ICS 13.310

A 90

DB4401

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

Anti-terrorism precaution management—Part 31: Telecommunications Internet

2019-12-24 发布　　2020-02-10 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31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工业和信息化局提出。

本部分由广州市反恐怖工作领导小组办公室归口。

本部分由广州市工业和信息化局具体解释和实施情况收集。

本部分起草单位：广州市工业和信息化局、广东省电信规划设计院有限公司、广州计量检测技术研究院、中国电信股份有限公司广州分公司、中国移动通信集团广东有限公司广州分公司、中国联合网络通信有限公司广州市分公司、中国铁塔股份有限公司广州市分公司、广州市公安局反恐怖支队。

本部分主要起草人：黄东旭、薛绮、郑耿、吴龙照、张金权、唐小军、张启星、李聪、郑欣旸、陈海涛、李梅菲、黄晓翔、陈仲、廖俊斌、吴朝阳。

本部分为首次发布。

反恐怖防范管理 第31部分：电信互联网

1 范围

本部分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、防范分类及等级划分、重点分目标及其重要部位、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。

本部分适用于广州市电信互联网基础设施类反恐怖防范重点目标的防范工作和管理，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/T 2887 计算机场地通用规范

GB 12663 入侵和紧急报警系统 控制指示设备

GB 16796 安全防范报警设备 安全要求和试验方法

GB/T 22239—2019 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 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 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 50526 公共广播系统工程技术规范

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/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 1132 车辆出入口电动栏杆机技术要求

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

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

电信 telecommunications

利用有线、无线的电磁系统或者光电系统，传送、发射或者接收语音、文字、数据、图像以及其它形式信息的活动。

3.2

互联网 internet

泛指广域网、局域网及终端（包括计算机、手机等）通过交换机、路由器、网络接入设备等基于一定的通信协议连接形成的，功能和逻辑上的大型网络。

3.3

电信互联网运行维护单位 telecom Internet operations and maintenance units

提供电信服务、互联网信息服务或政务信息服务的运行维护主体单位。

3.4

反恐怖防范重点目标的分目标 sub-target of the key prevention targets for anti-terrorism

以企业或行业为整体确定的反恐怖防范重点目标中，遭受恐怖袭击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、设施及分支机构等，为该整体性反恐怖防范重点目标的分目标，简称重点分目标。

3.5

电信互联网机房（楼） telecom Internet machine room (building)

为电信互联网设备提供运行环境的建筑物或场所。

3.6

互联网数据中心 internet date center

基于电信网和互联网，为集中式收集、存储、处理和发生数据的设施设备提供运行环境，网络条件，系统维护及相关服务的场所及配套设施。

3.7

周界 perimeter

机房局址建筑体或建筑群外部界面，局址范围包括独立院落的指独立院落周边外墙，局址为单体建筑物的指建筑物外立面及天顶，局址为合用建筑体（即机房局址与其他单位合用）的指建筑体周界及与其它单位交界处。

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 电信互联网运行维护单位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 重点分目标及其重要部位

6.1 确定原则

重点分目标由公安机关会同有关部门确定，报同级反恐怖工作领导机构（反恐办）备案。重点目标责任主体单位根据实际情况，将对国家安全、公共安全和人民生命财产安全有显著影响的部位确定为重点分目标的重要部位。

6.2 重点分目标

电信互联网反恐怖防范重点分目标主要有：

提供电信服务、互联网信息服务或政务信息服务的机楼、电信机房、数据中心，包含为上述提供支撑的配电系统、空调系统、网络管理监控中心、安防监控中心等。

6.3 重要部位

电信互联网反恐怖防范重点分目标的重要部位主要有：

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、空调主机室、网络管理监控室、安防监控室、消防监控室等。

7 常态反恐怖防范

7.1 人防

7.1.1 设置原则

人防设置应符合DB4401/T 10.1—2018中7.1.1的要求。

7.1.2 人防组织

7.1.2.1 应符合 DB4401/T 10.1—2018 中 7.1.2 的要求。

7.1.2.2 电信互联网运行维护单位应设置或确定承担与反恐怖防范任务相适应的反恐怖防范工作机构，明确第一责任人和责任部门，配备专（兼）职工作人员，负责反恐怖防范的具体工作。

