ICS 13.310
A 90

DB4401

广　州　市　地　方　标　准

DB4401/T 10.2—2019

反恐怖防范管理　第2部分：党政机关

Anti-terrorism precaution management—Part 2: party and government departments and offices

2019-11-29 发布　　2020-2-10 实施

广州市市场监督管理局
广州市反恐怖工作领导小组办公室　　联合发布

目　次

前　言

DB4401/T 10《反恐怖防范管理》计划分为以下 33 个部分，以后根据反恐怖防范工作需要，再视情况进行调整：

——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；
——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：船舶港口码头；
——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。

本部分为 DB4401/T 10 的第 2 部分。

本部分按 GB/T 1.1—2009 的规定起草。

本部分由广州市反恐怖工作领导小组办公室和广州市公安局警卫支队提出。

本部分由广州市反恐怖工作领导小组办公室归口。

本部分由广州市公安局警卫支队具体解释和实施情况收集。

本部分起草单位：广州市公安局警卫支队、中共广州市委办公厅保卫科、广州市人大常委会办公厅行政处保卫科、广州市人民政府办公厅保卫科、政协广州市委员会办公厅行政处保卫科、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。

本部分主要起草人：王虎成、吴志强、唐小军、周建斌、周日荣、张志强、毛雨清、田从军、廖俊斌、吴朝阳、陈淑宜。

本部分为首次发布。

反恐怖防范管理 第2部分：党政机关

1 范围

本部分规定了党政机关反恐怖防范管理的术语和定义、反恐怖防范原则、防范分类及等级划分、反恐怖防范重要部位、常态反恐怖防范、非常态反恐怖防范、应急准备要求和监督、检查。

本部分适用于在穗的党政机关类反恐怖防范重点目标的防范工作和管理，党政机关类反恐怖防范一般目标可参照执行。

注：反恐怖防范重点目标由公安机关会同有关部门确定。

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 12663 入侵和紧急报警系统 控制指示设备
GB 12899 手持式金属探测器通用技术规范
GB 15208（所有部分） 微剂量X射线安全检查设备
GB/T 17565 防盗安全门通用技术条件
GB/T 22239—2019 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 信息系统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 32581 入侵和紧急报警系统技术要求
GB/T 37078 出入口控制系统技术要求
GB 50198 民用闭路监视电视系统工程技术规范
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 50396 出入口控制系统工程设计规范
GA/T 367 视频安防监控系统技术要求
GA/T 594 保安服务操作规程与质量控制
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/T 1127—2013 安全防范视频监控摄像机通用技术要求
GA/T 1343—2016 防暴升降式阻车路障
DB4401/T 10.1—2018 反恐怖防范管理 第1部分：通则

3 术语和定义

DB4401/T 10.1—2018界定的以及下列术语和定义适用于本文件。

3.1

党政机关 party and government departments and offices

中国共产党机关、人大机关、行政机关、政协机关、监察机关、审判机关、检察机关，以及各级党政机关派出、派驻机构。

4 反恐怖防范原则

4.1 党政机关的反恐怖防范应坚持“属地负责，逐级监管”，“谁主管，谁负责”的工作原则。

4.2 党政机关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、党政机关主管部门履行安全管理、指导、监督和检查责任。
4.3 党政机关是反恐怖防范的责任主体，应按照反恐怖主义法等相关法律法规要求履行职责。

5 防范分类及等级划分

5.1 防范分类

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。

5.2 非常态反恐怖防范等级

非常态反恐怖防范等级按恐怖威胁预警响应的要求分为四级：
a） 四级非常态反恐怖防范，Ⅳ级（一般），用蓝色表示；
b） 三级非常态反恐怖防范，Ⅲ级（较大），用黄色表示；
c） 二级非常态反恐怖防范，Ⅱ级（重大），用橙色表示；
d） 一级非常态反恐怖防范，Ⅰ级（特别重大），用红色表示。

6 反恐怖防范重要部位

党政机关反恐怖防范重要部位应包括：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。

7 常态反恐怖防范

7.1 人防

7.1.1 设置原则

7.1.1.1 应符合国家、省、市的相关法律法规、规章及有关标准对安保力量的要求。
7.1.1.2 党政机关应根据有关规定，结合单位工作性质及地理位置、单位面积、工作人员数量、重要部位分布等反恐怖防范工作实际需要，设置保卫机构，配备专职的保卫干部和足够的安保力量。

7.1.2 人防组织

7.1.2.1 党政机关应成立由机关内部各单位责任领导为成员的反恐怖防范工作领导小组，下设办公室并指定工作联络人员，落实主体责任，做好反恐怖防范工作。
7.1.2.2 党政机关反恐怖防范工作领导小组办公室设在保卫部门，由专职保卫干部、在编工作人员和机关内部各单位指定的安保负责人组成，承担反恐怖防范日常工作。
7.1.2.3 党政机关应明确党政机关反恐怖防范重要岗位，重要岗位见表1。

