ICS 35.240.01
CCS A90

SF

中华人民共和国司法行政行业标准

SF/T 0088—2021

监狱信息化运行维护规范

Specification for operation and maintenance of prison informatization

2021－06－21 发布　　2021－06－21 实施

中华人民共和国司法部　　发布

目　　次

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。

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。

本文件由司法部信息中心提出并归口。

本文件起草单位：司法部监狱管理局、四川省监狱管理局、电子科技大学、四川司法警官职业学院、北京环亚信通信息科技有限公司。

本文件主要起草人：赵巩、徐平原、骆登耀、甘昀匀、张力、余训锋、蒋涛、徐贤勇、曹明生。

监狱信息化运行维护规范

1 范围

本文件规定了监狱信息化运行维护体系的总体架构和主要内容、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。

本文件适用于监狱信息化的运行维护服务和运行维护管理工作。

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—2012 信息技术服务 运行维护 第1部分：通用要求

GB/T 33745—2017 物联网 术语

GB/T 35295—2017 信息技术 大数据 术语

GB 50348—2018 安全防范工程技术标准

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

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件。

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的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。

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。

[来源：GB/T 28827.1—2012，3.2，有修改]

4 总体架构和主要内容

4.1 总体架构

监狱信息化运行维护主要包括监狱信息化运行维护服务和监狱信息化运行维护管理。

运行维护服务是采用信息技术手段和方法，依据监狱信息化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。监狱信息化运行维护服务可采用完全外包服务模式或辅助警务机制进行。

