

ICS号 35.240.01
CCS号 A90

团体标准

T/HSPA XXXX-XXXX

监狱安防系统运维服务标准

Prison security system operation and maintenance service standards

(征求意见稿)

2026-XX-XX发布

XXXX-XX-XX实施

湖北省安全技术防范行业协会 发布

目 录

前言	I
1 总则	1
2 规范性引用文件	1
3 术语和定义	2
4 业务架构	2
4.1 总体架构	3
4.2 监狱安防系统运行维护服务	3
4.3 监狱安防系统运行维护管理	4
4.4 监狱安防系统标准规范体系	5
4.5 监狱安防系统安全保障体系	5
5 运行维护服务对象	5
5.1 总述	5
5.2 安全保障类	5
5.3 狱务实战类	6
5.4 基础支撑类	6
5.5 信息应用系统	7
6 运行维护服务内容	7
6.1 总述	7
6.2 安全保障及狱务实战类软硬件运维要求	7
6.3 计算机网络子系统运维要求	10
6.4 综合布线子系统运维	11
6.5 机房及配套子系统运维	12
6.6 数据备份子系统运维	12
6.7 信息应用系统运维	13
6.8 运维服务台	17
6.9 事件管理	17
6.10 问题管理	18
6.11 配置管理	18
6.12 变更管理	19
6.13 发布管理	19
6.14 服务级别管理	19
6.15 能力管理	19
6.16 可用性管理	20
6.17 服务持续性管理	20
6.18 知识管理	20
6.19 资源库管理	20
6.20 备品备件管理	21
6.21 文档管理	21
6.22 资产管理	22
6.23 综合管理	23
6.24 应急保障	23
7 运行维护服务方法	25
7.1 安全保障类与狱务实战类运维服务方法	25
7.2 信息系统基础设施运行维护服务方法	27
7.3 信息应用系统运行维护服务方法	31

8 运行维护技术平台	31
8.1 智能监控	31
8.2 视频质量监测	32
8.3 管理与分析	32
8.4 大屏展示	34
8.5 云服务平台管理	34
8.6 机房动环监控	35
8.7 性能指标	36
9 运行维护队伍和组织	36
9.1 队伍与人员	36
9.2 运行维护组织	37
10 运行维护经费	38
10.1 基本要求	38
10.2 年度硬件运行维护经费	38
10.3 年度软件运行维护经费	38
10.4 运行维护设计经费	38
11 运行维护管理指标	39
11.1 总体指标	39
11.2 运行维护管理指标的定制	39
11.3 内容信息服务的运行维护管理指标	39
12 运行维护考核办法	39
12.1 运行维护考核办法	40
12.2 管理要求	40
12.3 工作要求	40
12.4 考核要求	41
13 运维内容及运维服务评价方法	41
13.1 一般要求	41
附录A（资料性）运维内容及运维服务相关用表	42
A-1 监狱维保人员考核表	42
A-2 信息化安防系统故障处理单	43
A-3 信息化安防系统维保服务评价表	44
A-4 项目运维月报样表	45
A-5 参考考核指标	46
参考文献	52

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。

本文件编制组经广泛调查研究，认真总结实践经验，并在广泛征求意见的基础上，编制本文件。

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。

本文件由湖北省安全技术防范行业协会归口。

本文件主要起草单位：武汉警官职业学院、悠锋科技有限公司、湖北省安全技术防范行业协会、湖北省司法厅。

本文件起草单位：达明科技股份有限公司、湖北朔望智能工程有限公司、莱讯通信（深圳）有限公司、乐锋智慧（深圳）科技有限公司、湖北省监狱管理局、湖北省戒毒管理局、湖北省沙洋江北监狱、湖北省沙洋广华监狱、湖北省沙洋汉津监狱、湖北省江汉监狱、湖北省宜昌监狱、湖北省未成年犯管教所、湖北邮电规划设计有限公司。

本文件主要起草人：陈风华、黄超民、余莉琪、陈雪松、王珏、李祖义、黄远军、余绍军、谭庆芳、程静、宋武、肖庆、陈昊、金导航、夏峻峰、程小攀、李永华、陈巍、王堃、黄辉、江威、冯树生、张波、廖强平、周小健、王庆、张新宇、何勇、郑凯豪、张楠、郭志刚、胡操、李磊、罗骁、宋文海、熊焰。

本文件主要审查人：曾松鸣。

监狱安防系统运维服务标准

1 总则

为实现监狱安防系统运行维护的规范性、安全性和及时性，确保各安防类电子信息系统与设备运行的稳定可靠，特制订本文件以确定各项运维工作的标准流程和相关岗位设置等，运维人员在制度和流程的规范和约束下协同操作。

本文件规定了监狱安防系统运行维护的总体框架、运行维护服务对象、运行维护服务内容、运行维护服务方法、运行维护技术平台、运行维护队伍和组织、运行维护经费、运行维护管理指标以及运行维护管理考核办法的要求。

本文件适用于监狱安防系统的运行维护服务工作和运行维护管理工作。安防系统的运行维护除应符合本文件外，还应符合国家现行有关标准的规定。

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 28827.1-2022 信息技术服务 运行维护 第1部分：通用要求

GB/T 51314-2018 数据中心基础设施运行维护标准

GB 50348-2018 安全防范工程技术标准

GB/T 50312-2016 综合布线系统工程验收规范

GB/T 33745-2025 物联网 术语

GB/T 35295-2017 信息技术 大数据 术语

GB/T 14394-2008 计算机软件可靠性和可维护性管理

GB/T 20988-2025 网络安全技术 信息系统灾难恢复规范

YD/T 1627-2019 通信网络运行维护服务规范

GA/T 70-2014 安全防范工程建设与维护保养费用预算编制办法

ISO/IEC 20000 IT服务管理体系

建标139-2010 监狱建设标准

SF/T 0088-2021 监狱信息化运行维护规范

SF/T 0082-2020 智慧矫正 远程视频督察系统规范

司法部《司法行政视频监控联网编码规则及视频图像命名规范》

3 术语和定义

GB/T 28827.1—2012、GB/T 33745—2017、GB/T 35295—2017界定的以及下列术语和定义适用于本文。

3.1

运行维护 operation and maintenance

采用信息技术手段及方法，对信息技术资产和环境进行技术保障和安全维护活动。 注：运行维护通常包括运行维护服务和运行维护管理。

运行维护可简称“运维”。

3.2

运行维护服务对象 operation and maintenance service object

运行维护服务的受体。 注：运行维护服务对象通常指机房环境、网络通信、硬件、软件、数据和应用等。

3.3

AB门出入监管理系统 AB Gate Inmate Entry and Exit Management System

监狱出入口设置的两道联动门禁系统（A门、B门），通过人脸识别、车底扫描、生命探测等技术实现人员/车辆进出监的双重验证与管控系统。

3.4

周界防范系统 Perimeter Security System

在监狱物理周界（围墙、铁丝网等）部署的光纤入侵报警、振动传感等设备，用于实时监测非法入侵行为的安防系统。

3.5

监外押解就医系统 Out-of-Prison Escort for Medical Treatment System

用于监狱罪犯外出押解、就医过程中，通过便携终端、定位技术实现全程监控与数据回传的系统。

4 业务架构

监狱安防系统运行维护主要包括监狱安防系统运行维护服务和监狱安防系统运行维护管理。运行维护服务是采用信息技术手段和方法，依据监狱安防系统运行维护实际需要的服务级别协议（SLA），对信息系统基础设施和信息应用系统等提供综合服务。监狱安防系统运行维护服务可采用自有人员与外包服务、辅助警务相结合等多种机制进行。

运维人员需通过监狱属地公安部门的无犯罪记录审查、无直系亲属在押审查，并签订《保密承诺书》。外包服务单位需具备涉密信息系统集成资质，外包人员的活动范围需要符合《中华人民共和国监狱法》第四十七条相关要求。

运行维护管理是对运行维护服务过程涉及的组织、队伍、经费和服务质量等进行的决策和控制活动。

4.1 总体架构

图1规定了监狱安防系统业务架构，包括标准规范体系模块、安全保障体系模块、运维管理体系模块、基础设施模块、监狱大数据模块、共享交换系统、综合应用模块、应用门户模块，各模块包括但不限于以下内容：

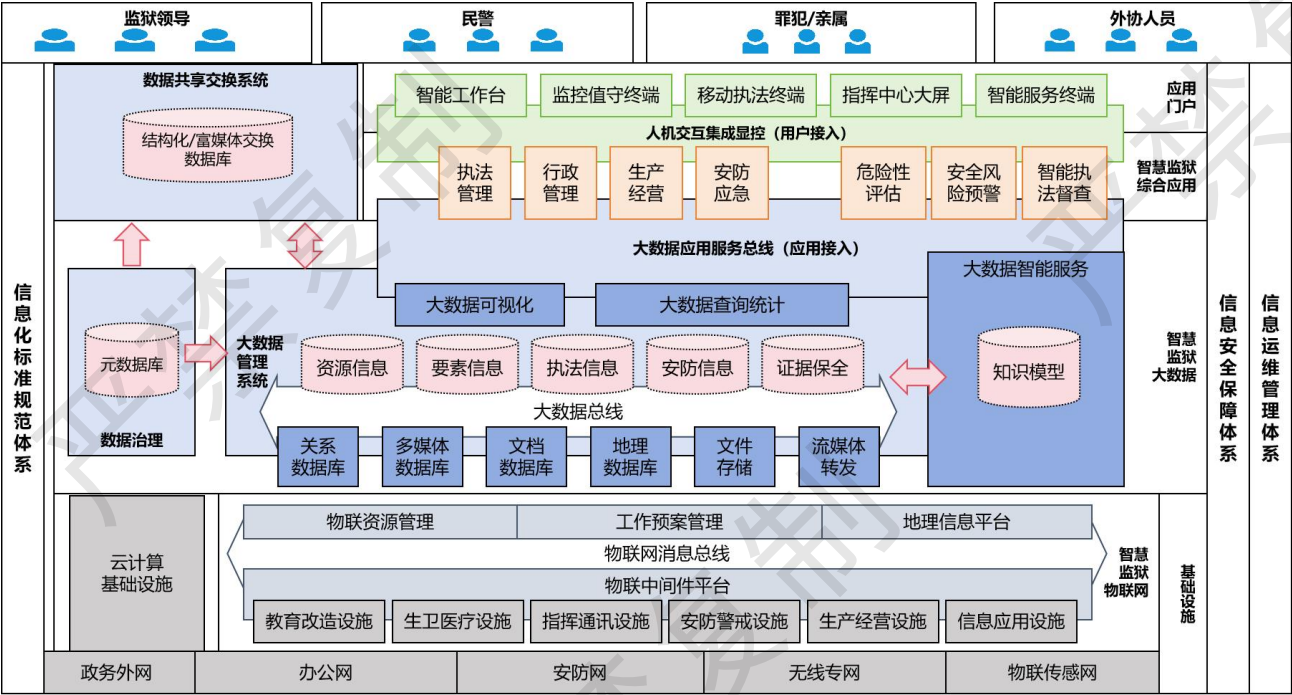


图1 监狱安防系统业务架构

4.2 监狱安防系统运行维护服务

A) 监狱安防系统运行维护服务主要包括运行维护服务对象、运行维护服务内容、运行维护服务方法和运行维护技术平台。

B) 运行维护服务对象：包括但不限于安全保障类、狱务实战类、基础支撑类和信息应用系统四大类运维对象，如下表所示：

表1 运维服务范围及对象清单

序号	范围类别	对象	备注
1	安全保障类	音视频监控系统	含软硬件运维
2		门禁控制系统	含软硬件运维
3		AB门出入监管理系统	含软硬件运维
4		周界防范系统	含软硬件运维
5		电子巡更系统	含软硬件运维
6		报警系统	含软硬件运维
7		监仓对讲系统	含软硬件运维
8		智能侦测分析系统	含软硬件运维
9		监外押解就医系统	含软硬件运维
10		数字广播系统	含软硬件运维
11		应急指挥中心	含软硬件运维

序号	范围类别	对象	备注
12		视频会议系统	含软硬件运维
13		武警联动系统	含软硬件运维
14		融合通信	含软硬件运维
15	狱务实战类	智能卡系统	含软硬件运维
16		会见管理系统	含软硬件运维
17		亲情电话系统	含软硬件运维
18		罪犯点名系统	含软硬件运维
19		信息公开系统	含软硬件运维
20		高清电教系统	含软硬件运维
21	基础支撑类	计算机网络系统	含软硬件运维
22		综合布线系统	含软硬件运维
23		机房及配套工程	含软硬件运维
24		备份系统	含软硬件运维
25	信息应用系统	应急指挥平台	软件运维
26		安防类配套软件	软件运维
27		办公自动化（OA）系统	软件运维

C) 运行维护服务内容：包括硬件运行维护及配套服务、软件运行维护及配套服务、网络安全运维及配套服务和应急保障等类别；

D) 运行维护服务方法：是对运行维护服务对象的具体运行维护手段和措施。包括但不限于安全保障类、狱务实战类、基础支撑类和信息应用系统运行维护服务方法；

E) 运行维护技术平台：是依托服务流程平台通过运维手段和工具建设实现监狱系统的各类信息化资源统一管理和运行监控、各数据中心机房远程可视化监控管理、全网骨干网络的实时监控。

F) 建立系统健康评估体系，用定性、定量的方式在指定的时间或所需的时间点进行全局或局部的评估，形成评估报告，作为运维的重要参考依据。

G) 通过技术手段和工具将运行维护服务内容和运行维护知识管理过程等固化，并开展主动性运行维护工作。包括但不限于运维管理系统、资源监控管理软件、资源可视化软件、IT服务管理软件、业务保障管理系统、IT资产管理软件、视频质量诊断系统。