7.1.3 人防配置

党政机关反恐怖防范应按照表1的规定进行人防配置。

表1 人防配置表

序号	项目	配设要求	设置标准
1	工作机构	健全组织、明确分工、落实责任	应设
2	责任领导	主要负责人为第一责任人	应设
3	责任部门	党政机关保卫部门	应设
4	专职联络员	指定联络员1名	应设
5	安保负责人	内部各单位指定人员	应设

表1　人防配置表（续）

序号	项目		配设要求	设置标准
6	安保力量	技防岗位	重要技防系统设施	应设
7		固定岗位	安防监控中心、机关大院（大楼）出入口、会议场所、枪支弹药存放场所、接访场所	应设
8		巡查岗位	重要办公区域、档案室、机要室、保密室、财务室、案件管理中心、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、餐厅、停车库（场）、周界	应设
9		网管岗位	网络安全维护	应设
10		机动岗位	机动	应设

7.1.4　人防管理

7.1.4.1　党政机关应建立与反恐怖主义工作领导机构、公安机关的工作联系，定期报告反恐怖防范措施落实情况，互通信息、完善措施。发现可疑人员、事件、违禁和管制物品及违法犯罪行为应及时制止，并向公安机关报告，同时采取措施保护现场。

7.1.4.2　党政机关应加强人防管理，按DB4401/T 10.1—2018 中7.1.4.2的要求执行：

a）加强出入口来访人员管理，核对、查验、登记来访人员、车辆信息，必要时对来访人员进行安全检查及身份核验；

b）党政机关应指定专职联络员，联络员宜为党政机关保卫部门的负责人，应确保24小时通信畅通；联络员的配置和变更，应及时向公安机关和反恐怖主义工作领导机构的办事机构备案；

c）安保负责人为机关内部单位安全责任部门的负责人，安保负责人的配置和变更，应及时报送党政机关反恐怖防范工作领导小组办公室。

7.1.5　安保力量要求

反恐怖安保力量应符合DB4401/T 10.1—2018中7.1.5的要求，并应符合以下要求：

a）反恐怖防范安保力量应熟悉机关地理环境和主要设施布局，熟悉消防通道和各类疏散路线、场所和途径；

b）积极应对相关涉恐突发事件，协助、配合反恐怖主义工作领导机构、公安机关及党政机关主管部门开展应急处置工作；

c）安保负责人应熟悉反恐怖防范工作情况及相关规章制度、职责及分工、涉及的应急预案等；

d）安保负责人应按党政机关反恐怖防范工作领导小组办公室的分工和要求，组织本单位的安保力量，落实本单位的反恐怖防范的责任，参与机关大院（大楼）的整体防范工作。

7.2　物防

7.2.1　配置原则

7.2.1.1　应符合国家、省、市的相关法律法规、规章及有关标准对工程建设的要求。

7.2.1.2　应纳入重点目标工程建设总体规划，新建或改建项目应同步设计、同步建设、同步运行。

7.2.1.3　使用的设备和设施应符合相关标准要求，并经检验或认证合格。

7.2.2　物防组成

重点目标物防包括实体防护设施、个人应急防护装备、公共应急防护装备及设施等。

7.2.3　物防配置

党政机关反恐怖防范应按照表2的规定进行物防配置。

表 2 物防配置表

序号	项目		安放区域或位置	设置标准
1	实体防护设施	机动车阻挡装置	机关大院（大楼）出入口	应设
2		防暴阻车路障	机关大院（大楼）出入口	应设
3		防盗安全门、金属防护门或防尾随联动互锁安全门	重要办公区域、配电站、通信系统、通风系统、空调系统、安防监控中心、数据信息中心、案件管理中心	应设
			枪支弹药存放场所、档案室、机要室、保密室	应设
4		防盗保险柜、防盗保险箱	财务室、档案室、机要室、保密室	应设
5		围栏或栅栏	周界	应设
6		人车分离通道	机关大院（大楼）出入口	应设
7		人行出入口通道闸	机关大院（大楼）出入口	应设
8	个人应急防护装备	对讲机、强光手电、防暴棍	传达室、执勤岗位、装备室	应设
9		毛巾、口罩	办公楼各楼层、供开放、参观区域、接访场所	应设
10		防毒面罩或防烟面罩	办公楼各楼层、供开放、参观区域、安防监控中心	应设
11		防暴盾牌、钢叉	传达室、执勤岗位、装备室、接访场所	应设
12		防暴头盔、防割（防刺）手套、防刺服	传达室、执勤岗位、装备室、接访场所	应设
13		化学防护服、铅衣及相关药品	传达室、执勤岗位、装备室、接访场所	宜设
14	公共应急防护装备及设施	防爆桶、防爆毯（含防爆围栏）	传达室、执勤岗位、备勤室	应设
15		应急警报器	传达室、保卫部门、安防监控中心、接访场所、执勤岗位、备勤室	应设
16		灭火器材	餐厅、会议场所、办公区域等室内各处、执勤岗位、备勤室	应设
注：阻挡装置指出入口的杆或闸门等，一般安装在机动车出入口，主要是对出入行为实施放行、拒绝、报警功能的设施；防暴阻车路障指能够有效防范汽车冲撞等暴力侵害的硬质设施，如防冲撞金属柱、翻板式路障机等高强度防汽车冲撞功能的设备。				

