恐吓等。

A.1.4 重点隐患识别：

- a) 重点部位和区域隐患：结合各重点部位特性识别隐患，如涉密部位的失泄密隐患、人员密集区域的聚集踩踏隐患、关键生产部位的内部威胁破坏隐患、财物集中部位的盗窃隐患等；
- b) 周边治安环境隐患：重点识别与公共安保力量缺乏联动机制、周边治安秩序存在风险等隐患。

A.2 风险分析

A.2.1 分析基础：在明确潜在威胁的具体类型、实施手段及实施能力的前提下，开展综合分析工作。

A.2.2 分析要素：综合考察以下关键要素，为风险等级划分提供依据：

- a) 根据单位的重要性、内部资产价值、涉密程度、重点部位数量；
- b) 根据单位面临威胁的可能性与紧迫性；
- c) 根据发生治安风险事件后对国家、社会 and 单位的影响程度；
- d) 根据单位所处地理位置环境、单位内部人数、作业面积、周边社会治安状况。

A.3 风险评价

A.3.1 评价指标：遵循国家相关法律法规、行业领域风险评估规范，对威胁发生可能性指标、影响程度指标、防控有效性指标进行定性或定量评价。

A.3.2 风险等级划分：可采用后果/可能性矩阵评估法，将单位安全风险划分为高、中、低三个等级，举例如下：

- a) 低风险（三级风险）：威胁发生可能性低，发生后仅造成轻微损失或局部影响，现有防控措施可完全管控；
- b) 中风险（二级风险）：威胁发生可能性中等，发生后将造成一定人员伤亡、财产损失或较大范围社会影响，现有防控措施需进一步强化方可有效管控；
- c) 高风险（一级风险）：威胁发生可能性高，且一旦发生将造成重大人员伤亡、巨额财产损失、核心涉密信息泄露或严重社会负面影响，现有防控措施难以有效遏制。

A.4 风险应对

A.4.1 风险承受度：结合国家法律法规及行业标准要求，设定风险承受度阈值，确保设定结果合法合规、贴合单位实际运营需求。

A. 4. 2 单位根据所面临的威胁、风险承受度及风险等级，确定防范对象及其手段和能力。

附录 B

(规范性)

单位内部安全防范管理工作职责

B.1 治安保卫机构与治安保卫管理人员的主要职责包括但不限于：

- a) 依法、文明履行职责，符合相关法律法规的禁止从业要求；
- b) 制定并组织落实本单位的内部治安保卫制度、工作计划及应急预案等；
- c) 评估单位安全风险，组织落实治安保卫措施，整改治安隐患；
- d) 监督检查单位安全防范设施的建设、使用、管理和维护；
- e) 管理单位自建护卫力量、保安员、群防群治组织等安保力量。
- f) 组织开展治安防范宣传、法治教育；
- g) 维护单位内部的治安秩序，制止发生在本单位的违法行为，发生的治安案件、涉嫌刑事犯罪案件立即报警，并采取措施保护现场，配合公安机关的侦查、处置工作；
- h) 负责指导、监督、协调单位内各部门做好治安保卫工作。

附录 C
(规范性)
单位内部安全防范制度内容

C.1 单位内部安全防范制度包括但不限于：

- a) 保卫责任制：明确各级责任，保障人力、财力、物力投入；
- b) 保卫管理类制度：出入控制与访客管理要求，重点部位和区域安全管理要求，重要物品、危险物品使用、保管、储存、运输安全管理要求，单位内部重要活动管理要求，交通安全管理要求、安全检查要求等；
- c) 人员管理类制度：安全防范重点岗位认定、甄选要求，单位内部矛盾纠纷排查化解要求，单位人员执行保卫管理的考核及奖惩、问责要求等；
- d) 安全教育培训类制度：安全防范知识宣传教育、保卫管理制度培训等；
- e) 风险评估制度：定期开展安全风险评估情况等；
- f) 安全防范措施类制度：门卫、值班、巡查等人力防范管理要求，安全防范设施管理以及维护要求，定期开展安全防范效能评估情况等；
- g) 检查整改类制度：安全巡查、治安保卫安全检查要求，治安风险隐患整改要求等；
- h) 应急预案与演练制度：定期组织应急演练情况，单位内部发生治安事件、刑事案件的报告及先期处置要求，组织实施非常态措施要求等。