4.3 监狱安防系统运行维护管理

监狱安防系统运行维护管理主要包括运行维护组织和队伍、运行维护经费、运行维护管理指标和运行维护考核办法。内容如下：

A) 运行维护组织和队伍：包括省级和监狱二级组织机构以及运行维护服务提供者、运行维护服务使用者和运行维护服务管理者三类角色；

B) 运维管理制度：采用管理制度规范运维的操作方法和流程，各单位可以根据自己的实际情况，在符合标准的前提下制定与自身特点相适应的具体操作规程；

C) 运行维护经费：主要包括年度硬件运行维护经费、年度软件运行维护经费和运行维护设计经费，以持续保障监狱安防系统运行维护服务的开展；

D) 运行维护管理指标：是监狱安防系统运行维护管理所需的各项指标；

E) 运行维护考核办法：是保障监狱安防系统运行维护所需的各项考核办法。

4.4 监狱安防系统标准规范体系

监狱安防系统标准规范体系包括监狱安防系统所需的各类标准和规范。

4.5 监狱安防系统安全保障体系

监狱安防系统安全保障体系为监狱安防系统提供各类安全技术保障。

5 运行维护服务对象

5.1 总述

安防系统运维的目的是保障运行维护服务对象在指定的时间内正常、有效运行。

运维服务对象通常指机房环境、网络通信、硬件、传输系统（包括线缆）、软件、数据和应用等。可以分为以下4个大类：

- A) 安全保障类；
- B) 狱务实战类；
- C) 基础支撑类；
- D) 信息应用系统。

5.2 安全保障类

安全保障类运维对象主要包括以下内容：

A) 音视频监控系统：包括但不限于：摄像头、云存储主机、网络设备、存储设备、显示设备、管理平台以及电源与环境设备、线缆等。

B) 门禁控制系统：包括但不限于：门禁控制器、读卡器、刷卡器、指纹识别器、人脸识别设备、线缆等。

C) AB门出入监管理系统：包括但不限于：A、B两道门、门禁控制器、读卡器、刷卡器、指纹识别器、人脸识别设备、报警装置、一体式自助登记终端、十字滚闸门、车底扫描系统、生命探测仪、车辆识别单元、车牌识别管理平台及软件、线缆等。

D) 周界防范系统：包括但不限于：光纤入侵报警器、光学模块、振动传感光缆、引导传输光缆、智能周界安防系统管理软件、线缆等。

E) 电子巡更系统：包括但不限于：巡更控制器、巡更读卡器、二维码、手持终端、电源等。

F) 报警系统：包括但不限于：手动报警按钮、红外双鉴探测器、声光报警器、红外光栅探测器、总线延伸模块、单防区触发器扩展模块、8防区触发器扩展模块、总线式网络报警主机、总线式分控报警主机、读卡器、控制器、控制键盘、LED警示灯、报警管理软件、线缆等。

G) 监仓对讲系统：包括但不限于：智能监仓对讲系统平台、IP网络高级对讲主机、IP网络一级对讲主机、IP网络金属防爆对讲分机、IP网络专用对讲分机、集中供电电源、线缆等。

H) 智能侦测分析系统：包括但不限于：人脸识别系统、图像分析GPU服务器等。

I) 监外押解就医系统：包括但不限于：外出押解便携箱、监外就医便携设备等。

J) 数字广播系统：包括但不限于：数码调谐器、DVD播放器、前置放大器、网络音频采集器、IP网络广播控制主机（含软件）、IP网络广播消防报警主机、IP网络广播电源控制器、IP网络寻呼话筒、IP网络监听音箱、吸顶喇叭、壁挂喇叭、草坪音箱、IP网络广播功放机、网络适配器、线缆等。

K) 应急指挥中心：包括但不限于：音频扩声系统、视频显示系统、视频会议系统、工作站、操作台、机架式一体化UPS、音视频切换及集中控制系统、线缆等。

L) 行政视频会议室：包括但不限于：音频扩声系统、视频显示系统、视频会议系统、工作站、操作台、机架式一体化UPS、音视频切换及集中控制系统、线缆等。

M) 武警联动系统：包括但不限于：管理客户端设备、无线对讲设备、可视对讲分机、联动终端设备、线缆等。

N) 融合通信：包括但不限于融合通信服务器、触摸屏调度台、融合通信网关、线缆等。

5.3 狱务实战类

狱务实战类运维对象主要包括以下内容：

A) 智能卡系统：包括但不限于：智能卡平台、服务器、数据库、管理电脑、卡务系统、发卡器、CPU感应卡、卡证打印机、线缆等。

B) 会见管理系统：包括但不限于：会见系统管理软件、对讲电话、监听话机、管理电脑、发卡器、排队叫号8字显示屏、通道显示屏、呼叫器、自助登记查询一体机、二代证读卡器、摄像头、打印机、智能储物柜、三辊闸、CPU读卡器、开门按钮、门禁控制器、人脸识别摄像机、会听话机、监听话机、功放、喇叭、信息发布显示屏、摄像机、音视频存储、双备份集成电源、语音网关、IPPBX、会见终端、线缆等。

C) 亲情电话系统：包括但不限于：系统软件、IPPBX、语音网关、CPU读卡器、话机、监听器、音视频同步摄像机、中继网关/IMS接入模块、发卡器（读写器）、音视频存储、摄像机电源及电源线缆、传输线缆等。

D) 罪犯点名系统：包括但不限于：点名系统管理平台、壁挂式触摸一体机、移动手持终端、线缆等。

E) 信息公开系统：包括但不限于：信息发布管理平台及软件、高清视频直播编码器、高清播放器、触摸查询机、显示屏、线缆等。

F) 高清电教系统：包括但不限于：高清电教平台、有线电视顶盒、高清视音频编码器、蓝光播放器、流媒体服务器、录像制作服务器、点播服务器、网络机顶盒、活动室电教终端、音箱、线缆等。

5.4 基础支撑类

基础支撑类运维对象主要包括以下内容：

A) 计算机网络系统：包括但不限于：计算机、服务器、数据库操作系统、交换机、路由

器、防火墙、有线及无线网络等。

B) 综合布线子系统：包括但不限于：线缆、连接器件、跳线、面板、配线架、箱柜、管理等。

C) 机房及配套系统：包括但不限于：供配电、UPS、空调、动环监控、消防、防雷接地等。

D) 数据备份系统：负责对监狱安防等业务数据、配置信息及日志进行定期备份与恢复管理，包括但不限于数据库、应用系统、网络设备配置文件等，确保数据的完整性、可用性和安全性。

5.5 信息应用系统

信息应用系统是根据监狱业务和特点建设的各类应用软件，包括但不限于应急指挥平台、安防类配套软件、办公自动化（OA、视频会议）系统等。

信息化公共应用平台（如OA、即时通讯平台等）及其他公共硬件设施（如电脑、打印机、扫描仪等）由信息化系统运维服务进行支撑，本文件仅对安防类相关信息应用系统的运维作出相应规范要求。

- A) 应急指挥平台；
- B) 安防类配套软件；
- C) 办公自动化（OA、视频会议）系统等。

6 运行维护服务内容

6.1 总述

- A) 运维分为运行（值守、文档等）和维护（巡检、评估等）两部分。
- B) 当运维中发现隐患和故障时，应交由系统维修进行处置。
- C) 当系统需要局部整理、升级、更改时，宜在充分准备后，启动系统整改工程。
- D) 在系统还处于建设阶段，未交付运维时，运维可参与建设，提前熟悉系统，并提供对运维有益的意见。
- E) 运维的全生命周期如下图所示。

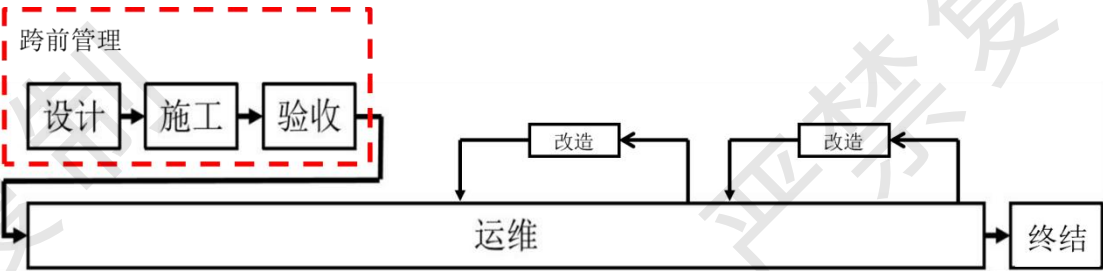


图2 安防系统运维的全生命周期过程图

6.2 安全保障及狱务实战类软硬件运维要求

- A) 此两类系统均包含前、后端硬件及平台软件，对应运维服务内容如下表所示：

表2 运维服务内容清单

序号	类别	运维内容	备注
1	安全保障类与狱务实战类	前端硬件	
2		服务器主机	
3		网络设备	
4		存储设备	
5		显示设备	
6		管理平台	
7		电源与环境设备	