7.2.4 物防要求

7.2.4.1 防护设备设施要求

7.2.4.1.1 一般要求

物防设施应符合DB4401/T 10.1—2018 中7.2.4.1及相关标准的要求。

7.2.4.1.2 实体防护设施

实体防护设施应符合以下要求：

a） 实体围墙一般采用钢筋混凝土预制板、砖混结构、钢栅栏等结构形式，高度不应低于2 m。

b） 采用砖石或钢筋混凝土结构时，墙厚不小于200 mm，砖混结构围墙的强度应符合相应的国家现行工程建设标准。

c） 采用钢栅栏时应采用单根直径不小于20 mm，壁厚不小于2 mm的钢管（或单根直径不小于16 mm的钢棒，单根截面不小于8 mm×20 mm的钢板）组合制作；用于窗的防护时，栅栏应安装在窗内侧；单个栅栏空间最大面积应不大于600 mm×100 mm；栅栏应采用直径不小于12 mm的膨胀螺丝固定，安装应牢固可靠。用于实体周界封闭时，栅栏的竖杆间距不大于150 mm，且不易攀爬，安装应牢固可靠；钢栅栏的设置应符合消防的有关规定。

d） 防暴阻车路障至少应符合GA/T 1343—2016中B2级的要求和其他相关标准的要求，且常态处于升起状态。

7.2.4.2 防护设备设施采购与维护

防护设备设施采购与维护应符合DB4401/T 10.1—2018中7.2.4.2的要求。

7.3 技防

7.3.1 建设原则

7.3.1.1 应符合国家、省、市的法律法规、规章及有关技术标准对工程建设的要求。
7.3.1.2 应纳入重点目标工程建设总体规划，新建或改建项目应同步设计、同步建设、同步运行。
7.3.1.3 使用的设备设施应符合相关技术标准的要求，并经检验或认证合格。

7.3.2 技防组成

党政机关技防设施包括电子防护系统、安防监控中心、公共广播系统、无线通信对讲指挥调度系统、通讯显示记录系统等，其中电子防护系统包括视频监控系统、入侵和紧急报警系统、出入口控制系统、停车库（场）管理系统、电子巡查系统（巡更系统）、安全检查及探测系统、无人机监控系统、信息隔离控制系统（防火墙）等。

7.3.3 技防配置

党政机关反恐怖防范应按照表3的规定进行技防配置。

表 3 技防配置表

序号	项目		安装区域或覆盖范围	设置标准
1	安防监控中心		—	应设
2	视频监控系统	摄像机	机关大院（大楼）出入口	应设
3			机关大院（大楼）出入口外 25m 范围	应设
4			机关大院内各办公楼出入口	应设
5			机关大院（大楼）周界	应设
6			办公楼大厅、电梯等候区	应设
7			电梯轿厢、自动扶梯口	应设
8			办公楼内各层楼梯口、通道	应设
9			机关大院内公共区域全覆盖	应设
10			会议室、餐厅的出入口	应设
11			水、气、电、油、网络通讯、空调控制区域、（新风系统）新风口	应设
12			枪支、弹药存放处的出入口	应设
13			传达室	应设
14			停车场（库）及其主要通道和出入口	应设
15			安防监控中心	应设
16			数据信息中心、文印中心、公文交换中心、档案室、机要室、保密室、案件管理中心的出入口	应设
17			重要办公室通道	应设
18			接访场所	应设
19		声音复核装置	主要出入口	宜设
20			枪支、弹药存放处（驻警单位自行安装管理）	应设
21			传达室	宜设
22			接访场所	应设
23		视频智能分析系统	安防监控中心、图像采集前端	宜设
24		人脸图像识别系统	传达室、安防监控中心、各楼层入口	应设
25		机动车号牌自动识别系统	停车库（场）、出入口	应设
26		控制、记录、显示装置	安防监控中心	应设
27	入侵和紧急报警系统	入侵探测（报警）器	办公院区（楼）周界	应设
28			办公楼一、二层与外界直接相通的窗户	应设
29			水、气、电、通讯、空调、通风控制区域	应设
30			枪支、弹药存放处（驻警单位自行安装管理）	应设
31			数据信息中心、文印中心、公文交换中心、档案室、机要室、保密室	应设
32		紧急报警装置（一键报警）	重要办公区域、执勤岗位、传达室、备勤室等	应设
33			安防监控中心	应设
34		报警控制器	安防监控中心及相关的独立设防区域	应设
35		终端图形显示装置	安防监控中心	宜设