7.1.2.3 电信互联网运行维护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、消防值守人员。

7.1.3 人防配置

电信互联网的人防配置应符合表1的要求。

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		安保部门兼任或独立	应设
4	联络员		指定联络员 1 名	应设
5	安保力量	技防岗位	重要技防系统设施管理维护	应设
6		固定岗位	机楼出入口、网络管理监控室、安防监控室	应设
7		巡查岗位	机房、周界、储油库、配电房、空调主机室、网络管理监控室、安防监控室等重要部位	应设
8		网管岗位	网络安全管理、网络管理监控	应设
9		机动岗位	备勤、周界	应设

7.1.4　人防管理

7.1.4.1　电信互联网运行维护单位应建立与反恐怖主义工作领导机构、公安机关及行业指导部门的工作联系，定期报告反恐怖防范措施落实情况。发现可疑人员、物品、信息安全隐患应立即向公安机关报告。发现违法犯罪行为，应当及时制止并报告公安机关，同时采取措施保护现场和相关信息记录。

7.1.4.2　电信互联网运行维护单位应加强人防管理：

a）　电信互联网运行维护单位负责领导、责任部门负责人应签订反恐怖防范目标责任书，重要岗位的从业人员应签订相应的反恐怖防范承诺书和工作保密承诺书；

b）　对重要岗位人员开展背景审查，建立人员档案并备案，确保用人安全；

c）　加强反恐怖防范教育宣传、开展应急技能训练和应急处突演练，提升人防技能；

d）　加强检查督导，开展制度体系实施与改进，提高人防效率；

e）　每 2 小时对机房、周界、储油库、配电房、空调主机室、网络管理监控室、安防监控室等重要部位巡查不少于 1 次；

f）　加强门卫与寄递物品管理、开展巡查与安检、技防系统的值守监看和运维，确保人防职责落实；

g）　应确保外部人员访问重点分目标前得到授权和审批，批准后由专人全程陪同和监督，限制和监控其活动范围，并登记在案和电子记录双重备案管理。

7.1.4.3　电信互联网运行维护单位应指定专职联络员，联络员应确保 24 小时通信畅通。联络员的配置和变更，应及时向反恐怖主义工作领导机构的办事机构和公安机关备案。

7.1.5　安保力量要求

7.1.5.1　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）　反恐怖防范专（兼）职工作人员应熟悉机楼、电信机房、数据中心等重点分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；

b）　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；

c）　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、消防值守人员等；

d） 电信互联网运行维护单位应根据有关规定，结合目标规模、人员数量、重点分目标和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。

7.1.5.2 常态安保力量配备原则如下：

a） 机楼出入口、网络管理监控室、安防监控室在岗安保力量不小于1人；

b） 网络安全管理在岗力量不少于1人；

c） 巡查岗位安保力量每组每班不少于2人；

d） 固定岗位、机动岗位安保力量可采用专兼职结合方式。

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、规章及有关标准的要求。

7.2.1.2 应纳入电信互联网建设工程建设总体规划，并应与新建或改建项目同步设计、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技术标准要求，并经检验或认证合格。

7.2.2 物防组成

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、行包寄存设施等。

7.2.3 物防配置

电信互联网的物防配置应符合表2的要求。

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	机楼与外界相通的出入口或所在院落与外界相通的出入口	应设
2		人车分离通道	机楼与外界相通的出入口或所在院落与外界相通的出入口	应设
3	实体防护设施	防盗安全门、金属防护门、防火安全门或防尾随联动互锁安全门	机房、网络管理监控室、安防监控室、储油库、配电房、空调主机室等重要部位出入口	应设
4		围墙或栅栏	机楼周界	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
6			网络管理监控室、安防监控室	应设
7		防盗保险柜、防盗保险箱	财务室	应设
8	个人应急防护装备	对讲机、强光手电、防护棍棒	保安员、安防监控室、门卫室、消防监控室	应设
9		毛巾、口罩、防护面罩	各工作区域	应设
10		防暴盾牌、钢叉	安防监控室或保安装备存放室、门卫室	应设
11		防暴头盔、防割（防刺）手套、防刺服	安防监控室或保安装备存放室	应设
12	公共应急防护装备及设施	防爆毯（含防爆围栏）	安防监控室或保安装备存放室	应设
13		应急报警器	安防监控室或门卫室	应设
14		灭火器材	各工作区域	应设
15	行包寄存设施		门卫室	应设