B) 具体运维服务应包括以下内容：

1) 前端硬件

(1) 维护内容：

清洁与检查：定期清洁前端硬件和外壳，避免灰尘、污渍影响监控画面质量。

网络连接检查：确保前端硬件与网络的连接稳定，避免因网络问题导致视频中断。

固件升级：定期检查前端硬件的固件版本，及时升级以修复漏洞或优化性能。

故障排查：如发现前端硬件画面模糊、黑屏、无信号等问题，及时检查电源、网络、镜头或传感器是否正常。

配置优化：根据实际需求调整前端硬件的参数（如分辨率、帧率、白平衡等），确保效果最佳。

日常巡检：检查前端硬件的运行状态、网络带宽、存储空间等，确保设备正常工作。

(2) 注意事项：

避免直接用手触摸镜头，使用专业清洁工具。

定期检查摄像头的物理位置是否安全，避免被遮挡或破坏。

2) 服务器主机

(1) 维护内容：

存储容量检查：定期监控云存储的使用情况，清理过期或无用的视频数据，确保存储空间充足。

数据备份与恢复：确保云存储的数据备份机制正常运行，定期测试数据恢复功能。

服务器健康状态检查：监控云存储主机的CPU、内存、硬盘等硬件资源的使用情况，避免因资源不足导致性能下降。

网络连接优化：确保云存储主机与摄像头、管理平台的网络连接稳定，避免因带宽不足导致视频卡顿。

固件与软件升级：及时升级云存储主机的固件和相关软件，修复潜在的安全漏洞或性能问题。

数据安全检查：确保云存储的数据加密和访问控制功能正常，防止数据泄露或被篡改。

冗余配置检查：检查云存储主机的冗余配置（如双机热备或分布式存储），确保在单点故障时系统仍能正常运行。

日常巡检：定期检查云存储主机的运行日志，排查异常告警。

(2) 注意事项：

避免随意删除存储数据，确保数据完整性和可用性。

期测试云存储的扩展能力，以应对未来可能的存储需求增长。

3) 网络设备

(1) 维护内容：

网络连接检查：确保前端硬件、服务器主机与其他设备之间的网络连接正常。

带宽优化：根据监控视频的分辨率和码率，合理分配网络带宽，避免网络拥塞。

交换机/路由器检查：定期检查网络交换机、路由器的配置和运行状态，确保数据传输的延迟、丢包、均保持在正常范围内。

故障排查：如发现网络延迟、丢包等问题，及时检查线路、设备或配置是否异常。

配置优化：调整网络设备的QoS（流量优先级）策略，优先保障视频会议、视频监控、门禁系统等核心业务数据的传输。

日常巡检：检查网络设备的运行日志，排查异常告警。

(2) 注意事项：

避免网络设备过载运行，确保有足够的冗余带宽。

定期备份网络设备的配置文件，防止因配置错误或设备故障导致数据丢失。

4) 存储设备

(1) 维护内容：

存储空间检查：定期清理存储设备中的过期或无用视频数据，释放存储空间。

数据完整性检查：确保存储的视频数据完整无损，避免因存储故障导致数据丢失。

存储介质健康状态检查：监控硬盘、SSD等存储介质的健康状态，及时更换损坏的设备。

固件升级：定期升级存储设备的固件，提升设备性能和稳定性。

冗余配置检查：检查存储设备的冗余配置（如RAID阵列），确保在单点故障时数据仍可访问。

数据迁移：在存储空间不足时，及时迁移数据至新的存储设备。

日常巡检：检查存储设备的运行日志，排查异常告警。

(2) 注意事项：

避免存储设备长时间满负荷运行，确保有足够的冗余空间。

定期测试存储设备的读写速度和稳定性，确保视频回放流畅。

5) 显示设备

(1) 维护内容：

显示效果检查：定期检查显示屏的画面质量（如分辨率、亮度、对比度等），确保监控画面清晰。

设备连接检查：确保显示设备与视频管理平台的连接正常，避免因线缆或接口问题导致画面丢失。

固件升级：定期升级显示设备的固件，修复潜在的显示问题或优化性能。

故障排查：如发现显示屏黑屏、花屏等问题，及时检查电源、信号线或设备本身是否正常。

日常巡检：检查显示设备的运行状态，确保画面实时更新。

(2) 注意事项：

避免长时间高亮度运行，定期调整显示参数以延长设备寿命。

定期清洁显示屏表面，避免灰尘或污渍影响显示效果。定期检查显示屏背部风扇及散热模组，确保设备温度在正常范围。

6) 管理平台

(1) 维护内容：

平台功能检查：确保管理平台的各项功能（如视频查看、录像回放、报警联动等）正常运行。

用户权限管理：定期检查和更新用户权限，确保只有授权人员可以访问敏感数据。

日志管理：定期清理和备份平台日志，防止日志文件占用过多存储空间。

系统安全检查：确保管理平台的安全性，定期更新安全补丁，防止被攻击。

数据备份与恢复：定期备份平台数据，测试数据恢复功能。

故障排查：如发现平台运行异常（如卡顿、死机等），及时检查系统资源使用情况或日志文件。

配置优化：根据实际需求优化平台的配置参数（如视频流数量、存储策略等）。

日常巡检：检查平台的运行状态，确保所有设备在线且功能正常（如画面显示等）。

(2) 注意事项：

避免随意修改平台配置，确保系统稳定运行。

定期测试平台的报警联动功能，确保在紧急情况下能够正常触发。

7) 电源与环境设备

(1) 维护内容：

电源检查：确保前端硬件、服务器主机、显示设备等的电源供应稳定，避免因电压不稳或断电导致设备损坏。

UPS（不间断电源）检查和保养：定期检查UPS的运行状态和电池健康并进行充放电保养，确保在断电时能够为设备提供应急电源。

接地检查：检查设备的外壳接地和防雷接地。

温湿度检查：确保设备运行环境的温湿度符合要求，避免因环境问题导致设备故障。

电磁干扰检查：检查设备是否受到电磁干扰，避免影响设备的正常运行。

防尘与防潮：定期清洁设备表面，检查设备是否处于防尘、防潮的环境中。

(2) 日常巡检：检查电源设备和环境设备的运行状态，确保设备正常工作。

注意事项：

避免设备长时间处于高温或高湿环境中，确保设备寿命。

定期测试UPS的供电时间，确保在断电时能够支持设备运行足够时间。

6.3 计算机网络子系统运维要求

6.3.1 日常巡检

A) 设备状态：每日检查核心/汇聚交换机端口状态、CPU/内存利用率（阈值 $\leq 70\%$ ）、日志告警。

B) 网络性能：每周监测网络延迟（ $\leq 50\text{ms}$ ）、丢包率（ $\leq 1\%$ ）、带宽利用率（峰值 $\leq 80\%$ ）。

C) 安全策略：每月验证防火墙规则有效性，漏洞扫描（按《GB/T 30276-2020 信息安全技术网络安全漏洞管理规范》执行）。

D) IP地址管理：检测网络IP地址、是否按照规范分配和使用。监测IP地址冲突。观察各个VLAN使用状态。

6.3.2 故障处理

A) 响应时效：

1) 核心设备故障：15分钟内响应，4小时内恢复；

2) 接入层故障：15分钟内响应，2小时内恢复。

3) 备件管理：关键设备备件库储备量 $\geq 10\%$ 。

6.3.3 配置管理

A) 网络拓扑图每季度更新，配置文件变更需通过CMDB（配置管理数据库）记录并留存版本。

6.4 综合布线子系统运维

6.4.1 物理层维护

A) 为快速找到跳线的对端，宜选用可追踪跳线。

注：在可追踪跳线的一端注入光、电信号时，另一端会发光，可在跳线密集时快速找到跳线的对端。

B) 外观检查：

1) 每月抽检3%的信息点，确保RJ45接头无氧化、线缆标签内容准确、字迹清晰。

2) 面板、机柜的两底角高差超过GB/T 50312-2016时，应进行调整；

3) 机柜内配线架正面的跳线应保持美观。

C) 性能测试：年度全量测试（按《GB/T 50312-2016》要求执行），应全部满足GB/T 50312-2016的性能参数：

1) 测试仪器应在有效期内；

2) 可分期分批进行性能测试，部分链路/信道可安排在系统不运行的节假日、断电维护期内进行；

3) 双绞线进行永久链路测试；

4) 光纤光缆进行信道测试。

5) 电子配线架应检查跳线异常时的告警功能。

注：当电子配线架系统正常运行时，人工插拔跳线会引起管理软件告警。

6.4.2 变更管理

1) 新增点位需提交变更申请，施工后提供测试报告及电子标签记录。

2) 跳线更改需提交变更申请，经审批后执行，并留下真实的记录。

注：如果未经审批，可能导致因一处跳线插拔引起另一处出现异常。同时，所有运维管理者都可以插拔跳线，会造成跳线混乱，最终无人敢插拔跳线。

6.4.3 巡检和评估

1 应在巡检时关注综合布线子系统的是否完好、承载综合布线子系统的桥架、管道是否完好。

2 应定期/不定期对系统的运行情况进行评估，形成评估报告。

1) 系统传输能力是否与承载的应用系统相匹配；

2) 是否存在隐患和潜藏的故障；

3) 是否存在已经影响信息传输的故障。

6.4.4 断电维护

当使用二维码标签系统时，断电期间可能会导致二维码服务器停止工作。应采取措施使二维码标签保持有效。

注：二维码标签系统能够承载更多的信息，是对运维有益的标签系统。

6.5 机房及配套子系统运维

6.5.1 环境监控

A) 动环系统：7×24小时监测温湿度（温度 $22\pm 2^{\circ}\text{C}$ ，湿度40%~60%）、UPS负载（ $\leq 80\%$ ）、电池健康度（内阻 $\leq 30\text{m}\Omega$ ）。

B) 市电中断：UPS续航 ≥ 60 分钟，柴油发电机10分钟内启动；

C) 空调故障：启用备用机组，温升速率 $\leq 1^{\circ}\text{C}/\text{分钟}$ 。

6.5.2 物理安全

A) 门禁管理：双因素认证（IC卡+生物识别），出入记录留存 ≥ 180 天。

B) 消防合规：气灭系统年检，烟感探测器覆盖率100%。

6.6 数据备份子系统运维

6.6.1 备份策略与周期

A) 全量备份：按照月度、年度两个策略同时执行。月度全量备份需至少保留最近12个版本，年度全量备份需至少保留最近3个版本。

B) 增量备份：日备份需至少保留最近30个版本。

C) 日志备份：实时同步操作日志至独立存储，保留周期 ≥ 180 天，用于审计与故障溯源。

D) 异地备份的同步频率：全量备份后 24 小时内同步至异地，增量备份实时同步。

6.6.2 备份介质管理

A) 存储介质：采用专用备份服务器、磁带库或云存储，定期检查介质健康状态（如磁带寿命是否 ≤ 3 年）。

B) 环境要求：备份介质存放环境需满足温度 $20\sim 25^{\circ}\text{C}$ 、湿度40%~60%，远离强磁场干扰。

C) 核心业务数据（如监控录像、罪犯信息）需在监狱属地外的“司法行政系统异地灾备中心”存放，备份介质与本地距离 ≥ 50 公里。

6.6.3 备份验证与恢复测试

- A) 数据校验：每次备份后执行完整性校验（如MD5校验），确保数据可恢复性。
- B) 恢复演练：每季度模拟数据丢失场景（如数据库崩溃、硬件故障），验证恢复流程有效性，恢复时间目标（RTO） ≤ 4 小时。

6.6.4 应急恢复流程

A) 故障分级：

P1级（数据丢失）：立即启动全量恢复，优先恢复核心业务数据，响应时间 ≤ 15 分钟。

P2级（部分数据损坏）：基于增量备份修复，响应时间 ≤ 2 小时。

B) 应急预案：制定多场景恢复方案（如勒索病毒攻击、存储设备故障），明确操作步骤与责任人。

6.6.5 安全与合规

A) 加密要求：备份数据采用AES-256加密，传输过程使用SSL/TLS协议，禁止明文存储。

B) 权限管控：备份操作仅限授权人员执行，访问日志留存 ≥ 1 年。

C) 合规标准：符合《GB/T 20988-2007 信息安全技术信息系统灾难恢复规范》要求，关键业务数据保留周期 ≥ 7 年。

6.6.6 文档与报告

A) 备份记录：详细记录备份时间、内容、介质编号及操作人员，归档周期 ≥ 3 年。

B) 故障报告：恢复操作后24小时内提交报告，包含故障原因、恢复过程及改进措施。

6.6.7 考核指标

A) 数据可用性：备份成功率 $\geq 99.9\%$ ，恢复成功率 $\geq 98\%$ 。

B) 响应时效：P1级故障恢复时间 ≤ 4 小时。

6.7 信息应用系统运维

安防信息应用系统的运维服务内容涉及系统的日常运行、维护、优化、安全管理和应急响应等多方面，目的是确保系统的稳定性和高效性，同时保障监狱的安全。

6.7.1 系统日常运维

确保安防信息应用系统的正常运行，及时发现和解决潜在问题。

（1）设备巡检

检查安防信息应用系统的硬件设备，包括但不限于：

检查设备的物理连接（电源线、数据线、信号线）是否牢固。

确保设备表面清洁，无灰尘或污渍影响性能。

（2）系统状态监控

使用监控工具实时监控安防信息应用系统的运行状态。

设置告警规则，及时发现设备故障或异常情况（如网络中断、设备离线、系统性能下降等）。

记录系统日志，分析设备运行数据，发现潜在问题。

（3）用户支持

提供用户操作指导，帮助员工或访客正确使用安防信息应用系统。

处理用户的常见问题（如刷卡失败、权限异常、摄像头画面模糊等），并及时反馈解决方案。
收集用户反馈，优化系统的使用体验。

6.7.2 预防性运维服务

通过定期维护和检查，延长设备使用寿命，减少故障发生。

（1）硬件维护

定期检查安防设备的运行状态，确保硬件正常工作。

检查设备的电源模块、电池等是否正常工作。

更换老化或损坏的设备部件。

（2）软件维护

定期更新安防信息应用系统的固件或软件版本。

检查系统配置文件，确保参数设置正确。

优化设备性能。

确保系统与监狱其他子系统的兼容性和集成性。

（3）网络维护

检查安防信息应用系统与管理平台之间的网络连接，确保通信稳定。

优化网络带宽分配，避免因网络拥塞导致系统响应迟缓。

检查与其他系统（如门禁系统、监控系统、报警系统）的集成接口，确保数据互通。

（4）备件管理

建立备件库，储备常用备件。

定期检查备件的有效性和兼容性，确保在需要时能够及时更换。

6.7.3 故障处理服务

快速响应和修复监狱安防信息应用系统的故障，保障系统的可用性。

（1）故障诊断

故障上报：通过用户反馈或监控系统发现故障。

故障定位：使用日志分析工具或现场检查快速定位故障原因。

故障分类：根据故障类型（如硬件故障、软件故障、网络故障等）采取相应的解决措施。

（2）故障修复

硬件修复：更换损坏的硬件设备。

软件修复：修复因软件配置错误、版本问题或数据损坏导致的故障。

网络修复：解决因网络中断、配置错误或设备通信问题导致的故障。

（3）故障报告

记录故障发生的时间、原因、处理过程和结果。

提交故障报告，分析故障原因，提出预防措施。

6.7.4 系统优化服务

根据实际需求和使用情况，优化监狱安防信息应用系统的性能和功能。

（1）性能优化

调整安防设备的配置参数以提升用户体验。

优化网络带宽分配，确保系统与管理平台的通信稳定。

优化存储策略，确保视频监控数据存储高效且安全。

(2) 功能优化

根据用户需求，增加或调整安防信息应用系统的功能模块（如访客管理、权限分级、联动报警等）。

优化管理平台的界面和操作流程，提升管理效率。

(3) 系统扩展

根据监狱规模或用户数量的增长，扩展存储容量或升级管理平台。

新增安防设备或集成其他系统（如消防系统、楼宇管理系统）。

6.7.5 安全性运维服务

保障监狱安防信息应用系统的安全性，防止未经授权的访问或数据泄露。

(1) 权限管理

严格控制安防信息应用系统的访问权限，确保只有授权人员可以操作。

定期审查和更新用户权限，防止权限滥用。

(2) 数据安全

对安防系统记录的事件数据（如视频监控录像、刷卡记录、报警记录）进行加密存储和传输。

定期备份重要数据，确保数据安全。

(3) 漏洞修复

定期扫描安防信息应用系统和管理平台的安全漏洞，及时修复。

配置防火墙、入侵检测系统等安全工具，提升系统的安全性。

6.7.6 用户管理服务

维护监狱安防信息应用系统用户的权限和信息，确保系统的安全性。

(1) 用户权限管理

添加、删除或修改用户权限（如视频查看权限、报警处理权限等）。

设置权限分级（如普通员工、访客、管理员等）。

(2) 用户信息管理

维护用户信息（如员工编号、姓名、部门等）。

确保用户信息与权限的一致性。

(3) 访客管理

提供访客登记和临时权限授予服务。

管理访客权限的有效期，确保访客权限及时失效。

6.7.7 数据管理服务

维护和管理监狱安防信息应用系统产生的数据，确保数据的完整性和可用性。

(1) 数据备份

定期备份安防系统的事件记录、用户权限等重要数据。

确保备份数据的完整性和可恢复性。

(2) 数据清理

定期清理过期的用户权限和历史数据，释放存储空间。

确保数据存储的规范性和安全性。

(3) 数据分析

分析安防系统的运行数据，发现潜在问题或优化空间。

提供数据统计报告（如刷卡记录、报警统计、视频监控分析等），支持决策。

6.7.8 应急响应与演练

制定应急响应预案，确保在突发情况下能够快速恢复系统。

(1) 应急响应

制定应急响应流程，确保在系统故障或安全事件发生时能够快速恢复。

提供7×24小时技术支持，确保问题及时解决。

(2) 演练与测试

定期进行系统应急演练，测试应急响应流程的有效性。

测试报警系统的联动功能（如报警与视频监控的联动）。

6.7.9 记录与报告服务

记录运维过程中的各项操作和数据，提供清晰的报告。

(1) 运行记录

记录安防信息应用系统的日常运行状态，包括设备状态、刷卡记录、报警记录等。

使用管理平台生成运行记录报告。

(2) 故障记录

记录安防信息应用系统的故障信息，包括故障时间、故障原因、处理过程和结果。

提交故障报告，分析故障原因，提出预防措施。

(3) 运维报告

定期生成运维报告，总结运维工作的成效和不足。

提供改进建议，优化运维流程。

6.7.10 升级与扩展服务

根据监狱需求和技术发展，对安防信息应用系统进行升级和扩展。

(1) 系统升级

定期更新系统的软件和硬件，提升系统性能和安全性。

升级设备固件，修复已知漏洞。

(2) 功能扩展

根据监狱需求，新增功能模块（如智能分析、移动监控等）。

扩展存储容量，支持更多数据的长期存储。

6.8 运维服务台

运维服务台是面向用户的、完成大部分支持工作的支持组。服务台的目的是响应和完成运行维护服务请求，及时跟踪服务请求的处理进展。服务台应包括以下要求：

- A) 建立服务台相关管理制度；
- B) 设置专门的沟通渠道作为与需方的联络点，沟通渠道可以是热线电话、传真、网站和电子邮箱等；
- C) 设置专人按照服务台相关管理制度的要求进行服务请求的处理工作，并留下记录；
- D) 建立服务请求的接收、记录、跟踪和反馈等机制以及日常工作的监督和考核办法。

6.9 事件管理

事件管理的目的是确保及时解决运行维护过程中发生的事件，尽快回复或响应服务请求。事件管理要求如下：

- A) 应设置事件分类、分级和升级机制；
- B) 应规范事件管理过程，并形成文件，建立事件管理的相关制度，包括但不限于事件处理的权限、报告机制和制定事件的处理程序；
- C) 应对事件发生的原因进行分析，并采取措施避免事件的再次发生；
- D) 应对可能发生的重大事件建立应急响应预案，应急响应预案应得到验证和演练，并根据验证和演练的结果对应急响应预案进行持续完善；
- E) 可按照制度文件的要求进行事件管理，包括事件受理、分类、初步支持、调查、诊断、解决、进展监控、跟踪和关闭等，并留下记录；
- F) 宜建立事件解决评估机制，包括事件解决率和事件平均解决时间等，并定期对事件管理情况进行总结与评估。