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。

监狱信息化运行维护总体架构如图1所示。

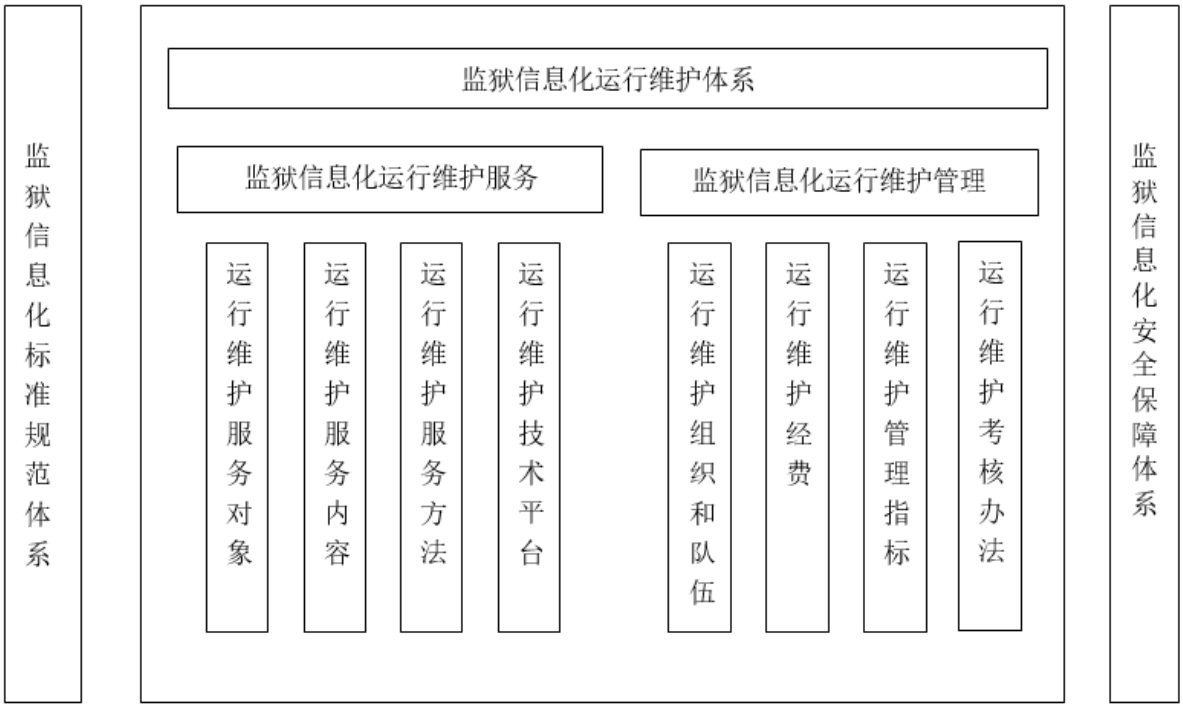

图1　监狱信息化运行维护总体架构

4.2　主要内容

4.2.1　监狱信息化运行维护服务

监狱信息化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。内容如下：

a)　运行维护服务对象：包括但不限于信息系统基础设施和信息应用系统；

b)　运行维护服务内容：包括但不限于服务台、事件管理、问题管理、配置管理、变更管理、发布管理、服务级别管理、能力管理、可用性管理、服务持续性管理、知识管理、资源库管理、备品备件管理、文档管理、资产管理、综合管理和应急保障；

c)　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。包括但不限于信息系统基础设施运行维护服务方法和信息应用系统运行维护服务方法；

d)　运行维护技术平台：是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。包括但不限于智能监控、视频质量监测、管理与分析、大屏展示、云服务平台管理、机房动环监控和相关性能指标。

4.2.2　监狱信息化运行维护管理

监狱信息化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：包括部、省和监狱三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，以持续保障监狱信息化运行维护服务的开展；

c)　运行维护管理指标：是监狱信息化运行维护管理所需的各项指标；

d)　运行维护考核办法：是保障监狱信息化运行维护所需的各项考核办法。

4.2.3　监狱信息化标准规范体系

监狱信息化标准规范体系包括监狱信息化所需的各类标准和规范。

4.2.4 监狱信息化安全保障体系

监狱信息化安全保障体系是为监狱信息化提供各类安全技术保障。

5 运行维护服务对象

5.1 信息系统基础设施

信息系统基础设施应包括以下内容：

a) 机房与机房基础设施：包括但不限于机房、电气系统、空调系统、消防系统、防雷接地系统、环境监控系统和综合布线系统；

注1：电气系统：指与信息系统相关的机房供电系统，如：（不间断电源）UPS系统。

注2：消防系统：指与信息系统相关的机房消防系统。

b) 网络设施：包括但不限于加密网、政务外网、互联网、其他专网（政府部门专网/自建专网）的路由器、交换机、通信设备、传输设备和传输链路；

c) 计算与存储设施：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 5G 移动边缘计算（5G MEC）相关的计算设备和存储设备；

注3：ARM 服务器：指采用基于ARM体系架构的处理器作为CPU 的服务器。

注4：X86服务器：指采用基于X86体系架构的处理器作为CPU 的服务器。

d) 物联网设施：包括但不限于电子戒具、生命探测设备、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、移动执法终端、目标跟踪系统、智能押解系统、无人机系统和配套设备设施；

e) 指挥调度设施：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、操作终端、安防集成平台、会议系统和视频点名系统；

f) 安防设施：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；

g) 桌面设施：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；

h) 应用支撑基础设施：包括但不限于操作系统、数据库和中间件；

i) 信息安全设施：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、加密卡、USB Key 和杀毒软件；

注5：USB Key：是用于保存数字证书和用户私钥的USB接口的硬件设备。

j) 信息资源与数据：包括但不限于罪犯信息库、警察职工信息库和监狱管理信息库。

5.2 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，包括但不限于办公自动化（OA）系统、地理信息系统（GIS）、业务管理系统、罪犯管理系统、警务管理系统、政法协同系统、指挥调度系统和行政后勤系统。

6 运行维护服务内容

6.1 服务台

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。

6.2 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。

6.3 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。

6.4 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。

6.5 变更管理

变更管理的目的是通过管理和控制变更的过程，确保更有序的实施。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。

6.6 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。

6.7 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。

6.8 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。

6.9 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。

6.10 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。

6.11 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。

6.12 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。

6.13 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。

6.14 文档管理

6.14.1 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) 字纸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。

6.14.2 文档管理的内容

6.14.2.1 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。

6.14.2.2 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。

6.14.2.3 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。

6.14.2.4 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：

a) 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。

b） 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。

c） 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。

d） 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。

6.15 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，以降低监管安全风险。资产设备使用年限按照 GB 50348—2018 中 11.1.4 的规定执行。