7.2.4 物防要求

7.2.4.1 应符合DB4401/T 10.1—2018中7.2.4的要求。

7.2.4.2 物防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） 机房及监控室应采用金属防盗防火安全门；

c） 应急报警器应符合GB 16796的要求；

d） 实体屏障的有效高度一般不低于1.8米。围墙高度不低于2.2米，顶部应设有防护装置，例如刺铁丝、刺刀圈等。

7.3 技防

7.3.1 建设原则

7.3.1.1 应符合国家、省、市的相关法律法规、规章及有关技术标准的要求。

7.3.1.2 应纳入电信互联网建设工程建设总体规划，并应与新建或改建项目同步设计、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。

7.3.1.4 技防设备设施的工程设计应采用主流和成熟的技术，可积极探索引用先进的技术，采用的技术宜符合数字化、网络化、智能化、一体化的要求，配置应结合建设项目初期、近期、远期的规模和容量设计；不易改扩建的基础设施宜按远期设计。

7.3.1.5 为提升遭受恐怖袭击的应急处置效率，应在规划设计建设环节增加发电车快速接入装置，并设置于便于接入的位置。

7.3.2 技防组成

电信互联网反恐怖防范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）安全管理系统、电子巡查系统、防爆安全检查系统、信息隔离控制系统（防火墙）等。

7.3.3 技防配置

电信互联网的技防配置应符合表3的要求。

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	机楼机房所在院落与外界相通的出入口	应设
3			机楼机房与外界相通的出入口	应设
4			机楼机房电梯轿厢内	应设
5			机房楼层的出入口、电梯厅	应设
6			机房所在楼层的主通道	应设
7			机房及其出入口	应设
8			安防监控室、网络管理监控室及其出入口	应设
9			机楼机房的配电房、空调主机室的出入口	应设

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
10	视频监控系统	摄像机	储油库的出入口	应设
11			门卫室	应设
12			停车库（场）及其主要通道和出入口	应设
13			电脑中心机房、财务室、贵重物品存放场所	应设
14		控制、记录、显示装置	安防监控室	应设
15	入侵和紧急报警系统	入侵探测（报警）器	重点分目标的周界	应设
16		紧急报警装置（一键报警）	安防监控室或门卫室	应设
17		报警控制器	安防监控室	应设
18		终端图像显示装置	安防监控室	宜设
19	出入口控制系统		机楼机房主要出入口	应设
20			安防监控室、网络管理监控室	应设
21			机楼机房的配电房、空调主机室	应设
22			储油库	应设
23	停车库（场）安全管理系统	停车库（场）管理系统	停车库（场）	应设
24		机动车号牌自动识别系统	停车库（场）	宜设
25	电子巡查系统		重点分目标的主要出入口和周界，储油库、门卫室、消防监控室、保安装备存放室、配电房、空调主机室、网络管理监控室、安防监控室等重要部位	应设
26	公共广播系统		区域全覆盖	应设
27	无线通信对讲指挥调度系统		区域全覆盖	应设
28	防爆安全检查系统	X 射线物品安检机	机楼出入口	宜设
29		通过式金属探测门	机楼出入口	宜设
30		手持式金属探测器	机楼出入口	应设
31		爆炸物探测仪	机楼出入口	宜设
32	通讯显示记录系统		服务、咨询电话、总机	宜设
33	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