C.2 安全防范重点岗位认定依据：

- a) 对重点单位或重点部位和区域的安全管理具有决策、指挥或执行责任的岗位；
- b) 易发生案事件，会影响重点单位安全的岗位；
- c) 直接影响安全防范工作执行的岗位；
- d) 行业主管部门要求确定的岗位；
- e) 其他经评估需确定的岗位。

C.3 安全检查内容要点：

- a) 安检点在启动安检前检查设备状态、清点装备数量；交接班时填写工作记录；安检结束后关闭并清点设备，做好工作数据统计、汇总；
- b) 在安检区设置警示信息、禁带限带等标识牌，告知通行人员主动接受并配合安全检查；拒不接受安全检查的，单位有权拒绝其通行；
- c) 发现携带禁带物品的，依照预案采取人、物分离等处置措施，并立即报告公安机关；
- d) 发现携带限带物品的，安检人员拒绝其通行，对安检过程中自弃的上述物品，安检人员予以登记；
- e) 发现携带单位管控物资的，依照单位相关管理制度采取处置措施；
- f) 安全检查的其他要求符合 GA/T 1799 的相关规定。

附录 D
(规范性)
常态防范设施配置

D.1 常态防范设施配置应符合表 D.1 的规定。

表D.1 常态防范设施配置

序号	具体部位	防护设施		一般单位
1	单位周界	实体防护系统	实体屏障	宜
2		电子防护系统	视频图像采集装置	宜
3	周界主要出入口	电子防护系统	视频图像采集装置	应
4	周界、建（构）筑物主要出入口	电子防护系统	出入口控制装置	宜
5	单位周界车辆出入口	实体防护系统	车辆减速和防冲撞设施	宜
6		电子防护系统	机动车识别装置	宜
7	人员密集部位周边	实体防护系统	车辆减速和防冲撞设施	宜
8	与外部相邻的建（构）筑物门窗	实体防护系统	防撬、防砸、防拆卸等防护装置	宜
9	单位内部主要通道	电子防护系统	视频图像采集装置	宜
10	建（构）筑物内主要通道	电子防护系统	视频图像采集装置	宜
11	电梯轿厢、电梯厅	电子防护系统	视频图像采集装置	宜
12	机动车停车场（库）出入口	电子防护系统	视频图像采集装置	应
13	非机动车集中停放处	电子防护系统	视频图像采集装置	宜
14	人员密集区域	电子防护系统	视频图像采集装置	应
15	对社会公共开放区域	电子防护系统	视频图像采集装置	应
16	门卫室（传达室）	电子防护系统	紧急报警装置	宜
17	安防监控中心（室）	电子防护系统	紧急报警装置	宜
18	易发生安全威胁事件的区域	电子防护系统	紧急报警装置	宜
19	集中存放贵重物品部位	电子防护系统	出入口控制装置	宜
20	其他经评估需要防护的部位和区域	电子防护系统	视频图像采集装置	应
21		电子防护系统	出入口控制装置	宜
22		电子防护系统	紧急报警装置	宜

附录 E
(资料性)
重点单位非限制区防护

E.1 重点单位非限制区防护以预警、震慑与缓解、应急处置为主要手段，包括但不限于以下方式：

E.1.1 预警

- a) 常态开展矛盾排查，建立网络舆情预警机制，提前对可能影响现场安全的信息进行梳理，评估风险。
- b) 加强与属地公安机关的外联互动，及时掌握针对本单位的安全风险信息。
- c) 利用安全防范领域技术创新手段，分析人群行为，及早发现异常个体或群体；治安保卫人员对现场表现紧张或行为可疑者进行询问、核实。
- d) 对单位内部人员开展识别潜在威胁的专项培训，倡导“看到即报告”的安保原则；潜在威胁行为包括但不限于威胁人身安全、窥探窥视限制区、盗窃挪用单位物品、试探单位安全防范设施、活动范围超出限定区域、探听敏感信息、破坏损毁公用设施、发现可疑物/无主物、无人航空器“黑飞”等情况；商贸零售类单位开展针对高风险商品的可疑购买行为的识别培训。
- e) 建立跨区域的可疑人员及车辆档案系统以核查特定人员或车辆是否在不同场所被重复识别。