表3 技防配置表（续）

序号	项目		安装区域或覆盖范围	设置标准
36	出入口控制系统	门禁系统	传达室	应设
37			停车场（库）与办公楼相通的人行出入口	宜设
38			无人值守的重要设备机房	应设
39			数据信息中心	应设
40			重要办公区域、档案室、机要室、保密室	应设
41			枪支、弹药存放处（驻警单位自行安装管理）	应设
42		虹膜识别系统等人体特征生物识别系统	重要办公区域	宜设
43			安防监控中心、图像采集前端	宜设
44			传达室、机关大院（大楼）出入口	宜设
45		身份证验证系统	传达室、机关大院（大楼）出入口	应设
46	停车库（场）管理系统		停车库（场）	应设
47	电子巡查系统（巡更系统）		办公院区周界、机关大院（大楼）出入口	应设
48			办公楼内各楼层	应设
49			重要部位	应设
50	公共广播系统		区域全覆盖	应设
51	无线通信对讲指挥调度系统		区域全覆盖、安防监控中心	应设
52	安全检查及探测系统	微剂量X射线安全检查装置	传达室或机关大院（大楼）出入口	宜设
53		通过式金属探测门	传达室或机关大院（大楼）出入口	宜设
54		手持式金属探测器	传达室或机关大院（大楼）出入口	应设
55	通讯显示记录系统		服务、咨询电话、总机	应设
56	无人机监控系统		区域全覆盖	宜设
57	信息隔离控制系统（防火墙）		网络通讯控制区域	应设

7.3.4 技防要求

7.3.4.1 技防系统总体要求

党政机关的反恐怖防范技防系统总体要求，应满足以下要求：

a） 系统应符合DB4401/T 10.1—2018中7.3.4条对技防要求；

b） 系统应满足GB 50348中技防设备设施的相关规定；

c） 承载安防信息的信息系统应符合GB/T 22239—2019和GB/T 22240中相应规定，当主要使用方为重点目标时，应符合GB/T 22239—2019中第二级网络安全保护等级要求；主要使用方为公安机关时，应符合GB/T 22239—2019中第三级网络安全保护等级要求。

7.3.4.2 安防监控中心

安防监控中心应符合以下要求：

a） 视频安防监控、入侵报警、电子巡查的终端设备，以及出入口控制系统的报警信号输出终端均应设置在安防监控中心，应能实现对各子系统的操作、记录和显示；

b） 安防监控中心配置的与报警同步的终端图形显示装置，应能准确地指示报警区域，实时声、光提示发生警情的区域、日期、时间等信息。

7.3.4.3 视频安防监控系统

7.3.4.3.1 系统要求

视频监控系统应符合以下要求：

a） 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，视频监控系统应同时满足GB 50198、GB 50395、GA/T 367、GA/T 669.1的要求。

b） 视频监控系统应采用数字系统。
c） 图像信号的采集使用的摄像机应符合 GA/T 1127—2013 的要求，与外界相通的出入口配置的摄像机应满足 C 类以上高清晰度，其他重要部位配置的摄像机应满足 B 类以上高清晰度。
d） 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、G.729 等音频编解码标准实现音频同步存储。新建、改建、扩建的视频监控系统音视频编解码宜优先采用 GB/T 25724 规定的 SVAC 编码方式。
e） 图像信号的传输、交换和控制应符合 GB/T 28181 的要求。
f） 图像信号的切换应具有手动和编程两种模式。
g） 图像信号的显示设备应采用 FHD（1920x1080）以上分辨率的大屏设备，当系统配备的超高清摄像机（GA/T 1127—2013 的 D 类）时，宜采用 4K（4096×2160）以上分辨率的大屏设备。
h） 图像信号的存储：
——外界相通的出入口的单路图像应具有 16CIF（1920×1080）或以上图像分辨率；
——非直接与外界相通的重要部位单路图像应具有 9CIF（1280×720）或以上图像分辨率；
——单路显示基本帧率不小于 25 fps；
——存储时间不小于 90 天。
i） 系统应能切换图像，并能根据系统的配置，控制摄像机云台、镜头等。
j） 带有云台、变焦镜头的摄像机应具有预制位，应有自动复位功能且自动复位时间可调。

7.3.4.3.2 摄像机

摄像机应符合以下要求：
a） 摄像机安装应减少或避免图像出现逆光，且摄像机工作时监视范围内的平均照度宜不小于 200 Lx。
b） 出入口、与出入口相连的通道摄像机安装应符合以下要求：
1） 出入方向上，具有正反向两组摄像机；
2） 监视区域内不应有盲区；
3） 通过监视屏应 24 小时均能清楚地辨别出入人员面部特征、机动车牌号；
4） 显示的人员正面面部有效画面宜不小于监视屏显示画面的 1/60。
c） 党政机关院区门外、公共区域及制高点宜安装带有云台、变焦镜头的摄像机， 通过监视屏应能清楚的显示视场半径不小于 25 m 监视范围内车辆、人员的活动情况。
d） 带有云台、变焦镜头的摄像机在云台、变焦停止操作后，摄像机应在（2±0.5）分钟内自动复位至初始设定状态。

7.3.4.3.3 声音复核装置

声音复核应与图像记录同步，回放应清晰。

7.3.4.3.4 人脸图像识别系统

人脸识别装置应建立数据库，并应满足以下主要要求:
a） 应能对照片或录像等比对源图像信号进行人脸识别；
b） 应能对不小于显示屏有效画面比例 1/8 的人脸识别；
c） 脸部小于 15° 的姿势变化应不影响识别的正确性；
d） 每个视频通道应能同时对 2 个（含）以上的人脸图像进行识别，识别速度应不小于 4 frame/s，一旦发现识别目标应立即显示并报警；
e） 人脸信息采集宜采用 500 万像素以上人脸抓拍摄像机。