电信互联网的反恐怖防范技防系统总体要求，应满足以下要求：

a）　系统应满足 DB4401/T 10.1—2018 中 7.3.4 的要求；

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。

7.3.4.2　安防监控中心

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） 安防监控中心宜采用二级设置，分别为电信互联网运行维护单位安防总监控中心、重点分目标安防监控分中心的管理架构；

c） 安防总监控中心接收、处理监控分中心发来的视频信息、报警信息、状态信息等，将处理后的报警信息、监控指令发往监控分中心；

d） 安防监控分中心接收、显示、记录、处理前端和各子系统发来的视频信息、报警信息、状态信息，与安防总监控中心进行通信，接受安防总监控中心的管理；

e） 安防监控中心内可根据需要整合相关技防系统功能；

f） 安防监控中心应能实时查看相关安防系统的工作状态；

g） 监控系统应接入管辖公安机关指挥部门、辖区派出所，做到技防系统资源共享；

h） 安防监控室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。

7.3.4.3 视频监控系统

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。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。

b） 视频监控系统应采用数字系统。

c） 视频信息应与公安机关联网。

d） 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。

e） 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。

f） 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。

g） 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（SVAC）。

h） 图像信号的传输、交换和控制应符合 GB/T 28181 的要求。

i） 图像信号的切换应具有手动和编程两种模式。

j） 图像信号的显示设备应采用 FHD（1920×1080）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（4096×216）以上分辨率的大屏设备。

k） 图像信号的存储：

1） 外界相通的出入口和其他重要部位在触发报警时的单路图像应具有 16CIF(1920×1080)或以上图像分辨率；

2） 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；

3） 单路显示基本帧率不小于 25fps；

4） 视频信息存储时间不少于 90 天。

注1：单路视频编码率为352×288=512(kbps)，为1CIF，其他分辨率的单路视频编码率为水平与垂直方向像素分辨率的乘积，除以（352×288），得到的商作为CIF的倍数，如4CIF的编码率为2048kbps。

注 2：存储时可结合视频移动等技术做帧率调整，以减少存储空间的需求。

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 16796、GB/T 32581、GB/T 36546、GB 50394、GA/T 368 等入侵和紧急报警系统相关标准的要求；

b） 入侵报警装置应有明显的警告标志；

c） 入侵和紧急报警系统应与视频监控系统联动，报警响应时间应不大于 2 秒；

d） 入侵和紧急报警系统信息本地保存时间应不少于 180 天，并具备与公安机关联动的接口；

e） 入侵和紧急报警系统备用电源应满足至少 24 小时正常工作的需要。

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/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；

c） 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；

d） 出入口控制系统授权等级宜根据运行维护单位对安全防范的总体要求进行设定。

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） 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） 电子巡查系统可独立设置，也可基于出入口控制系统组合设置；

d） 巡查路线应能根据安全管理的需求进行调整，并覆盖重要部位；

电子巡查系统可复用出入口控制系统相关设备实现在线巡查管理功能。

7.3.4.7 公共广播系统

公共广播系统应符合以下要求：

a） 公共广播系统应符合 GB 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。

7.3.4.8 无线通信对讲指挥调度系统

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、技防系统管理人员、巡查岗位人员、机动岗位人员、电力维护人员、消防岗位人员等用户之间的通信手段。

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

7.3.6.1　技防系统应用管理和维护保养应符合国家、省、市和行业等有关要求。
7.3.6.2　电信互联网运行维护单位应制定技防系统管理制度，建立运行维护保障的长效机制，设置专人负责系统日常管理工作，每年定期进行设备设施的检测、维护、保养。
7.3.6.3　技防系统应确保有人员值班，值班人员应培训上岗，掌握系统运行维护的基本技能。

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　制度防组成

制度防组成包括管理标准、工作标准和技术标准等。

7.4.3　管理标准

7.4.3.1　制定重点分目标管理制度，制定反恐怖防范领导小组管理制度，明确层级管理的联动要求。
7.4.3.2　制定反恐怖袭击专项应急预案、反恐通信保障专项预案、通信网络和设施安全管理制度、信息安全保护管理制度，管理标准要求见附录A。
7.4.3.3　制定反恐怖防范责任承诺制度，明确反恐怖防范目标责任书和承诺书的签订要求。
7.4.3.4　应对反恐怖防范管理活动中的主要管理内容建立反恐怖防范管理制度，应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的反恐怖防范管理制度体系。
7.4.3.5　应指定或授权专门的部门或人员负责反恐怖防范管理制度的制定，反恐怖防范管理制度应通过正式、有效的方式发布，并进行版本控制。