运维事件管理流程如下图所示。

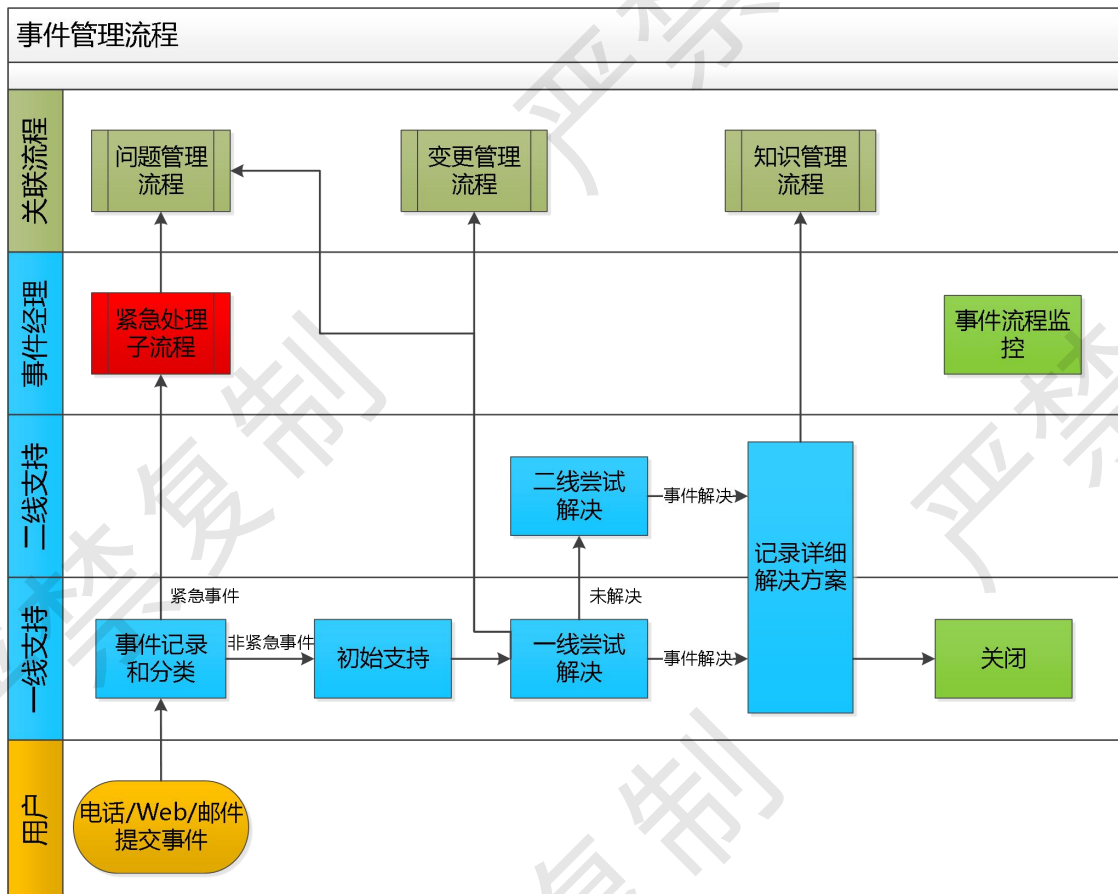


图3 运维事件管理流程图

6.10 问题管理

问题管理的目的是识别事件引起的原因并解决问题，预防同类事件的重复发生。问题管理要求如下：

- A) 应规范问题管理过程，包括问题建立、分类、调查、诊断、解决、错误评估和关闭等，并形成文件，建立问题管理相关制度；
- B) 应建立问题分类管理机制，包括问题影响的范围、重要程度和紧急程度，并确定优先级，按照文件要求进行问题管理，并留下记录；
- C) 可建立问题导入知识库机制，并定期对问题管理情况进行总结与评估；
- D) 可建立问题解决评估机制，包括问题解决率和问题平均解决时间等，对发现的问题进行整改，以保证问题管理过程持续改进。

6.11 配置管理

配置管理的目的是为保证配置数据的可靠性和时效性，关联支持其他服务过程。配置管理要求如下：

- A) 应规范配置管理过程，包括识别、记录、更新和审核等，并形成文件，建立配置管理相关制度；

B) 宜建立配置项审核机制，并定期对配置管理的情况，包括配置管理过程的完整性、配置数据的准确性、有效性、可用性和可追溯性进行总结与评估；

C) 宜对发现的问题进行整改，以保持配置管理过程持续改进。

6.12 变更管理

变更管理的目的是通过管理和控制变更的过程，确保更有序地实施。变更管理要求如下：

A) 应建立与变更管理过程一致的活动，包括请求、评估、审核、实施、确认和回顾等，规范变更管理过程，形成文件，建立变更管理相关制度；

B) 宜建立变更类型和范围的管理机制，并按照文件要求进行变更管理，留下记录，保持变更记录的完整性；

C) 宜对变更完成情况进行统计分析，包括未经批准变更数量占比、不同类型变更数量及占比、不成功变更数量和占比以及取消变更数量占比等，并定期对变更管理情况进行总结与评估；

D) 宜对发现的问题进行整改，以保证变更过程持续改进。

6.13 发布管理

发布管理的目的是为确保一个或多个变更的成功导入。发布管理要求如下：

A) 应建立与发布管理过程一致的活动，包括规划、设计、建设、配置和测试等，规范发布管理的过程，并形成文件，建立发布管理相关制度；

B) 应建立发布类型和范围的管理机制，并按照文件要求进行发布管理，留下记录；

C) 应制定完整的发布方案，包括发布计划、回退方案和发布记录等；

D) 宜对发布完成情况进行统计分析，包括发布成功率、发布及时率和是否更新配置管理数据库等，并定期对发布管理情况进行总结和评估；

E) 宜保证发布管理过程的完整性、发布记录的完整性和准确性，并对发现的问题进行整改，以保证发布管理过程持续改进。

6.14 服务级别管理

服务级别管理的目的是对一个组织的服务质量的关键绩效指标进行监控和管理。服务级别管理要求如下：

A) 应建立服务目录，规范服务级别管理过程，形成文件，建立服务级别管理相关制度；

B) 可根据需方的考核评估要求，建立SLA考核评估机制，包括SLA完成情况和达成率等；

C) 宜在SLA评估后制定改进内容及改进措施。

6.15 能力管理

能力管理的目的是在运行维护服务中，为更好地执行所有的运行维护进度安排，对其进行度量、监控和调整。能力管理要求如下：

A) 应制定服务能力管理相关要求或制度；

- B) 宜按照制度的要求对能力管理过程和实施结果进行监测、评审和记录;
- C) 宜对未达成的指标进行调查分析, 确定能力改进措施和改进计划。

6.16 可用性管理

可用性管理是有关设计、实施、监控、评价和报告信息化运行维护服务的可用性以确保持续地满足业务的可用性需求的服务管理流程。可用性管理要求如下:

- A) 可制定可用性管理的计划, 并根据可用性的要求进行评估和可用性监控;
- B) 可定期或不定期对可用性计划进行更新回顾, 更新回顾的频率 ≥ 1 次/年。
- C) 宜安排专人负责信息化运行维护的可用性管理、变更确认和风险评估等;
- D) 宜每月对运行维护服务的内容进行可用性分析, 形成可用性报告。

6.17 服务持续性管理

服务持续性管理的目的是预防灾难发生, 提高信息系统的恢复能力和容错能力, 并在灾难发生后迅速恢复信息系统正常运作的运行维护服务内容。服务持续性管理要求如下:

- A) 可制定服务持续性管理计划、预防措施和恢复方案等;
- B) 宜安排专人负责信息化运行维护的服务持续性管理、业务影响分析和风险评估等;
- C) 宜在灾难发生后, 提供有关灾难发生原因、影响以及如何成功应对的报告, 所有观察到的问题都在改进计划中得到处理。

6.18 知识管理

知识管理的目的是对知识、知识创造过程和知识的应用进行规划和管理。知识管理要求如下:

- A) 应将常见问题的描述、分析和解决办法建立知识库, 并制定相关管理策略和制度, 采用“录入、审批和发布”的管理流程;
- B) 应确保整个组织内的知识是可用的和可共享的, 根据知识库管理策略和制度要求对知识进行管理, 并留下记录;
- C) 应根据知识的不同类型, 对知识库进行分类记录和管理;
- D) 知识库应具备知识的增加、更新、删除、查询、讨论和移动功能;
- E) 应定期对知识管理情况进行总结和评估, 对知识管理发现的问题及时进行整改;
- F) 知识库的建立、知识文件的增加、更新、删除、查询、讨论和移动均宜设定不同权限, 以保证知识库应用的安全性。

6.19 资源库管理

资源库管理应包括以下要求:

- A) 建立资源库管理制度;
- B) 根据资源产品的类型、资源来源、所属项目名称、质保日期、售后服务联系人和联系方

式等建立资源库；

C) 实时更新或定期更新资源库，最长更新周期 ≤ 1 个月。

6.20 备品备件管理

应由信息化部门牵头制定备品备件的计划、采购、仓储、使用、监督和检查考核的管理办法，备品备件包括但不限于自备备件、特定备件和紧急备件，备品备件管理要求如下：

A) 应明确备品备件管理的责任人和管理职责；

B) 应根据不同类型的设施设备制定相应的库存备件比例要求；

C) 备品备件的计划、采购宜向信息化部门报批；

D) 备品备件宜定期进行盘点，最长盘点周期 ≤ 1 个月，发现盘盈和盘亏应查明原因，落实责任，妥善处理；

E) 备品备件宜定期进行测试，以确保备品备件的有效性和可用性，最长定期测试周期 ≤ 6 个月。

6.21 文档管理

6.21.1 基本要求

文档管理基本要求如下：

A) 运行维护服务提供者应形成明确的文档管理制度，并通过运行维护服务管理者的审核；

B) 运行维护服务提供者应建立文档的登记、查阅、流转和审批制度；

C) 文档管理应按照日常运行维护工作类、报告类、资产类和技术资料类，并以月为单位，按照时间的先后顺序进行归档；

D) 纸质文档应装订成册归档、电子文件应统一保存分类归档并有 ≥ 2 个以上介质备份，防止数据丢失；

E) 文档管理涉及到保密的内容应严格按照保密管理的相关要求执行；

F) 文档管理的文档包括但不限于例行报告、事件报告、故障总结报告、检查报告和应急预案。可根据运行维护服务对象的不同而确定不同的文档。

6.21.2 文档管理的内容

A) 例行报告

例行报告包括周报和月报等。例行报告内容应包括但不限于报告名称、报告周期、服务综述、服务内容、完成情况、运行维护对象的风险隐患分析、改善措施与建议以及下一步工作计划。

B) 事件报告

事件报告是指事件发生后运行维护服务提供者向运行维护服务管理者提交的报告。安全事件和重大事件应在事件处置完成后 ≤ 3 个工作日提交事件报告。

事件报告的内容包括但不限于事件名称、事件描述（包括事件现象、受理时间、处理时间和当前状态等）、事件影响程度与范围、事件的处置方法、事件原因分析和后续改善计划。

C) 故障总结报告

故障总结报告是指故障处置完成后运行维护服务提供者向运行维护服务管理者提交的总结报告。重大故障应在故障处置完成后3个工作日提交故障总结报告。

故障总结报告内容应包括但不限于报告名称、故障概述（包括故障现象、故障产生时间、故障发现时间、处置时间和当前状态等）、故障影响程度与范围、故障的处置方法、故障原因分析、经验教训和后续工作安排等。

D) 检查报告

检查报告是指运行维护服务提供者在各类运行维护检查工作完成后向运行维护服务管理者提交的检查报告。

检查报告内容应包括但不限于日常例行巡检报告、定期现场巡检报告、重大节假日巡检报告和临时性检查报告。各报告内容要求如下：

1) 日常例行巡检报告

应1次/月提供日常例行巡检报告，并附日常巡检记录表。内容应包括但不限于报告名称、月度例行巡检概述（包括巡检主要内容和整体情况）、巡检发现的问题、问题处理情况、遗留问题情况和风险、改善措施和建议以及下月计划等。

2) 定期现场巡检报告

应≥1次/0.5年提供定期现场巡检报告，并附定期现场巡检记录表。内容应包括但不限于报告名称、定期现场巡检整体情况、主要完成内容、巡检发现的问题、问题处理情况、遗留问题情况和风险、改善措施和建议以及下一步计划。

3) 重大节假日或重要活动巡检报告

重大节假日或重要活动巡检报告是指在重大节假日或重要活动前运行维护服务提供者按运行维护

4) 服务管理者的要求完成的巡检工作并提交的巡检报告。

内容应包括但不限于报告名称、整体情况概述、主要完成内容、巡检发现问题、问题处理情况、遗留问题情况和风险、改善措施和建议以及节假日或重要活动保障计划等。

5) 临时性检查报告

临时性检查报告是指因运行维护服务管理者的临时性或突发性重要任务需求，对运行维护服务对象进行临时检查而形成的报告。内容应包括但不限于报告名称、检查情况概述、主要完成内容、检查发现问题情况、问题处置情况、遗留问题情况和风险、改善措施和建议以及下一步计划。

6.22 资产管理

资产管理是指运行维护服务提供者对运行维护对象中的所有信息化资产进行管理。资产管理要求如下：

A) 应识别与信息系统相关的所有运行维护服务对象，建立资产台账，台账内容包括但不限于资产名称、资产品牌、资产型号、资产所在位置、资产来源、资产用途、资产供应商、资产责任人和联系方式；

B) 应为每项已识别的资产指定所属关系并根据资产的重要性进行分级管理；

- C) 应建立资产管理相关制度，包括但不限于日常管理制度、资产变更制度和报废制度；
- D) 资产管理宜通过运行维护技术平台进行无纸化管理；
- E) 宜实时更新资产台账；
- F) 应及时更换使用年限过长的老旧资产设备，减低设备故障风险。资产设备使用年限按照GB50348—2018中11.1.4的规定执行。

6.23 综合管理

综合管理包括但不限于咨询与培训服务、技术支持服务以及综合系统服务。

6.23.1 咨询与培训服务

- A) 运行维护服务提供者应为运行维护服务使用者和运行维护服务管理者提供7X24小时咨询服务；
- B) 运行维护服务提供者应根据SLA的规定为运行维护服务使用者和运行维护服务管理者提供培训服务，应 ≥ 1 次/年开展培训服务；
- C) 培训服务应由运行维护服务提供者组织，运行维护服务使用者和运行维护服务管理者共同参与；
- D) 运行维护服务提供者应提前编写培训服务方案，报送运行维护服务管理者，审核通过后方可开展培训服务工作；
- E) 培训服务完成后应进行培训考核，确保培训质量；
- F) 培训服务方式可采取远程培训或现场培训等方式进行。

6.23.2 技术支持服务

- A) 运行维护服务提供者应为运行维护服务使用者和运行维护服务管理者提供的技术支持服务应包括但不限于电话支持、远程支持和现场支持；
- B) 技术支持服务的内容应包括但不限于服务请求、故障处理、数据迁移、设备搬迁和升级优化；
- C) 技术支持服务的响应标准应根据运行维护服务使用者和运行维护服务管理者的实际需要，由运行维护服务使用者、运行维护服务管理者和运行维护服务提供者协商确定，并在SLA中进行明确约定。