7.3.4.4 入侵和紧急报警系统

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/T 32581、GB 50394 等入侵和紧急报警系统相关标准的要求；
b） 应按需要选择、安装入侵探测器，防区内不应有盲区；
c） 防区划分应有利于报警时准确定位，周界封闭屏障防区间距应不大于 50 m；

d) 周界报警系统应24小时设防；
e) 紧急报警装置应安装在隐蔽、便于操作的部位，并应设置为不可撤防模式，且应有防误触发措施。当被触发报警后应能立即发出紧急报警信号并自锁，复位应采用人工操作方式；
f) 除周界封闭屏障处以外，无人看守的场所安装入侵探测器的部位均应安装声光告警器，其报警声压不小于80 dB（A），报警持续时间不小于5分钟；
g) 独立设防区域的入侵和紧急报警系统应与配置专职值守人员的安防中心控制室联网。安防中心控制室应安装与区域报警中心联网的紧急报警装置；系统使用专用电缆传输报警信号时报警响应时间应不大于3秒；使用公共电话网络传输时报警响应时间应不大于20秒；
h) 以公共电话网络作为报警传输专线时，不应在线路上挂接其他通信设施；
i) 系统应具有时间、日期的显示、记录和调整功能，时间误差应在±30秒以内；
j) 系统布防、撤防、报警、故障等信息的存储时间应不少于180天，并能输出打印；
k) 系统的备用电源应满足24小时正常工作；
l) 宜配备图片复核及视频复核功能；
m) 入侵和紧急报警系统应能与视频安防监控系统、人脸识别图像系统、声音复核装置、出入口控制系统等联动使用。

7.3.4.5 出入口控制系统

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 50396、GB/T 37078等出入口控制系统相关标准的要求；
b) 对非法进入的行为或连续3次不正确的识读，系统应发出报警信号，系统安装部位的报警声压不小于80 dB（A），报警持续时间不小于5分钟；
c) 不宜使用仅具有密码按键式识读功能的设备；
d) 系统时间误差应在±10秒内，记录保存时间应不少于90天；
e) 用于重要办公区域的出入口控制系统应符合GB/T 37078—2018中等级3中高安全等级的要求；
f) 身份证验证系统应与公安机关数据联网。

7.3.4.6 电子巡查系统

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) 巡查点安装应牢固、隐蔽，高度应便于识读；
c) 保存时间应不少于90天。
可使用出入口控制系统相关设备实现电子巡查功能。

7.3.4.7 安全检查及探测系统

安全检查及探测系统应符合以下要求：
a) 微剂量X射线安全检查设备应符合GB 15208的要求；
b) 手持式金属探测器应符合GB 12899的要求；
c) 通过式金属探测门应符合GB/T 17565的要求。

7.3.4.8 通讯显示记录系统

通讯显示记录系统应符合以下要求：
a) 来电号码显示应清晰，时间误差应在±30秒以内；
b) 来电通话录音回放时应清晰可辨，通话记录保存时间应不少于90天。

7.3.5 系统检验与验收

系统验收前应进行检验，系统检验和验收应符合法律、法规、行业有关技术标准及公安机关的相关要求。

7.3.6 运行维护及保养

运行维护及保养按DB4401/T 10.1—2018中7.3.6要求进行。

7.4 制度防

7.4.1 一般要求

制度防应符合DB4401/T 10.1—2018中7.4要求。

7.4.2 管理标准

管理标准配置除符合DB4401/T 10.1—2018中7.4.3.2要求外，还应符合以下要求：

a) 建立门卫登记与检查制度，明确核对、查验、登记来访人员、车辆信息，安全检查的管理要求，参见附录A；
b) 制定会议（活动）保卫制度，明确各类会议期间人防、物防、技防的保卫措施，参见附录B；
c) 制定党政机关反恐怖防范工作领导小组及办公室制度，见附录C；
d) 制定党政机关内部安保信息采集、调取、使用管理制度。

7.4.3 工作标准

工作标准配置应符合DB4401/T 10.1—2018中7.4.3.3要求。

7.4.4 技术标准

技术标准配置应符合DB4401/T 10.1—2018中7.4.3.4要求。

8 非常态反恐怖防范

8.1 非常态反恐怖防范启动

根据反恐怖主义工作领导机构、公安机关发布的恐怖威胁预警，进入非常态反恐怖防范。

党政机关可根据实际工作需要进入非常态反恐怖防范。

8.2 非常态反恐怖防范实施

党政机关应积极响应恐怖威胁预警要求，采取的非常态反恐怖防范等级应不低于有关部门或机构发布的恐怖威胁预警等级。

非常态反恐怖防范等级和恐怖威胁预警等级对应关系见表4。

表4 非常态反恐怖防范等级和恐怖威胁预警等级对应关系表

非常态反恐怖防范等级	恐怖威胁预警等级	恐怖威胁预警颜色
四级（Ⅳ）	四级（Ⅳ）	蓝色
三级（Ⅲ）	三级（Ⅲ）	黄色
二级（Ⅱ）	二级（Ⅱ）	橙色
一级（Ⅰ）	一级（Ⅰ）	红色