7.4.4　工作标准

7.4.4.1　制定电信互联网运行维护单位责任领导、责任部门的正（副）职、联系员的职责和权限。
7.4.4.2　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。
7.4.4.3　制定详细的考核条件和奖惩办法，明确检查考核部门和时间要求，明确考核程序和考核办法，应有考核记录。

7.4.5　技术标准

7.4.5.1　配备反恐怖防范工作中所涉及到物防、技防等相关的国家、行业和地方标准。
7.4.5.2　对于尚未有国家、行业和地方标准的技术事项，应制定企业标准。

8　非常态反恐怖防范

8.1　非常态反恐怖防范启动

8.1.1　根据反恐怖主义工作领导机构和公安机关发布的恐怖威胁预警，进入非常态反恐怖防范。
8.1.2　电信互联网运行维护单位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

8.2.1 电信互联网运行维护单位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。

8.2.2 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

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） 电信互联网运行维护单位安保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） 监控中心不得少于2人，24小时监视；
f） 对机楼机房出入口进行控制，对重要部位加强巡查、值守；
g） 保持通信联络畅通，及时通报信息，做好沟通、协调和信息报送；
h） 联系管辖公安机关指导防范工作，每天主动向管辖公安机关报告防范工作落实情况，重要情况应及时报告；
i） 根据反恐怖主义工作领导机构及其办事机构、公安机关和行业指导部门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） 电信互联网运行维护单位主管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70%以上；
c） 重要部位巡查频率较常态提高50%；
d） 巡查人员可对区域内可疑人员、车辆、物品进行安全检查；
e） 联系管辖公安机关派员指导防范工作，每半天向管辖公安机关报告防范工作落实情况，重要情况应及时报告。

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） 电信互联网运行维护单位主要领导及分管领导共同带班组织防范工作；
b） 在常态安保力量的基础上增派100%以上；
c） 重要部位巡查频率较常态提高1倍；重点分目标出入口派员加强值守；
d） 主要出入口设置障碍，控制出入口，严禁无关人员、车辆进入；
e） 联系管辖公安机关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） 责任主体主要领导、分管领导及领导班子其他成员共同带班组织防范工作；
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） 封闭重点分目标出入口，严密监视内外动态；
f） 对目标区域进行全面、细致检查；
g） 危急情况下对相关要害部位、设施、场所实施关闭，暂停相关活动。

8.4 非常态反恐怖防范的人防、物防和技防配置

电信互联网运行维护单位应有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 应急处置的总体要求

9.1.1 应符合 DB4401/T 10.1—2018 中第 9 章相关规定。

9.1.2 电信互联网运行维护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。

9.2 反恐应急

9.2.1 电信互联网运行维护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。

9.2.2 在反恐防范工作中，电信互联网运行维护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。

9.2.3 电信互联网运行维护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。

9.3 反恐应急演练

9.3.1 电信互联网运行维护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”。

9.3.2 电信互联网运行维护单位每年应至少组织一次反恐应急综合演练，对重点分目标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。

10 监督、检查

10.1 应符合 DB4401/T10.1—2018 第 10 章的要求。

10.2 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。

10.3　电信互联网运行维护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一次，不定期检查根据实际工作需要开展。

10.4　电信互联网运行维护单位每年应对其反恐怖防范系统开展至少一次的自我评价，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。电信互联网运行维护单位应及时向公安机关递交自我评价报告。

10.5　反恐怖防范工作检查实施按附录 B 规定进行。

附 录 A
（规范性附录）
管理标准要求

A.1 范围

A.1.1 电信互联网反恐怖防范各项管理标准的管理要求按DB4401/T 10.1—2018的附录A规定进行。

A.1.2 本附录规定了反恐怖袭击专项应急预案、反恐通信保障专项预案、通信网络和设施安全管理制度、信息安全保护管理制度的管理要求。

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) 制度的管理目的（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 反恐怖袭击专项应急预案