6.23.3 综合系统服务

SF/T0088综合系统服务主要指运行维护服务提供者为保障运行维护服务工作的正常开展，寻求专业的其他第三方提供的服务。

6.24 应急保障

6.24.1 应急响应过程

应急响应过程包括4个主要阶段：应急准备、监测与预警、应急处置和总结改进。如下图所示：

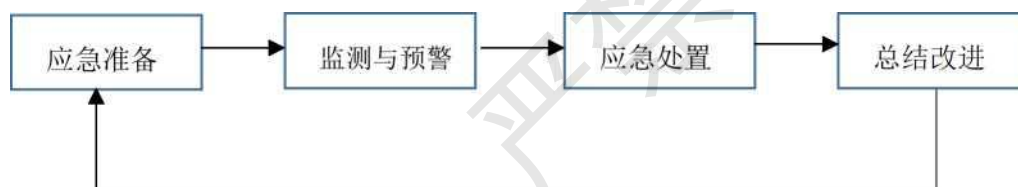


图4 应急响应过程图

6.24.2 应急响应各阶段的工作内容

A) 应急准备阶段的工作包括：组建应急响应组织、确定应急响应制度、系统性识别运行维护服务对象及运行维护活动中可能出现的风险、定义应急事件级别、制定应急响应预案、开展培训和演练；

B) 监测与预警阶段的工作包括：进行日常监测、及时发现应急事件并有效预警、进行核实和评估、以规定的策略和程序启动预案以及保持对应急事件的跟踪；

C) 应急处置阶段的工作包括：采取必要的应急调度手段、基于预案开展故障排查和诊断、对故障进行有效快速地处理和系统恢复、及时通报应急事件、提供持续性服务保障、进行结果评价以及关闭事件；

D) 总结改进阶段的工作包括：对应急事件发生原因、处理过程和结果进行总结分析、持续改进应急工作以及完善信息系统。

6.24.3 应急准备

A) 应建立应急响应组织，应急响应组织应由相关利益方组成，包括运行维护服务使用者、运行维护服务管理者、运行维护服务提供者和其他机构专家团队；

B) 应明确应急响应组织相关利益方的角色和职责；

C) 应制定应急响应制度，并明确应急响应的目标、原则和范围等；

D) 应划分应急事件级别，并根据应急事件的级别制定应急预案；

E) 应急响应预案应经过相关利益方的评审，并由运行维护服务管理者发布应急预案；

F) 应结合业务领域突发事件级别和运行维护服务中的应急事件级别，制定总体预案，开展培训和演练；

G) 应定期（ ≥ 1 次/年）进行应急演练和培训，以确保相关人员熟悉处置的操作规范和操作流程；

H) 宜定期进行重要信息系统的风险评估，确保应急响应组织了解其在运行维护过程中的关键活动、所需资源、限制条件和信息系统面临的各种风险要素。

6.24.4 监测与预警

A) 持续开展日常监测活动，实施有效预警，监测预警的范围包括所有运行维护服务对象；

B) 建立监测和预警的记录以及报告制度，并按照约定的形式和时间间隔上报现场负责人；

C) 发现应急事件时，按照应急响应制度和应急响应过程进行报告，并保持持续跟踪，直到应急事件关闭。

6.24.5 应急处置

应根据应急预案进行应急事件的处置。

6.24.6 总结改进

- A) 定期对应急响应工作进行分析和回顾，总结经验教训，并采取适当的后续措施；
- B) 定期对应急响应制度和应急响应过程进行完善。

7 运行维护服务方法

7.1 安全保障类与狱务实战类运维服务方法

7.1.1 预防性运维

预防性运维的核心是通过定期检查和维修，避免设备故障的发生。

7.1.2 定期巡检

每周对摄像头、云存储主机、网络设备等进行检查，检查设备的运行状态、网络连接、存储空间、电源供应等。

使用自动化工具（如监控系统）实时监控设备的运行状态，及时发现异常。

7.1.3 预防性维护

定期清洁设备表面，避免灰尘积累影响散热。

检查设备的物理连接（如电源线、网络线、信号线）是否牢固，避免因松动导致设备故障。

定期备份重要数据，确保数据安全。

7.1.4 设备健康评估

定期评估设备的健康状态，如硬盘的剩余寿命、电池的健康度等，提前更换老化设备。

对设备的性能进行压力测试，确保其在高负载下仍能稳定运行。

7.1.5 应急响应运维

应急响应运维是指在设备或系统出现故障时，快速恢复其正常运行。

7.1.6 故障诊断与修复

当设备出现故障时，快速定位问题（如网络中断、设备损坏、软件故障等），并采取相应措施修复。

使用日志分析工具排查故障原因，缩短故障恢复时间。

7.1.7 备件管理

建立备件库，储备常用备件（如硬盘、电源、网络模块等），确保在设备故障时能够快速更换。

定期检查备件的有效性和兼容性。

7.1.8 应急预案

制定应急预案，明确故障发生时的处理流程 and 责任人。

定期进行应急演练，提高团队的故障处理能力。

7.1.9 优化性运维

优化性运维的目标是提升设备和系统的性能、可靠性和用户体验。

7.1.10 性能优化

根据实际需求调整设备的配置参数（如摄像头的分辨率、云存储的压缩率等），提升性能和

效率。

优化网络带宽分配，确保视频流传输的稳定性。

7.1.11 系统升级

定期检查设备的固件、软件版本，及时升级以修复漏洞、提升性能。

升级管理平台的功能，增加新的监控功能或优化现有功能。

7.1.12 资源扩展

根据存储需求的增长，及时扩展存储容量（如增加硬盘、升级云存储套餐）。

在网络带宽不足时，升级网络设备或调整带宽分配策略。

7.1.13 安全性运维

安全性运维是保障设备和系统免受攻击或数据泄露的重要措施。

7.1.14 权限管理

严格控制设备和系统的访问权限，确保只有授权人员可以操作。

定期审查和更新用户权限，防止权限滥用。

7.1.15 数据加密

对存储和传输的视频数据进行加密，防止数据泄露。

确保云存储的数据加密机制正常运行。

7.1.16 漏洞修复

定期扫描设备和系统的安全漏洞，及时修复。

配置防火墙、入侵检测系统等安全工具，提升系统的安全性。

7.1.17 规范性运维

检查安防设施的设备编码、设备时间、OSD字符是否符合规范，正常显示。

7.1.18 运维自动化

通过自动化工具和技术，提升运维效率，减少人为错误。

7.1.19 自动化监控

运维工具需符合优先选用国产工具要求。

使用监控系统实时监控设备的运行状态，自动告警异常情况。

设置自动化巡检任务，定期检查设备的健康状态。

7.1.20 自动化备份

配置自动化的数据备份策略，定期备份重要数据。

设置自动化的数据清理任务，释放存储空间。

7.1.21 自动化修复

配置自动化的故障修复脚本，如自动重启故障设备、自动恢复配置等。

使用自动化工具修复常见的软件或网络问题。

7.1.22 运维管理

良好的运维管理是保障运维工作高效执行的关键。

7.1.23 运维文档管理

建立详细的运维文档，包括设备清单、配置参数、操作手册、故障记录等。

定期更新文档，确保其准确性和完整性。

7.1.24 运维团队培训

定期对运维团队进行培训，提升团队的技术能力和应急处理能力。

通过案例分析和经验分享，提升团队的协作效率。

7.1.25 运维绩效评估

定期评估运维工作的绩效，如故障率、平均修复时间（MTTR）、用户满意度等。

根据评估结果优化运维策略和流程。

7.2 信息系统基础设施运行维护服务方法

7.2.1 机房与机房基础设施运行维护服务方法

机房与机房基础设施的运行维护包括但不限于对机房、电气系统、消防系统、空调系统、防雷接地系统、环境监控系统和综合布线系统的运行维护。

A) 应建立机房管理制度，对出入机房的人员采取审批和登记管理；

B) 应定期对机房基础设施进行日常巡检，掌握设备运行和机房环境情况，其中监狱核心机房基础设施巡检包括日常巡检应 ≥ 1 次/天，非核心机房应 ≥ 1 次/周；

C) 应定期（ ≥ 1 次/月）对机房基础设施的运行情况进行综合检查分析，形成设备运行分析报告；

D) 应定期（ ≥ 1 次/月）对机房基础设施进行清洁保养，如：机房清洁除尘、设备清洁除尘、设备线缆整理、标识标签完整性与准确性检查等，完成保养检查日志记录；

E) 对UPS进行放电测试宜 ≥ 1 次/每季度，对蓄电池进行性能测量和放电测试，检查电气连接及电池开关，保证UPS电池活性，对不满足放电时间要求的电池进行更换；

F) 应及时响应用户提出的服务请求，并按照SLA约定的内容进行问题处理；

G) 宜利用运行维护技术平台实时监控机房基础设施运行状态和故障告警等情况；

H) 宜针对当前基础设施运行情况，给出优化建议并实施，提升运行性能。

7.2.2 网络设施运行维护服务方法

网络设施运行维护包括但不限于对加密网、政务外网、互联网和其他专网（政府部门专网或自建专网）的路由器、交换机、通信设备、传输设备和传输链路的运行状态的运行维护，确保系统正常、高效、稳定和可靠运行。运行维护服务方法要求如下：

A) 应定期对网络设施进行日常巡检，掌握设备状态和环境情况，其中核心网络设施（包括核心网络设备、核心传输设备和核心网络链路）的日常巡检应 ≥ 1 次/天，非核心网络设施的日常巡检应 ≥ 1 次/周；

B) 应对网络设施开展定期预防性检查，核心网络设施（包括核心网络设备、核心传输设备和核心网络链路）应 ≥ 1 次/周开展预防性检查，非核心网络设施应 ≥ 1 次/月开展预防性检查；

C) 网络设施的数据宜实时进行备份或可定期进行数据备份，定期备份周期应不少于每月1次，在网络设施配置发生变化后应立即进行数据备份，以减少网络设施设备故障带来的数据风险；

D) 应定期(≥1次/月)对网络设施进行清洁保养,如:设备除尘、设备线缆整理、标识标签完整性与准确性检查等,完成保养检查日志记录;

E) 应进行网络适应性改进、预防性改进和增强性改进,改进内容包括但不限于路由策略调整、固件升级加固和软件版本升级优化,以提升网络设施的稳定性和可靠性;

F) 应及时响应用户提出的服务请求,并按照SLA约定的内容进行问题处理;

G) 宜利用运行维护技术平台实时监控网络设施的运行状态、网络流量和故障告警等情况;

H) 主备网络设备和链路的切换测试频率宜≥1次/季度,以检查备用设备或链路的可用性。

7.2.3 计算与存储设施运行维护服务方法

计算与存储设施运行维护包括但不限于ARM服务器、X86服务器、磁盘阵列、磁带库、云服务平台(含司法公有云、私有云和政务云)、与5GMEC相关的计算设备和存储设备的运行维护。

A) 应定期对计算与存储设施进行日常巡检,掌握设备状态和环境情况,其中核心业务应用的服务器、存储设备、云服务平台应≥1次/天开展日常巡检,非核心业务计算与存储设施应≥1次/周开展日常巡检;

B) 应定期(≥1次/月)对计算与存储设施进行清洁保养,如:设备除尘、设备线缆整理、标识标签完整性和准确性检查等,完成保养检查日志记录;

C) 应定期(1次/周)对计算与存储设施进行杀毒,以确保设备设施的稳定性和可靠性;

D) 应进行计算与存储设施适应性改进、预防性改进和增强性改进,改进内容包括但不限于操作系统升级、漏洞补丁加固、固件升级加固和软件版本升级优化等,以提升计算与存储设施的稳定性和可靠性;

E) 应及时响应用户提出的服务请求,并按照SLA约定的内容进行问题处理;

F) 宜利用运行维护技术平台,实时监控计算与存储设施的运行状态和故障告警等情况。

7.2.4 物联网设施运行维护服务方法

物联网设施运行维护包括但不限于电子戒具、生命探测设备、车底扫描设备、入侵报警设备、智能锁具、物联网终端、物联网智能设备、生物特征识别设备、目标跟踪系统、智能押解系统、移动执法终端、无人机系统和配套设备设施的运行维护。运行维护服务方法要求如下:

A) 应每天对物联网设施进行日常巡检,检查物联网设施的运行状态和故障告警等情况;

B) 应定期对物联网设施的功能进行检查,以确保功能的有效性;

C) 应及时修复物联网设施的运行故障,不可影响监管安全;

D) 应定期对物联网设施进行保养,保养内容包括但不限于设备除尘、设备线缆整理、标识标签完整性和准确性检查,完成保养检查日志记录;

E) 应及时响应用户提出的服务请求,并按照SLA约定的内容进行问题处理。

7.2.5 指挥调度设施运行维护服务方法

指挥调度设施运行维护包括但不限于指挥调度大屏显示设备、音频设备、视频设备、管控设备、执勤设备、报警设备、调度设备、安防集成平台、视频会议系统和视频点名系统的运行维护。

A) 应建立指挥调度运行维护服务管理制度;

B) 应及时修复运行故障,不可影响监管安全;

C) 应定期进行保养,保养内容包括但不限于设备除尘、设备线缆整理、标识标签完整性和

准确性检查，完成保养检查日志记录；

D) 应定期进行设施适应性改进、预防性改进和增强性改进，改进内容包括但不限于操作系统升级、漏洞补丁加固、固件升级加固和软件版本升级优化，以提升指挥中心设施的稳定性、可靠性；

E) 应及时响应用户提出的服务请求，并按照SLA约定的内容进行问题处理；

F) 宜定期进行应急演练；

G) 宜1次/天进行日常巡检，检查指挥调度设施的运行状态、故障告警，并形成巡检记录；

H) 宜 ≥ 1 次/周进行视频会议系统的点名联调测试，确保设备设施稳定、高效和可靠运行；

I) 宜定期对安防集成平台、视频会议系统、视频点名系统和指挥调度系统的功能进行检查，以确保功能的有效性。

7.2.6 安防设施运行维护服务方法

安防设施运行维护包括但不限于视频监控系统、广播系统、监听对讲系统、报警系统、出入口控制系统、安检系统、电子巡查系统、门禁系统、电话系统和驻狱武警信息化执勤设施的运行维护。运行维护服务方法要求如下：