8.3 非常态反恐怖防范措施

8.3.1 四级非常态反恐怖防范

党政机关应在符合常态反恐怖防范的基础上，同时采取以下工作措施：

a) 启动反恐怖应急指挥部，各类防范、处置装备设施处于待命状态；
b) 党政机关保卫部门负责人带班组织防范工作；
c) 在常态安保力量的基础上增派50%以上；
d) 严格执行各项管理制度，检查物防、技防设施；
e) 严格控制来访人员进出；

f） 主要出入口设置障碍，严格控制来访车辆进入；
g） 联系属地公安机关和党政机关主管部门指导防范工作；
h） 对外来物品进行拆包检查；
i） 加强对机关周边区域的巡查；
j） 每天主动向公安机关和党政机关主管部门报告防范工作落实情况，重要情况应随时报告；
k） 配合反恐怖主义工作领导机构及其办事机构、公安机关开展工作；
l） 根据反恐怖主义工作领导机构及其办事机构、公安机关要求采取的其他防范措施。

8.3.2 三级非常态反恐怖防范

应在符合四级非常态反恐怖防范的基础上，同时采取以下工作措施：
a） 党政机关保卫部门负责人24小时值班；
b） 在常态安保力量的基础上增派70%以上；
c） 加强对区域内人员、车辆、物品进行安全检查；
d） 每半天主动向属地公安机关报告防范工作落实情况，重要情况应随时报告；
e） 联系属地公安机关和党政机关主管部门派员指导防范工作。

8.3.3 二级非常态反恐怖防范

应在符合三级非常态反恐怖防范的基础上，同时采取以下工作措施：
a） 党政机关反恐怖防范工作领导小组负责人带班组织防范工作；
b） 在常态安保力量的基础上增派100%以上；
c） 重要部位巡查频率提高；出入口派员加强值守；
d） 联系属地公安机关和党政机关主管部门派员参与反恐怖防范工作。

8.3.4 一级非常态反恐怖防范

应在符合二级非常态反恐怖防范的基础上，同时采取以下工作措施：
a） 党政机关反恐怖防范工作领导小组负责人24小时值班；
b） 装备、力量、保障进入临战状态；
c） 重要部位应有2名以上安保人员守护，实行24小时不间断巡查；
d） 对无关工作人员进行疏散，必要时转移重要信息、物资；
e） 封闭出入口，严密监视内外动态；
f） 对目标区域进行全面、细致检查；
g） 对相关要害部位、设施、场所实施现场管控。

8.4 非常态反恐怖防范的人防、物防和技防配置

党政机关应建立相关机制，确保启动非常态反恐怖防范时人防、物防和技防配置的要求，确保增派的安保力量、物防设备设施和技防系统能及时到位。

9 应急准备要求

9.1 总体要求

符合DB4401/T 10.1—2018中第9章相关规定。

9.2 应急预案

9.2.1 预案体系

重点目标的应急预案体系主要由综合应急预案、专项应急预案和现场处置方案构成。重点目标应根据本单位组织管理体系、单位规模、危险源的性质以及可能发生的事故类型确定应急预案体系，并应根据本单位的实际情况制定各项专项应急预案。

9.2.2 综合应急预案

综合应急预案是重点目标应急预案体系的总纲，主要从总体上阐述事故的应急工作原则，包括重点目标的应急组织机构及职责、应急预案体系、事故风险描述、预警及信息报告、应急响应、保障措施、应急预案管理等内容。

9.2.3 专项应急预案

专项应急预案是重点目标为应对某一类型或某几种类型事故，或者针对重要部位设施、重大危险源、重大活动等内容而定制的应急预案。专项应急预案主要包括事故风险分析、应急指挥机构及职责、处置程序和措施等内容。

9.2.4 现场处置方案

现场处置方案是重点目标根据不同事故类型，针对具体的场所、装置或设施所制定的应急处置措施，主要包括事故风险分析、应急工作职责、应急处置和注意事项等内容。重点目标应根据风险评估、岗位操作规程以及危险性控制措施，组织本单位现场作业人员及安保等专业人员共同编制现场处置方案。

9.3 反恐应急演练

9.3.1 党政机关应根据各实际情况，因地制宜，按应急预案要求开展应急演练。

9.3.2 党政机关每年应组织一次综合反恐应急综合演练。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，保证安全、有序、可控。

10 监督、检查

10.1 应符合 DB4401/T 10.1—2018 第 10 章的要求。

10.2 党政机关实施的自我检查应符合 DB4401/T 10.1—2018 中附录 C 的要求。公安机关、党政机关主管部门开展的部门检查、反恐怖主义工作领导机构的办事机构开展的督导检查，可使用抽查重点项目的方式开展，抽查项目参见附录 D。