E.1.2 威慑与缓解

- a) 增加区域内着装安保巡逻力量。
- b) 在外部人员机动车停车场（库）、内部交通枢纽点位设置交通管理人员或停靠有安保标识的本单位车辆。
- c) 结合本行业实际情况，申请公安机构设立警务室或临时治安处置点，开展联合巡逻等必要的外部安保支持手段。
- d) 采用出入口闸机、计数器、电子票及视频统计等手段开展人群聚集监测。
- e) 在人流密集区域设置人流、人车障碍物。
- f) 避免在非限制区设置重点部位；对非限制区水电油气和新风空调设施设置实体防护；在与危险物距离大于 5m 处设置管制性标识提示高压电气设施、压力容器、深水等危险物的位置和种类。
- g) 通过预约方式对外部人员进行实名认证。
- h) 设置禁限带物品清单，在非限制区出入口进行人身、随身物品安全检查。
- i) 增加视频监控设施并在明显位置提示公众进入公共视频监控区域。
- j) 根据需要在偏僻场所、服务窗口等位置设置紧急报警装置。

E.1.3 应急处置

- a) 制定拒检、人员聚集、人员活动范围超限、秩序扰乱及突发事件处置预案，明确处置程序。
- b) 制定应急疏散与就地避险预案；紧急疏散路线和避难场所设置合理，安全导向标识清晰。
- c) 根据人流情况，配备足够数量的最小应急单元治安保卫人员；最小应急单元治安保卫人员除配备必要的防护、防御、对抗性装备设施外，还根据单位实际情况配备现场维护类（硬质隔离护

栏、手持扩音器、客流统计终端、安全导向标识等）和应急处置类（应急广播、应急照明、应急电源、应急指挥、应急通信、应急物资等）装备设施。

- d) 当非限制区举办大型群众性活动时，按照《大型群众性活动安全管理条例》与 GB/T 33170 有关安全要求开展安全防范。

附录 F

(规范性)

重点单位常态防范设施配置

F.1 重点单位常态防范设施配置应符合表 F.1 的规定。

表F.1 重点单位常态防范设施配置

序号	具体部位	防护设施	重点单位		
			三级	二级	一级
1	/	实体防护系统	应	应	应
2		实体防护系统	应	应	应
3		电子防护系统	应	应	应
4		电子防护系统	宜	应	应
5		电子防护系统	宜	应	应
6	易发生误侵入位置	实体防护系统	/	/	宜
7	穿越周界的河道、涵洞等地下空间	实体防护系统	应	应	应
8	人员出入口	实体防护系统	应	应	应
9	车辆出入口	实体防护系统	应	应	应
10	主要出入口	实体防护系统	应	应	应
11		实体防护系统	应	应	应
12		电子防护系统	/	应	应
13		电子防护系统	应	应	应
14		电子防护系统	应	应	应
15	手持式金属探测器或通过式金属探测门等安全检查装置	电子防护系统	/	应	应
16		电子防护系统	/	/	应
17	通向重点部位和人员密集区域的道路	实体防护系统	应	应	应
18	室外人员密集区域周边	实体防护系统	应	应	应
19	门卫室（传达室）与外界相通的窗户	实体防护系统	/	应	应
20	门卫室（传达室）与外界相通的出入口	实体防护系统	/	应	应
21	信访接待场所	电子防护系统	应	应	应
22		电子防护系统	应	应	应
23		电子防护系统	应	应	应
24		电子防护系统	应	应	应
25	高风险车辆行驶路线	电子防护系统	应	应	应