A) 应及时对安防系统进行适应性防护环境的调整，以满足监管使用的相关要求；

B) 应及时修复安防设施的运行故障，不可影响监管安全；

C) 应定期对安防设施的软硬件配置数据进行数据备份，数据更新后应实时进行数据备份，降低设备故障而引发的数据丢失风险；

D) 安防设施应定期进行保养维护，保养维护内容包括但不限于设备除尘、设备线缆整理、标识标签完整性和准确性检查，户外安防设备应 ≥ 1 次/每季度进行定期设备除尘，室内安防设备应 ≥ 1 次/每半年进行定期除尘；

E) 应及时响应用户提出的服务请求，并按照SLA约定的内容进行问题处理；

F) 宜1次/天对安防设施进行日常巡检，检查安防设施的运行状态和故障告警，并形成巡检记录。

G) 应每日检查安防设施在线率、监控视频推送率、录像保存完整率。

7.2.7 桌面设施运行维护服务方法

A) 桌面设施运行维护包括但不限于台式计算终端、移动计算终端、输入输出设备和移动存储介质的运行维护。运行维护服务方法要求如下：

B) 应建立桌面设施运行维护管理制度；

C) 应按SLA的约定及时修复硬件故障、软件故障和系统故障，并响应用户的服务响应需求；

D) 应及时检查台式计算机终端和移动计算终端的补丁，并进行补丁升级；

E) 计算机终端应安装防病毒软件，并及时更新病毒库，更新周期宜 ≥ 1 次/周；

F) 应 ≥ 1 次/年组织用户培训，提升用户使用水平；

G) 应不定期发布桌面和外围设备风险安全隐患报告；

H) 应及时响应用户提出的服务请求，并按照SLA约定的内容进行问题处理。

7.2.8 应用支撑基础设施运行维护服务方法

应用支撑基础设施运行维护包括但不限于操作系统、数据库和中间件的运行维护。

A) 应制定应用支撑基础设施运行维护的日常管理制度，建立管理规范 and 流程；

B) 应制定应用支撑基础设施日常巡检制度；

C) 对应用支撑基础设施的操作，均应事先制定详细操作流程，经过审核后存档，并在后期严格执行；

D) 应 ≥ 1 次/月对应用支撑基础设施进行运行状况分析，包括但不限于健康状况分析、性能情况分析等；

E) 应及时根据运行情况做稳定性和性能型的改进和调整；

F) 应及时检查应用支撑基础设施中的漏洞和补丁，并进行修复；

G) 应配备具有相应能力的人员和必要的工具，并定期进行专业培训，以提高服务可用性；

H) 应定期对设施运行状态数据进行统计和趋势量化分析，对于异常趋势，做出预警及相关预案；

I) 宜对应用支撑基础设施早、晚各进行1次/天日常巡检，检查应用支撑基础设施的运行状态和故障告警等情况；

J) 宜建立应急预案并定期进行演练。

7.2.9 信息安全设施运行维护服务方法

信息安全设施运行维护包括但不限于防火墙、网闸、漏洞扫描设备、入侵检测设备、防病毒网关、堡垒机、蜜罐、加密卡、USBKey、杀毒软件、保密检查软件等的运行维护。

A) 应根据网络安全等保测评有关要求，制定信息安全管理度，构建满足信息安全运行维护服务的组织机制、岗位角色、人员职责和权限；

B) 应建立信息安全运行维护服务内容，明确操作规范和工作流程，支撑安全管理活动的实施；

C) 应定期对信息安全设施进行检查，检查内容包括但不限于信息安全设施的运行状态和故障告警；

D) 应定期分析信息安全资产的安全监控数据，定期形成安全分析报告，包括但不限于状态分析、影响分析和趋势分析；

E) 应定期分析和总结频繁发生的安全事件和重大安全事件，明确安全事件等级、影响程度和响应优先级，制定信息安全事件报告程序；

F) 应制定有效的应急预案，每年至少组织一次应急演练；

G) 应定期对信息安全设施进行适应性改进、预防性改进和增强性改进，改进内容包括但不限于配置优化、漏洞补丁加固、固件升级加固和软件版本升级优化，按时进行防火墙规则库升级和杀毒软件的及时升级等，以提升信息安全设施的稳定性和可靠性；

H) 应及时响应用户提出的服务请求，并按照SLA约定的内容进行问题处理；

I) 宜 ≥ 1 次/0.5年重新进行密码设置，密码位数应设置为 ≥ 8 位的复杂密码，且密码组合方式采用大写字母、小写字母、数字和符号中至少3种。

7.2.10 信息资源与数据运行维护服务方法

信息资源与数据运行维护包括罪犯信息库、警察职工信息库和监狱管理信息库的运行维护。

- A) 应制定信息资源与数据运行维护服务的日常管理制度，建立管理规范 and 流程；
- B) 应制定信息资源与数据运行维护服务的日常巡检制度；
- C) 对信息资源与数据的操作，均应事先制定详细操作流程，经过审核后存档，并宜建立运行维护知识库，并在后期严格执行；
- D) 应做好信息资源与数据的及时备份；
- E) 应对运行维护服务人员进行相关安全管理及安全要求培训，并定期对服务人员进行考核，以确保服务人员了解并遵守安全和保密相关规定；
- F) 宜定期对信息资源与数据的运行状态进行统计和趋势量化分析，对异常趋势做出预警及相关预案；
- G) 宜建立信息资源与数据处理的应急预案并定期进行演练；
- H) 宜进行数据审计，数据更改历史可查。

7.3 信息应用系统运行维护服务方法

信息应用系统运行维护包括但不限于安防类配套软件等的运行维护。

- A) 应制定运行维护服务的日常管理制度；
- B) 应制定运行维护服务的日常巡检制度；
- C) 特殊时间段（如：法定节假日或重大事件日等），应提升响应级别，提供必要的现场支持；
- D) 应 ≥ 1 次/月对系统进行运行状况分析，包括但不限于健康状况分析和性能情况分析；
- E) 应及时根据系统运行情况做稳定性和性能型的改进和调整；
- F) 宜及时对系统进行更新和升级；
- G) 宜建立运行维护服务的应急预案并定期进行演练；
- H) 宜按照不少于1次/天的频率对系统进行日常巡检，检查系统的运行状态和故障告警等情况。

8 运行维护技术平台

8.1 智能监控

8.1.1 基本要求

运行维护技术平台宜实现业务全栈跟踪、安防设施监控、信息应用系统监控、网络设施与信息安全设施监控、云服务平台监控、中间件监控以及操作系统和数据库监控。

8.1.2 业务全栈跟踪

- A) 业务全栈实时跟踪应以可视化方式显示与之具有关联关系的中间件、数据库、操作系统、承载应用的虚拟机、服务器和交换机等；
- B) 宜实现虚拟机或服务器的操作系统等对象之间的逻辑关系对应，并实时监控相关故障、性能指标和设备状态，为运行维护服务提供者提供监控手段。

8.1.3 安防设施监控

应实现对门禁系统、报警系统、广播系统和视频监控系统等安防设施的状态监控。

8.1.4 应用系统监控

宜实现应用系统进程数和请求个数/分钟等关键指标，超过设定的指标阈值应能预警。

8.1.5 网络设施与信息安全设施监控

应实现交换机、路由器、防火墙等网络设施和信息安全设施的状态监控，获取设备告警信息。

8.1.6 云服务平台监控

应能够实时查看云服务平台的CPU使用情况、内部的数据传输情况、磁盘使用情况和系统日志。

8.1.7 中间件监控

应实现国内外主流常见中间件和相应系统的中间件的实时状态监控。

8.1.8 操作系统和数据库监控

宜实现操作系统和数据库的运行状态和性能数据的统一有效管理。支持主流数据库的监控管理。

8.2 视频质量监测

应实现对信号丢失、图像模糊、亮度异常、图像偏色、噪声干扰、条纹干扰、画面冻结、黑白图像、视频抖动、对比度异常、视频畸变、视频遮挡、场景变更、图像过暗、信令时延、视频流时延和关键帧时延等视频质量问题的故障诊断，并主动发现视频异常、取流失败、解码失败和诊断失败等问题。

8.2.1 视频异常响应

视频质量异常分级处置，P1 级（信号丢失、黑屏），15 分钟内触发告警，30 分钟内到场处置；P2 级（图像模糊、偏色），1 小时内触发告警，2 小时内到场处置；视频质量异常时，指挥中心声光告警，同时运维人员手机APP推送。

8.3 管理与分析

8.3.1 报修管理

- A) 应提供流程化的报修功能，实现用户在线报修、报修进度跟踪和服务反馈等功能；
- B) 应具备报修单状态查询功能；
- C) 宜使用手机等移动设备进行在线报修。

8.3.2 工单管理

- A) 应实现对服务/事件工单和问题工单的统一管理；
- B) 工单应包括系统告警转工单、人工派工单和报修单转工单等不同类型；
- C) 应实现工单各个状态信息统计、过滤、排序、导出和打印等；
- D) 可实现工单的提交、自定义查询、查阅、处理、导出和打印等功能；
- E) 可实现工单模板配置；
- F) 宜支持工单流程和表单内容可定制。

8.3.3 资产管理

A) 应具备资产录入、变更、统计、位置关联和资产的健康度分析等功能；

B) 宜实现以机房和机柜为源头，对服务器、交换机和防火墙等运行维护服务对象的关联关系登记；

C) 宜能够展示机柜、服务器、防火墙、交换机、存储、数据库、中间件、操作系统和应用系统之间的逻辑关系，方便资产统计和管理。

8.3.4 拓扑管理

A) 应具备监控对象组网的逻辑拓扑图，并能展示监控对象组网的逻辑关系；

B) 逻辑拓扑图应能直观地区分监控对象正常、断链和异常等网络状态；

C) 逻辑拓扑图应能动态显示各种网络设备和关键线路的负载数据；

D) 可通过自动发现和手动绘制等方式构建逻辑拓扑图；

E) 逻辑拓扑图可支持被管理设备的连接线状态查看、正常/异常状态区分以及增加、删除、修改和复制等相关功能。

8.3.5 告警管理

A) 应能够实时采集监控对象的告警信息，告警的严重级别、数据推送和通达方式可配置；

B) 应具备告警自动确认、告警清除和告警转工单等功能；

C) 可进行告警规则的设置，包括但不限于邮件转发告警、告警配置、过滤规则和级别重定义规则。

8.3.6 巡检管理

A) 应具备周期性智能巡检功能；

B) 应具有巡检模板，包括但不限于系统自动巡检模板和人工巡检模板；

C) 系统自动巡检完成后应能自动生成巡检报告，巡检报告宜支持Word和WPS等格式版本的查看、导出和打印；

D) 可对巡检任务进行增加、删除、修改和查看，并具备巡检对象设置、巡检指标设置和巡检方式设置等功能；

E) 宜具备巡检计划任务的定时调度执行、复制、启用和禁用等功能。

8.3.7 知识及问题管理

A) 应实现按知识库的分类，可分为告警知识库、问答知识库、安全知识库和维修知识库等；

B) 所有知识库的分类都应支持查询、增加、编辑、删除和导出；

C) 可对问答知识库进行管理，应具备在线问答功能，能够对自己的答案进行编辑、关闭和删除，提问者可对问题回答进行评价。

8.3.8 应急演练管理

A) 具有应急预案库管理功能，支持应急预案的登记、修改、删除、查看、取消、打印、导出、上传和下载等功能；

B) 具备支持应急演练计划登记、修改、删除、查看、取消、打印和导出等相关功能；

C) 应急演练登记内容包括但不限于演练标题、演练开始时间、结束时间、使用的应急预案

（从已经登记的预案中选择）、专家支撑（从系统专家库选择）、演练的目的、演练的内容、演练的参演人员、演练的实施步骤、演练的结果登记和演练的总结等。

8.3.9 报表管理

A) 应能自动生成报表，包括运行维护报表、资产设备报表、性能报表、告警报表和统计报表等，并能下载至本地保存；

B) 统计报表应包括工单统计、工单完成率统计、工单总数趋势统计、工单时间统计和事件工单统计等报表；

C) 统计报表可根据具体需求定制。

8.3.10 专家信息库管理

A) 应建立专家信息库，实现专家信息的录入、查询、修改、删除、统计和打印等功能；

B) 可对专家的水平、科研成果、专利获取、基金资助、论著发表和留学经历等信息进行增加和删除。

8.3.11 运行维护分析与研判

A) 运行维护分析

1) 具备对监控数据、告警数据和重要事件数据进行系统分析评估的功能，提供包括基于区域、系统和监狱的健康评估；具备基于设备类型、厂商、区域、系统和时间等多维度的告警分析功能；

2) 具备基于服务器CPU、内存和磁盘等性能利用率的分析功能；

3) 具备基于设备类型、厂家、型号和质保期的资产分析功能。

B) 运行维护研判

1) 应具备对服务器和网络设备的CPU、内存和磁盘等多类历史性能指标数据进行离线数据分析研判的功能；

2) 宜具备对硬盘预计可使用时间、应用崩溃和性能不足等情况进行研判的功能，并提供建议。

8.4 大屏展示

A) 具备运行维护大屏展示功能，并通过仪表盘和进度条等多种方式实现设备的可视化展示；

B) 具备对运行维护服务对象的整体运行情况和故障情况等多种信息进行统一展示的功能。

8.5 云服务平台管理

A) 宜具备对云服务平台可视化管理能力；

B) 宜具备应用服务路径分析功能，实现虚拟机间的映射关系视图；

C) 宜具备虚拟数据中心的储存分析能力，包括但不限于每秒读写操作次数（IOPS）、读写延迟和使用率等关键指标；

D) 宜具备流量分析功能，实现每个主机、虚拟交换机、网络端口、虚拟主机和应用的网络流量分析，并按照端口使用流量大小显示；

E) 宜具备定制仪表板功能, 呈现管理员关心的各项性能指标, 并以颜色等级区分严重程度;

F) 可提供虚拟机到虚拟机之间的数据包捕获功能;

G) 可具备智能基线学习功能, 可实现依据前1小时或前1天, 前1周及特定一段时间作为基准学习的设置;

H) 可实现自定义的虚拟机组仪表监控, 呈现如CPU利用率、CPU等待延迟、内存利用率、内存等待延迟、存储IOPS、读写延迟、网络延迟、重传、零窗口和应用响应时间等的关键指标;

I) 宜实现通过时间窗口回溯到任意时间段内的性能指标展示, 最小时间窗口支持到1分钟的数据变化情况;

J) 宜支持私有云的端到端大数据可视化分析, 提供相关业务应用的一一对应关系, 包括但不限于宿主机、虚拟机、存储、网络、服务路径和应用。

8.6 机房动环监控

8.6.1 供配电系统监测

A) 可实时监测配电柜内市电、UPS、空调的三相、单相输出电压、电流、频率、功率、功率因数、有功功率、无功功率、视在功率、有功电度和无功电度等数字化电力参数;