重点目标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.3.2 反恐通信保障专项预案

重点目标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.3.3 通信网络和设施安全管理制度

重点目标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.3.4 信息安全保护管理制度

重点目标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。

附 录 B
（规范性附录）
反恐怖防范工作检查实施

B.1 概述

电信互联网反恐怖防范工作检查的实施按DB4401/T 10.1—2018的附录C规定进行。

B.2 检查表格

检查表格应包括依据标准的条款，检查内容概要，检查过程记录和项目结论。格式参见表B.1。

表 B.1 检查表格

序号	标准条款		内容概要	检查记录	项目结论
1	6 重点分目标及其重要部位		重点分目标和重要部位分布图/列表是否清晰、完整，是否及时报备		
2	7.1 人防	7.1.3	是否按要求建立了专责、健全的反恐怖防范工作机构并在主要负责人的领导下开展工作，做到分工明确，责任落实		
3			是否按要求配备了技防岗位、固定岗位、巡查岗位、网管岗位和机动岗位等安保力量		
4		7.1.4.1	与反恐怖主义工作领导机构、公安机关及电信互联网行业指导部门的工作联系途径是否有效		
5		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		
6			是否建立重要岗位人员档案并备案，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			是否对外部人员的访问进行授权和审批，全程专人陪同和监督并且双重备案管理，查看相关记录		
9			是否对寄递物品进行验视、签收和登记管理，检查记录		
10			是否按有效的路径和方式开展巡查，检查记录		
11			是否在正确的位置正确使用安检设备开展安检工作		
12			视频监控系统的值班监看是否到位		
13			检查教育培训计划和教育培训记录		
14			检查训练计划和训练记录		
15			检查演练计划和演练记录		
16			是否开展自我检查督导和反恐怖防范体系自我评价工作，查看相关记录		
17		7.1.4.3	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		
18		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，查看备案回执		
19			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		
20			是否按配置原则配置常态安保力量		
21			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		
22			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		
23			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		
24			年内是否存在网络失控情况		

表 B.1　检查表格（续）

序号	标准条款		内容概要	检查记录	项目结论
25	7.2 物防	7.2.3	机楼或所在院落与外界相通的出入口是否设置了机动车阻挡装置		
26			机楼或所在院落与外界相通的出入口是否设置人车分离通道		
27			机房、网络管理监控室、安防监控室、储油库、配电房、空调主机室等重要部位出入口有否设立防盗安全门等实体防护设施		
28			财务室有否设立防盗保险柜或防盗保险箱		
29			机楼周界是否设置围墙或栅栏		
30			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、安防监控室是否设置了栅栏		
31			是否按实际需要配备了对讲机、强光手电、防护棍棒、毛巾、口罩、防护面罩、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		
32			是否按实际需要配备了防爆毯和防爆围栏等公共应急防护装备		
33			安防监控室或门卫室是否已按要求设置了应急警报器		
34			各工作区域是否按要求设置了灭火器材		
35			行包寄存设施是否设置在门卫室		
36			其它需要设置的物防设施		
37		7.2.4	机房及监控室是否采用金属防盗防火安全门		
38			实体屏障的有效高度是否满足要求		
39			实体屏障的顶部是否设有防护装置		
40			是否建立设备设施台帐和档案，信息是否准确、完整，是否对设备设施制定操作规程		
41			是否存在失效设备设施，是否对正常使用周期内失效的设备设施进行失效原因分析并制定纠正和预防措施		