表F.1 重点单位常态防范设施配置（续）

序号	具体部位		防护设施		重点单位		
					三级	二级	一级
26	周界	单位内部主要道路	电子防护系统	视频图像采集装置	应	应	应
27		人员密集区域	电子防护系统	视频图像采集装置	应	应	应
28		室外重要部位	电子防护系统	视频图像采集装置	应	应	应
29		单位内部易发生安全威胁事件的区域	电子防护系统	紧急报警装置	应	应	应
30		机动车停车场（库）出入口	电子防护系统	视频图像采集装置	应	应	应
31			电子防护系统	电子巡查装置	应	应	应
32		非机动车集中存放处	电子防护系统	视频图像采集装置	应	应	应
33			电子防护系统	电子巡查装置	应	应	应
34		门卫室（传达室）	电子防护系统	紧急报警装置	/	应	应
35			电子防护系统	视频图像采集装置	/	应	应
36			电子防护系统	有线/无线通信装置	/	应	应
37			电子防护系统	手持式金属探测器等安全检查装置	/	应	应
38		制高点	电子防护系统	视频图像采集装置	/	/	宜
39		重点部位所在建（构）筑物	周边	实体防护系统	实体屏障	/	/
40	出入口		电子防护系统	视频图像采集装置	应	应	应
41	大厅		电子防护系统	视频图像采集装置	应	应	应
42	主要通道		电子防护系统	视频图像采集装置	应	应	应
43	楼顶		电子防护系统	视频图像采集装置	应	应	应
44	电梯轿厢		电子防护系统	视频图像采集装置	应	应	应
45	电梯厅		电子防护系统	视频图像采集装置	应	应	应
46	楼梯间		电子防护系统	视频图像采集装置	应	应	应
47	多个单位共用同一建（构）筑物的管理边界		电子防护系统	出入口控制控制装置	应	应	应
48	人员、车辆通道		电子防护系统	出入口控制装置	/	/	应
49	低于 2.5m 的室外空气进气口		实体防护系统	安全隔离设施	/	应	应
50	外立面		实体防护系统	防攀爬、防盗设施	应	应	应
51	建（构）筑物周边		电子防护系统	入侵探测装置	应	应	应
52	无人值守出入口		电子防护系统	入侵探测装置	宜	应	应
53	保卫执勤岗		电子防护系统	视频图像采集装置	/	应	应
54			电子防护系统	紧急报警装置	/	/	应
55	应急疏散出入口		实体防护系统	紧急开启设施	应	应	应
56	直通室外的通道、管口		实体防护系统	实体防护设施	应	应	应
57	无人值守的出入口		实体防护系统	防盗安全门	应	应	应

表F.1 重点单位常态防范设施配置（续）

序号	具体部位		防护设施		重点单位		
					三级	二级	一级
58	重点部位	/	电子防护系统	电子巡查装置	应	应	应
59		室外重点部位周边	实体防护系统	实体屏障	/	/	应
60		重点部位所在楼层	电子防护系统	出入口控制装置	宜	应	应
61		出入口	电子防护系统	手持式金属探测器等安全检查装置	/	/	应
62			电子防护系统	视频图像采集装置	应	应	应
63			电子防护系统	出入口控制装置	宜	应	应
64		内部	电子防护系统	入侵探测装置	宜	应	应
65		内部主要通道	电子防护系统	视频图像采集装置	应	应	应
66		/	实体防护系统	防盗、防砸的防护设施	应	应	应

附录 G
(规范性)
单位内部检查内容

G.1 人力防范检查包括但不限于：

- a) 保卫力量背景；
- b) 资质审查情况；
- c) 保卫力量履行职责情况；
- d) 防范工作执行情况；
- e) 问题发现、报告、处置情况；
- f) 岗位管理情况等。

G.2 实体防范检查包括但不限于：

- a) 建（构）筑物空间布局情况；
- b) 实体防范设施配置情况；
- c) 实体防护装置、材料使用情况；
- d) 设施设备使用维护与保养情况等。

G.3 电子防范检查包括但不限于：

- a) 电子防护设施的配置情况；
- b) 验收情况；
- c) 运行情况；
- d) 防范效果情况；
- e) 系统使用维护与保养情况等。

G.4 制度检查包括但不限于：

- a) 制度内容情况；
 - b) 制度程序性情况；
 - c) 制度执行情况等。
-