B) 可实时监测配电柜的重要开关状态, 供配电系统工作状态异常时自动报警。

8.6.2 UPS电源监测

可对UPS电源的输入三相电压、输出三相电压电流、内部整流器、逆变器、电池、旁路和负载等各部件的运行状态进行实时监控, UPS电源工作状态异常时, 应能按照预设条件自动报警。

8.6.3 蓄电池组监测

可对UPS蓄电池组进行实时监控, 包括单体蓄电池的电压、表面温度、内阻、鼓包情况、组电压和充放电电流等参数, 蓄电池组出现异常时, 应能按照预设条件自动报警。

8.6.4 精密配电柜监测

可实时监测精密配电柜进线电源的三相电压、三相电流、三相电能、各支路的电流、功率因数、有功功率和各支路的空开状态等参数, 精密配电柜出现异常时, 系统应自动报警。

8.6.5 直流/交流配电屏监测

可实时监测直流/交流配电屏输出电压、电流、各支路开关和熔断状态等参数, 一旦发生故障或报警, 应能通过系统发出对外报警。

8.6.6 静态开关柜(STS)和动态开关柜(ATS)监测

可实时监测STS、ATS输入电源的三相电压、电流、功率因数、有功功率、无功功率、断路器、各空开和设备运行状态等参数, 出现异常或故障时, 系统应立即启动报警。

8.6.7 精密空调监控

可对机房内精密空调的运行状态及参数进行实时监控, 同时可对精密空调进行远程开关机控制操作。

8.6.8 普通空调远程监控

可实时监控机房内普通空调运行状态, 包括回风温度、送风温度、空调模式、开关机状态和

来电自启动等，确保机房保持正常的温湿度范围，使数据中心服务器等设备在恒温恒湿的环境下稳定运行。

8.6.9 温湿度监测

可实时监测机房温湿度状况，一旦温湿度异常，系统能自动报警。

8.6.10 漏水监测

可对机房实时进行漏水监测，一旦机房发生漏水，系统能自动报警。

8.6.11 防雷监测

可实时监测防雷器提供的干接点报警状态，一旦发生报警情况，系统能立即对外发出报警。

8.6.12 消防监测

可实时监测机房内的烟雾状态，监测机房内火警情况，一旦发生报警，系统能自动报警。

8.7 性能指标

运行维护管理技术平台系统应支持 ≥ 200 个用户并发，访问平均响应时间应 $< 3s$ ，复杂查询和统计的平均响应时间应 $< 6s$ 。

9 运行维护队伍和组织

9.1 队伍与人员

应建立信息化运行维护组织机构，信息化部门为机构负责部门，其他相关业务部门为机构成员。各级信息化运行维护组织机构按照实际情况制定各部门运行维护工作职责分工。队伍与人员包括运行维护服务提供者、运行维护服务使用者和运行维护服务管理者三类角色。包括以下要求：

A) 运行维护服务提供者应具备中国安全防范产品行业协会颁发的“安防工程企业设计施工维护能力证书”，等级为二级以上的单位。

B) 运行维护人员应具备省级职业技能鉴定指导中心颁发的“视频监控系统安装和运行”或“入侵报警系统安装和运行”等安防行业相关“专项职业能力证书”人员；

C) 运行维护人员应具备省级安全技术防范行业协会或省级职业技能鉴定指导中心颁发的“智能楼宇管理员”、“安全防范系统安装维护员”等安防行业相关“职业技能等级（职业资格）证书”，等级为三级以上人员。

D) 运行维护服务提供者主要是提供运行维护服务的单位或个人，职责如下：

- 1) 负责提供信息化运行维护服务；
- 2) 负责对运行维护服务对象进行管理。

E) 运行维护服务使用者主要是所有使用运行维护服务的单位或个人，职责如下：

- 1) 按相关要求和规范，正确地使用信息化设备设施，及时遵守运行维护管理者的相关通知及要求；
- 2) 及时按流程向运行维护服务提供者报修、请求响应，且应尽可能详尽地描述报修或请求响应的内容；
- 3) 对运行维护服务提供者进行客观、公正地评价；

4) 可向服务台和运行维护服务管理者进行投诉。

F) 运行维护服务管理者主要包括部级、省级和监狱三级信息化部门，职责如下：

1) 负责管理、检查、监督运行维护服务提供者按SLA执行的情况；

2) 负责对运行维护服务提供者进行考核和评估，以改进运行维护服务质量；

3) 负责协调、处理运行维护使用者的投诉和其他意见；

4) 负责履行SLA约定的责任和义务；

5) 按照实际运行维护服务的工作量和难易程度核定运行维护服务提供者的人员员额、准入标准、人员技能要求和工作规范要求等。

9.2 运行维护组织

9.2.1 基本要求

应建立信息化（安防系统）运行维护组织机构，信息化部门为机构负责部门，其他相关业务部门为机构成员。省和监狱各级信息化运行维护组织机构按照实际情况制定各自的运行维护工作职责分工。

9.2.2 省级运行维护组织机构、职能及管理架构

A) 组织机构

省级运行维护组织机构应为省监狱管理局信息化部门。

B) 职能

1) 按司法部监狱管理局信息化部门的相关要求落实运行维护管理工作；

2) 指导和监督所管辖监狱做好运行维护管理工作；

3) 发布运行维护管理的相关信息和要求；

4) 从技术和业务上指导所管辖监狱的运行维护管理工作；

5) 做好省监狱管理局信息化设备设施的运行维护管理工作，并对运行维护服务提供者进行考核。

C) 管理架构

省级运行维护管理架构可参照部级运行维护管理架构，并结合本省的情况制定符合本省实际的管理架构。

9.2.3 组织机构

监狱运行维护组织机构应为监狱信息化部门。

A) 职能

1) 按省级运行维护组织的相关要求落实本监狱的运行维护管理工作；

2) 组织开展本监狱运行维护管理工作；

3) 发布运行维护管理的相关信息和要求；

4) 从技术和业务上指导运行维护服务提供者落实相关工作；

5) 做好监狱信息化设备设施的运行维护管理工作，并对运行维护服务提供者进行考核。

B) 管理架构

监狱运行维护管理架构可参照省级运行维护管理架构制定符合本监狱实际的运行维护管理

架构。

10 运行维护经费

10.1 基本要求

年度运行维护经费应包括年度硬件运行维护经费和年度软件运行维护经费，对复杂和核心的信息化系统运行维护还可包括运行维护设计经费。

目前，湖北省各监狱运维经费标准参考《关于印发湖北省省级办公用房维修等省级通用项目预算支出标准的通知》（鄂财预发〔2023〕40号文）执行，如遇政策调整，以最新政策要求为准。

10.2 年度硬件运行维护经费

年度硬件运行维护经费包括维护保养服务费、备品备件购置费和其他费用。

A) 维护保养服务费：指开展日常维护保养工作、承担维护保养责任和义务所需的费用。可包括驻场劳务服务费、非驻场服务费、企业管理费、利润和税金等；

B) 备品备件购置费：指保障信息化系统正常运行需要进行的备品备件购买、维修和更换等费用；

C) 其他费用：指A、B项之外的其他费用，包括但不限于系统或设备检测费、重大节假日/重大活动费、基础环境运行维护费、云服务租赁费、托管费、线路租赁费、机房租赁费和特殊原因需运行保障而产生的费用。

年度硬件运行维护经费应按信息化硬件资产购置使用年限进行取费计算，计费额基准应为信息化硬件设备资产总金额。取费规则应符合表3规定。

监狱可根据实际情况对表3中各子项费率进行调整，总费率不低于其中总费率的取费规则。

表3 年度硬件运行维护经费取费规则

序号	费用名称	购置使用年限 ≤3年费率	3年<购置使用年限≤5年费率	购置使用年限 >5年费率
1	维护保养服务费	4%	5%	6%
2	备品备件购置费	8%	9%	10%
3	其他费用	1%	2%	3%
总费率		13%	16%	19%

10.3 年度软件运行维护经费

软件运行维护和升级宜采取单一来源方式确定供应商。年度软件运行维护经费要求如下：

- A) 年度软件运行维护经费取费应参照年度硬件运行维护经费的维护保养服务费执行；
- B) 软件的升级改造应根据实际情况按项目进行单独测算，相关费用纳入保障。

10.4 运行维护设计经费

运行维护设计经费计算方法采用差额定率累进法，应符合GA/T 70-2014文的规定，计费额基准应为信息化软件资产和信息化硬件资产总金额。取费规则应符合表4规定。

表4 运行维护设计经费取费规则

序号	计费额（万元）	费率%
1	<10	2.25
2	10~50（含）	2.16
3	50~100（含）	2.10
4	100~200（含）	1.98
5	200~500（含）	1.85
6	500~1000（含）	1.68
7	1000 以上	1.50

11 运行维护管理指标

11.1 总体指标

运维服务管理的总体目标包括

- A) 服务响应及时率 $\geq 98\%$;
- B) 系统故障修复率 $\geq 95\%$;
- C) “1252”工程相关网络系统全年正常运行率 $\geq 99\%$;
- D) 服务满意率 $\geq 95\%$;
- E) 实现信息资产的保密性、完整性和可用性安全保障;
- F) 为业务用户提供及时的、持续的和高品质的信息技术服务并不断改进。

11.2 运行维护管理指标的定制

运行维护管理指标应根据各单位的需求进行定制和扩充。各类信息化运行维护服务管理的指标通常包括但不限于:

信息系统基础设施和应用系统运行维护服务的运行维护管理指标, 包括:

- A) 监控类服务: 异常报告及时率和异常漏报率等;
- B) 日常维护类服务: 维护作业计划的及时完成率、故障隐患发现率、故障服务请求及时满足率和问题解决率等;
- C) 维修保障类服务: 服务响应及时率、到达现场及时率、故障修复及时率和客户满意度等。

11.3 内容信息服务的运行维护管理指标

内容信息服务的运行维护管理指标通常包括但不限于:

- A) 检索成功率;
- B) 响应及时率。
- C) 综合管理指标, 包括:
 - 1) 平均响应时间;
 - 2) 问题解决比率。

12 运行维护考核办法

12.1 运行维护考核办法

A) 为了保障监狱信息化（安防系统）基础设施安全稳定运行，切实加强信息技术维保人员的规范管理，特制定本办法。

B) 本办法所称信息技术维保人员（以下简称维保人员），是指由信息化项目承建单位或服务外包承包单位按照合同约定派遣的长期驻点在监狱提供信息化项目质保或运行维护保养服务的人员。

C) 本办法适用于本监狱各类信息化（安防系统）软、硬件设施的运维保养行为。

12.2 管理要求

A) 监狱信息化管理科为信息技术维保人员的管理部门，负责全过程的管理、考核、监督、指导维保人员的维保工作。

B) 管理部门要全面落实《中华人民共和国网络安全法》等法规要求，对维保人员进行安全背景审查，与其签订保密协议，并定期开展安全检查和安全教育。项目结束时或维保人员离岗离职时，应落实专人对离职离岗人员开展保密教育，并全覆盖签订离岗保密承诺书，督促其清退或删除涉及监狱信息的各类书面、电子资料。实行发生网络安全重大问题“一票否决制”。

C) 管理部门应给每名维保人员分配唯一、高强度、定期更换密码的操作账号，设置相应的操作权限，实现操作行为精准监管。严禁多名维保人员共用一个操作账号。

D) 维保人员的维保行为应在管理部门的监管下进行，管理部门应定期对维保人员开展考核评价，对维修单据进行审核。

12.3 工作要求

A) 维保人员须根据合同约定提供相应的维保服务。

B) 维保人员每天上下班进行打卡，周末与节假日均须安排人员值守，遵守上下班纪律，有事须提前请假。每月制定排班表，一份交于指挥中心，一份交于信息化管理科，如有换班要提前告知，做到随时待命。

C) 维保人员的电话必须24小时开机，休息日不值班的维保人员至少保证一种能被及时联系到的联络方式。

D) 维保人员须做好办公场所和仓库的卫生打扫和办公物品的定置管理，由管理部门不定期开展检查。

E) 维保人员须对每次维保任务进行当日记录，填写书面维修单，并将维修单按月整理成册，作为监狱考核维保人员的重要依据，管理部门定期或不定期进行抽查。对于民警投诉较多、满意度较差（包括技术能力、服务态度等）且累计三个月考核不合格的维保人员，监狱有权向维保人员所在单位提出撤换要求。

F) 维保人员须每日对所有设备在线情况进行在线巡查，每月配合管理部门对所有机房进行现场巡查并完成巡检月报，每季度对UPS、精密空调、机房灭火系统、防雷系统等重要设备进行专业技术检测和维护保养并出具检测报告，每半年对所有设备进行一次保养（包括清理蛛网、除

尘、调整清晰度等），对发现的问题要限期解决。

G) 所有设备的维修均应在监狱内部进行，确需送修或返厂的设备，须经过管理部门确认同意并拆除设备中的存储部件后送出，并做好记录。如维修涉密设备，必须具备相应涉密资质且在管理部门监督下进行。

H) 维保人员须提供7*24小时的服务响应，在接到维修通知后白天半小时内、夜间一小时内开展维修，并在4小时内修复故障。因客观原因（如现场漏水、基建设施破坏等）导致无法修复的问题要向管理部门报备，并在具备修复条件后一天内完成修复。因问题复杂一天内无法修复的，要提出相应的解决方案和维修期限。如设备需要拆回维修，维保要提供备用设备替代使用。

I) 维保人员有义务做好监狱内部资料的保密工作。在维保服务期间掌握的一切资料信息（包括但不限于视频资料、设备配置、平台账号密码、施工图纸、监狱内部资料）均不得私自外借、转发和复制。

12.4 考核要求

A) 管理部门每月根据维保人员工作纪律、工作实绩两大方面进行评分，基础分为100分，得分85分以上为合格，85分以下为不合格。

B) 管理部门每季度对维保公司服务情况开展服务满意度调查，由各支部分别对维保公司进行评价，不合格数超过40%则总体评价为不合格。

13 运维内容及运维服务评价方法

13.1 一般要求

A) 评价分为：1. 运维整体质量考核指标（300分）、2. 应急响应处置考核指标（200分）、3. 日常运维考核指标（100分）、4. 安全规范指标（300分）、5. 优化提升指标（100分）；

B) 评价总分为1000分，按分项打分总和；

C) 总分900及以上的为优秀，800及以上的为良好，700分以上的为合格，

D) 700分以下需立即整改，重新评价。

附 录 A

(资料性)