附 录 A
（资料性附录）
门卫登记与检查制度

A.1 目的

加强党政机关出入口管理，建立门卫登记与检查管理要求。

A.2 制度框架

符合DB4401/T 10.1—2018中A.2要求。

A.3 管理要求

A.3.1 人员进出管理

A.3.1.1 工作时段进出管理

A.3.1.1.1 工作人员

党政机关应设置入口控制系统，工作人员凭授权的有效证件进出，并配合安保人员的安检。

A.3.1.1.2 来访人员

来访人员，凭有效工作证件、证明或党政机关内单位印发的会议通知或内部工作人员确认，并经安保人员验证、登记、检查后进入。

A.3.1.1.3 物品

进出党政机关的物品应经安保人员安检后放行。

A.3.1.2 非工作时段进出管理

A.3.1.2.1 党政机关应制定非工作时间（包括晚间、周末、节假日）人员进入党政机关大院的管理工作制度。

A.3.1.2.2 党政机关内各单位应建立节假日值班机制，明确值班人员安全责任和情况报告机制。

A.3.2 车辆进出管理

A.3.2.1 建立机关内部车辆管理制度。

A.3.2.2 党政机关应建立党政机关内单位的公务车辆备案机制，设置车辆通行专用标志，凭有效证件进出和停放。

A.3.2.3 党政机关应建立来访车辆预约备案和登记机制。

A.3.2.4 车辆的乘客及物品按要求进行管理（见A.3.1）。

附 录 B
（资料性附录）
会议（活动）保卫制度

B.1 目的

为了确保在党政机关内召开的重要会议安全，加强安全防范的力度。

B.2 制度框架

符合DB4401/T 10.1—2018中A.2要求。

B.3 管理要求

B.3.1 党政机关应制定有关会议（活动）的安全管理制度。
B.3.2 党政机关召开有关会议按照“谁主办、谁负责”的原则，落实安全责任。
B.3.3 在党政机关内举办的各类重要会议（活动），提前向保卫部门报备。
B.3.4 保卫部门应根据会议的规模制定具体的会议（活动）保卫方案，明确人防、物防、技防及相关管理要求，明确主（承）办单位的责任、重要会议（活动）场所的管理单位及保卫部门的分工、职责。
B.3.5 主（承）办单位、保卫部门等各方要开展会议（活动）风险评估，同时做好相关应急处置的准备，必要时报告公安机关。
B.3.6 保卫部门应协助重要会议（活动）主（承）办单位，做好会前安全检查以及会议期间的安全保卫工作。

附 录 C
（规范性附录）
党政机关反恐怖防范工作制度

C.1 目的

为共同做好党政机关反恐怖防范工作，加强联系与沟通，建立党政机关反恐怖防范工作制度，形成一体防范的机制。

本制度适用于机关大院或多个党政机关共同办公的场所。

C.2 制度框架

符合DB4401/T 10.1—2018中A.2要求。

C.3 管理要求

C.3.1 机构组织

C.3.1.1 党政机关反恐怖防范工作领导小组由机关内部各单位的责任领导组成。

C.3.1.2 党政机关反恐怖防范工作领导小组下设办公室，办公室设在党政机关保卫部门，由党政机关保卫部门中保卫干部、在编工作人员和机关内部各单位指定的安保负责人组成。