表 B.1　检查表格（续）

序号	标准条款		内容概要	检查记录	项目结论
42	7.3 技防	7.3.3	是否已按要求设置了安防监控室，安防监控室是否设有控制、记录、显示等装置		
43			摄像机是否已覆盖机楼机房所在院落与外界相通的出入口、机楼机房与外界相通的出入口、机楼机房电梯轿厢内、机房楼层的出入口和电梯厅、机房所在楼层的主通道、机房及其出入口、安防监控室和网络管理监控室及其出入口、机楼机房的配电房和空调主机室的出入口、储油库的出入口、门卫室、停车库（场）及其主要通道和出入口、电脑中心机房、财务室、贵重物品存放场所等区域		
44			入侵探测（报警）器是否已覆盖重点分目标的周界		
45			紧急报警装置（一键报警）是否已设置在安防监控室或门卫室		
46			报警控制器是否已设置在安防监控室		
47			出入口控制系统是否已设置在机楼机房主要出入口、安防监控室、网络管理监控室、机楼机房的配电房和空调主机室、储油库		
48			停车库（场）是否设置停车库（场）管理系统		
49			重点分目标出入口和周界，储油库、门卫室、消防监控室、保安装备存放室、配电房、空调主机室、网络管理监控室、安防监控室等重要部位是否设置了电子巡查系统		
50			公共广播系统是否已区域全覆盖		
51			无线通信对讲指挥调度系统是否已安装并做到区域全覆盖		
52			机楼出入口是否设置了手持式金属探测器		
53			是否配置了信息隔离控制系统（防火墙）		
54			其它需要设置的技防设施		
55		7.3.4	报警系统信息本地保存时间是否不少于 180 天，并具备与公安机关联动的接口		
56			视频录像保存时间是否不少于 90 天		
57			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		
58			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 小时正常工作的需要		
59			安防监控中心设置是否符合要求		
60			视频监控系统设置是否符合要求		
61			入侵和紧急报警子系统设置是否符合要求		
62			出入口控制系统设置是否符合要求		
63			电子巡查系统设置是否符合要求		
64			公共广播系统设置是否符合要求		
65			无线通信对讲指挥调度系统设置是否符合要求		
66		7.3.5	系统检验与验收是否符合要求		
67		7.3.6	运行维护及保养是否符合要求，是否有技防系统的总台帐、各系统的设备设施台帐、系统操作手册（使用、维护和保养），并建立系统管理档案		

表 B.1　检查表格（续）

序号	标准条款		内容概要	检查记录	项目结论
68	7.4 制度防	7.4.1	是否制定了可量化考核和可实现的防范工作目标，是否与指导方针与总体目标一致		
69			是否制定了人防组织和配置的架构图，并明确责任领导的管理职责和责任部门的工作职责。是否指定专人负责反恐怖防范制度管理工作		
70		7.4.1 7.4.3	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、门卫与寄递物品管理制度、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、应急管理制度等		
71		7.4.3	是否按要求制定了重点分目标管理制度、反恐怖防范领导小组管理制度、反恐怖袭击专项应急预案、反恐通信保障专项预案、通信网络和设施安全管理制度，信息安全保护管理制度、反恐怖防范责任承诺制度		
72			是否有指定或授权专门的部门或人员负责反恐怖防范管理制度的制定		
73		7.4.1 7.4.4	工作标准配置是否符合要求		
74		7.4.1 7.4.5	技术标准配置是否符合要求		
75	其它防范管理	8	是否按要求制定了各级非常态反恐怖防范应对措施		
76		9.1	是否制定了应急预案		
77			应急预案的内容是否全面		
78		9.2	是否有组建应急处置队伍并建立有效增援保障措施		
79		9.3	是否按规定开展应急预案的演练		
80		10	是否定期开展自我评价并向公安机关递交自我评价报告		
81			是否对反恐怖防范工作中存在的问题实施持续改进		
82		DB4401/T 10.1—2018 附录 A 中 A.3	专项经费是否符合实际防范工作需要		
83			情报信息管理是否符合要求		
84			恐怖威胁预警是否得到快速有效响应		
85			是否开展恐怖威胁风险评估工作		
86			是否建立有效联动配合机制		

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] 《中华人民共和国网络安全法》 中华人民共和国主席令 第五十三号
[4] 《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
[5] 《保安服务管理条例》 中华人民共和国国务院令 第564号
[6] 《中华人民共和国电信条例》 中华人民共和国国务院令 第666号
[7] 《电信和互联网用户个人信息保护规定》 工业和信息化部令 第24号
[8] 《广东省安全技术防范管理条例》 广东省人大常委会公告第133号
[9] 《广东省安全技术防范管理实施办法》 广东省人民政府[2017]238号
[10] 《广东省公安厅关于<广东省安全技术防范管理实施办法>的操作细则》 广东省公安厅[2018]