运维内容及运维服务相关用表

A-1 监狱维保人员考核表

考核月份:

被考核人:

考核时间:

考核人:

考核内容	考核条款	得分
工作纪律	将手机带入罪犯生活、劳动区域的，一次扣100分。	
	保密意识不强，设备或资料保管不当，造成监狱内部工作秘密泄露或网络安全事故，一次扣100分。	
	迟到或早退一次扣1分，无故旷工一次扣5分。	
	下班后办公室空调、电灯、电脑等未关的，一次扣1分。	
	通讯不畅通，联系不上，一次扣0.5分。	
	维修中工具管理不到位，将维修工具遗留在罪犯生活、劳动区域，一次扣5分。造成严重后果的，扣100分。	
	利用工作间接私活做兼职的，一次扣3分。	
	消极怠工，不服从监狱工作安排，视情一次扣1~5分。	
	办公室卫生状况差，垃圾不及时清理，物品摆放杂乱，一次扣1分。	
	工作时间做与工作无关的事，在办公室看电影、玩游戏、打牌等，一次扣1分。	
工作实绩	因违反监狱规章制度，被监狱指挥中心通报的，视情一次扣1~5分。	
	工作效率低，没有时间观念，接到报修后未在规定时间内响应，视情一次扣1~10分。	
	未按规定时间开展巡检和保养工作，同一运维服务项目的所有运维人员均扣10分。	
	维修单据记录不清晰不完整，未按时上交月报，技术巡检未开具巡检报告，或存在造假行为的，视情扣1~5分。	
	机房、弱电间卫生状况差，灰尘较多未清理的，一次扣2分。	
	业务能力、服务态度差，收到民警投诉的一次扣0.5分，电话回访民警不满意的一次扣0.5分。	
	同一类型设备中故障设备占比超过1%，一次扣3分。	
	维修不及时，超出约定时间的，一次扣2分。	
	因操作不当导致故障情形加重或故障范围扩大的，视情扣1~10分。	
	工作中主动发现隐患并改善，避免事故发生的，视情一次加1~5分。	
奖励加分	积极完成监狱安排的额外临时性任务，表现较好的，视情加1~10分。	
	工作表现突出，受到单位或领导表扬的，视情加1~3分。	
	当月全勤加5分。	
总分	总分=100+加分-扣分	

A-2 信息化安防系统故障处理单

报修单位		报修人		报修时间	
故障情况 及位置					
维修内容及配件 更换情况					
维修人员 名单					
管理部门 审核意见					
验收意见	验收人签名： 年 月 日				

A-3 信息化安防系统维保服务评价表

服务单位	_____公司		
服务内容			
服务时间	_____年 _____月 _____日 ———— _____年 _____月 _____日		
使用单位	维保服务评价（分为“合格”“不合格”）		
一监区（盖章） 经办人：		二监区（盖章） 经办人：	
三监区（盖章） 经办人：		四监区（盖章） 经办人：	
XXXXX（盖章） 经办人：		XXXXX（盖章） 经办人：	
狱政科（盖章） 经办人：		指挥中心（盖章） 经办人：	
总体评价： 业务管理部门（盖章） 经办人： 日期：			

A-4 项目运维月报样表

(月)

本月总体运行情况	主要描述本月巡检次数（包括线上巡检和实地巡检），常规维护保养次数，共计解决各类故障次数（包括软件故障和硬件故障），耗材使用数量，维保人员出勤情况、响应情况等内容。
巡检问题汇总分析	对本月巡检中（包括线上巡检和实地巡检）中发现的问题进行汇总、分类，分析问题原因、解决方案，提出合理化建议。
上月巡检问题解决整改情况	对上月巡检发现的问题的解决和整改情况。

A-5 参考考核指标

考核项目	分数	考核方法
一、运维整体质量考核指标	(总分300分，扣分制)	
1. 系统整体可用性	单个系统/平台离线/宕机：每次扣5分	通过系统监控平台（如Zabbix、Nagios）导出运行状态报表，结合值班日志核实离线/宕机时间；
	单次离线/宕机超2小时：每超1小时加扣10分（最高单次故障扣分不超过系统上限）。	核查故障恢复时间记录，确认超时扣分依据。
2. 前端设备故障率	单类设备故障率 $\geq 2\%$ ：扣10分/类；	核查设备巡检记录表及故障工单，计算故障率（故障次数/设备总数 $\times 100\%$ ）；
	单类设备故障率 $\geq 10\%$ ：扣40分/类；	现场抽查设备运行状态（如摄像头在线率、门禁响应速度）。
	因故障导致安防失效（如监控盲区）：每次额外扣20分。	
3. 系统功能稳定性	功能、接口不稳定（响应超时、报错率 $\geq 5\%$ ）影响监狱工作业务：每项扣20分；	通过接口监控工具（如Postman、API测试报告）核查成功率及错误类型；
	导致业务中断超1小时：额外扣10分。	查看业务部门反馈记录，确认是否因接口问题影响使用。
4. 系统整体兼容性	新设备/系统接入未报备兼容性测试方案：每次扣10分；	核查新设备/系统接入前的测试方案报备记录及测试报告；
	因兼容性问题导致故障且未24小时内解决：每次扣30分。	查看故障工单及技术分析报告，确认是否因兼容性问题引发故障。
二、应急响应处置考核指标	(总分200分，扣分制)	

1. 响应时效性	接到通知后未在 30分钟内首次电话响应 ：每次扣15分；	核查应急事件工单或值班记录，确认接警时间、首次响应时间、到达现场时间；
	未在 1小时内到达故障现场 （以签到或定位记录为准）：每次扣15分。	结合现场签到表或GPS定位记录验证到场时效。
2. 问题定位与处置效率	故障原因未在 3小时内准确定位 ：每次扣10分；	查看故障处理全流程记录（如故障描述、排查步骤、修复时间、复盘报告）；
	未在 24小时内完成故障修复 （以系统恢复正常运行时间为准）：每次扣30分。	核对系统恢复时间与工单关闭记录。
3. 现场处置规范性	未按《监狱安防系统应急操作规程》操作导致事故扩大：每次扣20分；	现场检查应急处置过程录像或旁站监督记录；
	因违规操作导致人员受伤或设备损坏：按损失程度加扣20~50分。	核查事故扩大的原因分析及损失评估报告。
4. 事后分析与改进	未在 72小时内提交事件分析报告 （需包含根本原因、整改措施）：每次扣10分；	查看事件分析报告的提交时间、内容完整性及整改措施落实记录；
	同一类型问题 3个月内重复发生 ：每次加扣20分。	核查同类事件工单记录及整改闭环验证材料。
5. 演练与实战匹配度	应急演练方案与实际事件处置流程存在较大 差异 ：每次扣5分；	对比演练方案与实际事件处置流程记录，统计关键差异项；
	差异导致演练失败或效果不佳：加扣10分。	查看演练评估报告中对场景真实性的评分及改进记录。
6. 预案动态更新	未根据演练结果或事件教训在 15日内更新预案 ：每次扣5分；	核查预案版本号、修订记录及修订依据（如演练评估报告、事件分析报告）；
	预案未覆盖关键场景或责任不明确导致事件处置失败：每次扣15分。	通过事件处置记录验证预案的适用性及执行效果。

7. 系统恢复完整性	系统恢复后未执行 功能验证测试 或遗留问题未闭环：每次扣8分；	
	因恢复不彻底导致 72小时内再次发生同类故障 ：每次扣15分。	
三、日常运维考核指标	（总分100分，扣分制）	
1. 日常巡检执行率	未按计划完成巡检：每次缺检扣2分，漏检（未覆盖全部区域或设备）扣1分/次；	核查巡检记录表（纸质/电子版），确认计划完成率及覆盖范围；
	单月累计缺检≥3次：额外扣5分。	现场抽查设备状态与记录一致性。
2. 巡检记录规范性	记录不完整（如未填写时间、人员、设备状态）：每次扣1分；	抽查巡检记录内容，对比实际设备状态；
	关键问题未记录（如设备异常、安全隐患）：每次扣3分；	通过监控录像或第三方反馈确认记录真实性。
	记录弄虚作假：每次扣5分。	
3. 系统测试规范性	未按月度计划测试通讯、报警、视频会议、安防系统等连通性或稳定性：每项未测试扣5分；	查看系统测试计划及测试报告，确认测试频率与覆盖范围；
	测试结果异常未闭环整改：每项扣8分。	核查异常问题的整改记录及闭环证明。
4. 人员组织规范性	未按预案组织响应数量的运维人员到场：每少1人扣5分；	核查人员出勤记录及资质文件（如证书、培训合格证明）；
	人员资质不符（如无相关证书或未通过考核）：每人扣10分；	查看任务执行记录或故障报告，确认人员响应效率与协作效果。
	团队协作不力导致任务延误：扣15分。	
5. 交接规范	人员变动未履行审批报备交接流程：每次扣8分；	查看交接记录表、审批单及签署确认文件；
	工作交接不完整（如未移交密码、文档或未说明故障隐患）：每次	通过故障工单或事故报告追溯交接问题的影响。

	扣5分；	
	因交接问题导致系统故障：扣20分。	
6. 备用设备/备件管理	备用设备未按季度检测或检测记录缺失：每次扣5分；	
	备件库存低于安全阈值（如低于需求量的30%）：每次扣10分；	
	应急使用时设备故障或备件不足：每次扣15分。	
四、安全和规范指标	（总分300分，扣分制）	
1. 安全事故	发生火灾、安全生产事故、监管安全事故、人员伤亡、网络安全重大事故等，实行一票否决	根据省局、监狱或其他官方文件通报。
2. 物理安全（防火/防水/防雷）	电线电缆未按规定敷设导致火灾隐患（如未穿管、绝缘破损）：每处扣20分；	现场检查电缆敷设、设备防水、防雷接地设施；
	设备未防水处理（如机房渗水、设备泡水）：每处扣15分；	核查防雷检测报告及静电防护装置有效性记录。
	防雷接地未定期检测或失效：每次扣10分；	
	因静电未防护导致设备损坏：每处扣10分。	
3. 监管安全制度执行	未按规定管理危险劳动工具（如未按编号管理、未按规定保管）：每次扣50分；	查看危险工具台账、工具进出监记录；
	携带违禁品、违规品（如手机、火种、现金等）进入监管区：每次扣100～300分；	核查监控录像或巡查记录，确认违规行为发生及处理情况。

	施工时与罪犯攀谈、传递物品/信息：每次扣50~200分。	
4. 用电、动火作业规范性	未办理动火/用电作业审批：每次扣15分；	查看动火/用电作业审批单及现场安全措施记录；
	动火作业未配备灭火器或未隔离易燃物：每次扣30分；	抽查用电设备负载率及线路安全状态（如红外测温）。
	临时用电未按规定接线或超负荷运行：每处扣30分。	查看监狱、指挥中心等文件通报
5. 登高作业规范性	未佩戴安全帽、安全绳或未系牢：每次扣20分；	现场监督或通过监控录像核查作业人员防护装备及操作流程；
	未设置安全监护人：每次扣10分；	核查登高作业审批单及监护人履职记录。
	超过安全高度未使用专业设备（如脚手架）：每次扣20分。	
6. 网络安全制度建设	未制定网络安全管理制度或未更新（如未涵盖新系统）：扣20分；	查看网络安全管理制度文件及版本号；
	不定期组织网络安全培训（年度少于2次）：扣15分；	核对培训记录、签到表及制度执行过程文档。
	未留存制度执行记录（如会议纪要、签到表）：扣10分。	
7. 网络安全技术防护	管理员密码未定期更换（超过90天）或弱口令（如“123456”）： 每个账号扣10分；	通过密码审计工具核查密码复杂度及更新记录；
	用户权限分配未遵循最小权限原则：每处扣15分；	检查权限分配表与角色职责匹配度；
	未在7日内修复高危漏洞：每个漏洞扣20分。	核查漏洞扫描报告及修复闭环记录。
8. 技术文档规范	未建立技术台账（如设备清单、网络拓扑图）：扣20分；	现场检查技术台账完整性及更新时间戳；
	台账更新滞后（超过3个月未更新）：扣5分；	核对文档版本号、签署人及归档记录。

	交付文档缺失或错误（如未标注版本号）：扣10分/次。	
9. 设备标识规范	设备/线缆未使用机打标签或标签信息错误：每处扣8分；	现场抽查设备标签、线缆标识及走线规范性；
	标签脱落、模糊或未及时更新：每处扣5分；	核对机房/设备间图纸与实际标识一致性。
	线缆走线未按规范（如强弱电混杂、未绑扎）：每处扣10分。	
五、优化提升指标	满分100分，加分制	
1. 系统性能优化	系统响应速度提升 $\geq 10\%$ ：加10分，每提升1%加1分，最高加20分。	提供性能对比报告（如响应时间、资源利用率）、优化方案及验收测试结果。
2. 主动隐患排查	提前发现并消除重大安全隐患（如系统漏洞、硬件故障）：每次加20分	提交隐患排查记录、风险评估报告及闭环处理证据（如漏洞修复截图）。
3. 技术创新应用	引入新技术新手段提升安防能力：最高加20分。	提供技术方案、试点效果数据（如误报率降低）、推广计划或专利/奖项证明。
4. 用户满意度提升	客户对运维服务满意度 $\geq 90\%$ ：最高加20分。	发放满意度调查问卷（需覆盖至少70%用户），统计评分结果及改进建议。
5. 标杆案例或奖项	获得监狱系统内/行业奖项或形成可复制的运维经验推广：最高加20分。	获奖证书、表彰文件、案例文档或推广材料

参 考 文 献

- [1]GB/T 28827.2—2012信息技术服务运行维护 第2部分：交付规范
 - [2]GB/T 28827.3—2012 信息技术服务 运行维护 第3部分：应急响应规范
 - [3]GB/T 28827.4—2019 信息技术服务 运行维护 第4部分：数据中心服务要求
 - [4]GB/T 28827.6—2019 信息技术服务 运行维护 第6部分：应用系统服务要求
 - [5]GB/T 51314—2018 数据中心基础设施运行维护标准
 - [6]GB/T 29264—2012 信息技术服务 分类与代码
 - [7]SF/T 0008—2017 全国司法行政信息化总体技术规范
 - [8]SF/T 0028—2018 智慧监狱技术规范
 - [9]SJ/T 11564.5-2017 信息技术服务 运行维护 第5部分：桌面及外围设备规范
 - [10]司法通〔2016〕137号 司法部关于进一步加强司法行政信息化建设的意见
-