C.3.2 职责分工

C.3.2.1 党政机关反恐怖防范工作领导小组

党政机关反恐怖防范工作领导小组的职责：

a） 审议年度反恐防范工作报告；

b） 反恐怖防范体系有效性的评审、监督和指导；

c） 针对反恐防范存在的问题进行决议。

C.3.2.2 党政机关反恐怖防范工作领导小组办公室

党政机关反恐怖防范工作领导小组办公室作为党政机关反恐怖防范工作领导小组的办事机构，其职责：

a） 党政机关反恐怖防范体系的建立、运行、完善及自我监督检查；

b） 党政机关反恐怖防范的日常管理，包括人防、物防、技防管理及制度防的落实；

c） 制定年度反恐怖防范工作计划；

d） 组织反恐怖防范安全宣传教育；

e） 组织各项联合演练；

f） 向党政机关反恐怖防范工作领导小组提交年度反恐防范工作报告；

g） 重要会议一体防范的策划及防范；

h） 与公安机关、反恐怖工作领导机构的办事机构的联动联防；

i） 完成上级部署的工作任务。

C.3.3 工作规则

C.3.3.1 党政机关反恐怖防范工作领导小组原则上一年召开1次会议，可根据工作需要临时召开；会议形成会议纪要，并印发相关部门和单位。

C.3.3.2 党政机关反恐怖防范工作领导小组办公室原则上每季度召开1次会议，可根据工作需要临时召开。

附 录 D
（资料性附录）
党政机关反恐怖防范工作重点项目检查实施

D.1 概述

党政机关反恐怖防范工作重点项目检查的实施按DB4401/T 10.1—2008的附录C规定进行。

D.2 检查表格

检查表格应包括依据的标准条款，检查内容概要，检查过程记录和项目结论。格式参见表D.1。

表 D.1 重点项目检查表格

序号	标准条款		内容概要	检查记录	项目结论
1	7.1 人防	7.1.3	是否按实际需要配备了技防岗位、固定岗位、巡查岗位、网管岗位和机动岗位等安保力量		
2		7.1.4.1	与反恐怖主义工作领导机构、公安机关及党政机关主管（监管）部门的工作联系途径是否有效		
3		7.1.4.2	是否对重要岗位人员开展背景审查，查看审查记录		
4			是否建立重要岗位人员档案并备案，查看档案资料		
5			是否对出入口人员、车辆进行登记检查，检查记录		
6			是否按有效的路径和方式开展巡查，检查记录		
7			是否在正确的位置正确使用安检设备开展安检工作		
8			视频监控系统的值班监看是否到位		
9			检查培训计划和培训记录		
10			检查训练计划和训练记录		
11			检查演练计划和演练记录		
12			是否指定了专职联络员，联络员的配置和变更，是否及时按要求报备，年内是否存在工作联系不到的情况		
13		7.1.5	反恐怖防范工作机构设置、责任领导、责任部门等是否按要求报备		
14			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		
15			反恐怖防范专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		
16			反恐怖防范专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		
17	7.2 物防	7.2.3	机动车阻挡装置设置是否已覆盖机关大院（大楼）的主要出入口		
18			防暴阻车路障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		
19			控制中心等重要部位出入口是否安装防盗安全门等实体防护设施		
20			周界是否设置围墙或栅栏		
21			出入口是否设置人车分离通道		

表D.1 重点项目检查表格（续）

序号	标准条款		内容概要	检查记录	项目结论
22	7.2 物防	7.2.3	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		
23			是否按实际需要配备了防爆毯（含防爆围栏）等公共应急防护装备		
24			传达室、保卫部门、安防监控中心等是否已按要求设置了应急警报器		
25			各工作区域是否按要求设置了灭火器材		
26	7.3 技防	7.3.3	是否已按要求设置了控制中心，控制中心是否设有控制、记录、显示等装置		
27			摄像机是否已覆盖机关大院（大楼）出入口外 25m 范围、机关大院（大楼）周界、机关大院内公共区域全覆盖、机关大院（大楼）出入口、机关大院内各办公楼出入口、办公楼大厅、电梯等候区、电梯轿厢、自动扶梯口、办公楼内各层楼梯口及通道、会议室、餐厅的出入口、水、气、电、油、网络通讯、空调控制区域、新风口（新风系统）、枪支、弹药存放处的出入口、传达室、停车场（库）及其主要通道和出入口、安防监控中心、数据信息中心、文印中心、公文交换中心、档案室、保密室、机要室的出入口、财务室、重要办公室通道、接待场所等区域		
28			主要出入口、传达室、枪支、弹药及危险物品存放场所、信访接待场所是否已安装声音复核装置		
29			入侵探测（报警）器是否已覆盖办公院区（楼）周界、办公楼一、二层与外界直接相通的窗户、水、气、电、通讯、空调、通风控制区域、枪支、弹药存放处（驻警单位自行安装管理）、数据信息中心、文印中心、公文交换中心、档案室、机要室、保密室等重要场所		
30			紧急报警装置（一键报警）是否已设置在重要办公区域、传达登记处、传达室、安防监控中心、接待场所		
31			报警控制器是否已设置在安防监控中心及相关的独立设防区域		
32			出入口控制系统是否已设置在传达室、停车场（库）与办公楼相通的人行出入口、重要办公室、无人值守的重要设备机房、数据信息中心、档案室、保密室、机要室、枪支、弹药存放处（驻警单位自行安装管理）		
33			停车场是否设置停车场（库）管理系统		
34			出入口、周界、重要部位和人员密集区域是否设置了电子巡查系统		
35			公共广播系统是否已区域全覆盖		
36			无线通信对讲指挥调度系统是否已安装在安防监控中心并做到区域全覆盖		
37			视频录像保存时间是否不少于90天		
38			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；入侵和紧急报警系统备用电源是否满足至少24正常工作的需要		

表D.1　重点项目检查表格（续）

序号	标准条款		内容概要	检查记录	项目结论
39	7.4 制度防	7.4.1 7.4.2	是否按要求配置了相关管理制度，包括教育培训制度、人员背景审查制度、人员档案及备案制度、巡查与安检制度、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、恐怖威胁预警响应制度、恐怖威胁风险评估制度、联动配合机制、应急管理制度、门卫登记与检查制度、会议（活动）保卫制度、党政机关反恐怖防范工作制度等		
40	9 应急准备	9	是否制定了应急预案		
41		9	应急预案的内容是否全面		
42		9	是否有组建应急作战队伍并建立有效增援保障措施		
43		9	是否按规定开展应急预案的演练		

参 考 文 献

[1] 《中华人民共和国反恐怖主义法》 中华人民共和国主席令 第三十六号
[2] 《中华人民共和国突发事件应对法》 中华人民共和国主席令 第六十九号
[3] 《企业事业单位内部治安保卫条例》 中华人民共和国国务院令 第421号