6.16 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。综合管理要求如下：

a） 咨询与培训服务
  1） 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 7×24 小时咨询服务；
  2） 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；
  3） 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；
  4） 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；
  5） 培训服务完成后应进行培训考核，确保培训质量；
  6） 培训服务方式可采取远程培训或现场培训等方式进行。
b） 技术支持服务
  1） 运行维护服务提供者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；
  2） 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；
  3） 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。
c） 综合系统服务

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。

6.17 应急保障

6.17.1 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。如图2所示：

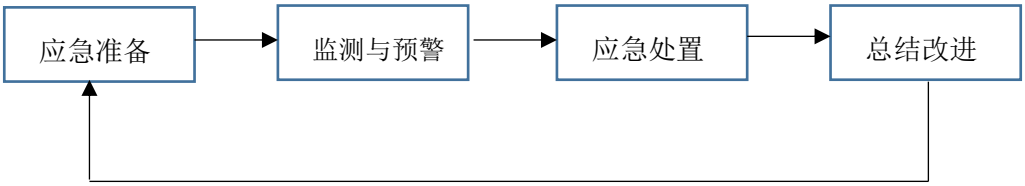

图2 应急响应过程

6.17.2 应急响应各阶段的工作内容

应急响应各阶段的工作内容如下：

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的处理和系统恢复、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。

6.17.3 应急准备

应急准备要求如下：

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。

6.17.4 监测与预警

监测与预警应包括以下要求：

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。

6.17.5 应急处置

应根据应急预案进行应急事件的处置。

6.17.6 总结改进

总结改进应包括以下要求：

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 信息系统基础设施运行维护服务方法

7.1.1 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。运行维护服务方法要求如下：

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 进行放电测试应≥1 次/0.5 年，保证 UPS 电池活性，及时检查 UPS 放电时间，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。

7.1.2 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≤1 个月，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。

7.1.3 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5G MEC相关的计算设备和存储设备的运行维护。运行维护服务方法要求如下：

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。

7.1.4 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、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。

7.1.5 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。运行维护服务方法要求如下：

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。

7.1.6 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/1 季度进行定期设备除尘，室内安防设备应≥1 次/0.5 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。

7.1.7 桌面设施运行维护服务方法

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：

a) 应建立桌面设施运行维护管理制度；
b) 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；
c) 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；
d) 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；
e) 应≥1 次/年组织用户培训，提升用户使用水平；
f) 应不定期发布桌面和外围设备风险安全隐患报告；
g) 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。

7.1.8 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。运行维护服务方法要求如下：

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

7.1.9 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、加密卡、USB Key和杀毒软件的运行维护。信息安全设施运行维护服务方法要求如下：

a) 应制定信息安全管理制度，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) 宜制定有效的应急预案，并定期开展演练；
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，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。

7.1.10 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。信息资源与数据的运行维护服务方法要求如下：

a) 应制定信息资源与数据运行维护服务的日常管理制度，建立管理规范和流程；
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。

7.2 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OA系统、GIS、业务管理系统、罪犯管理系统、警务管理系统、政法协同系统、指挥调度系统和行政后勤系统的运行维护。信息应用系统运行维护服务方法要求如下：

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 1 次/天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

业务全栈跟踪包括以下要求：

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/分钟等关建指标，超过设定的指标阀值应能预警。

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用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、视频剧变、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。

8.3 管理与分析

8.3.1 报修管理

报修管理要求如下：

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

工单管理要求如下：

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

资产管理要求如下：

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

拓扑管理要求如下：

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的区分监控对象正常、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

告警管理要求如下：

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

巡检管理要求如下：

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

知识及问题管理要求如下：

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

应急演练管理应包括以下要求：

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

报表管理要求如下：

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

专家信息库管理要求如下：

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

8.3.11.1 运行维护分析

运行维护分析应包括以下要求：

a) 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；

b) 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；
c) 具备基于服务器 CPU、内存和磁盘等性能利用率的分析功能；
d) 具备基于设备类型、厂家、型号和质保期的资产分析功能。

8.3.11.2 运行维护研判

运行维护研判要求如下：

a) 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；
b) 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

大屏展示应包括以下要求：

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

云服务平台的管理要求如下：

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

供配电系统监测要求如下：

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测，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测，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。
b) 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，且应尽可能详尽的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、公正的评价；
   4) 可向服务台和运行维护服务管理者进行投诉。

c） 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。部、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 部级运行维护组织机构、职能、管理架构

9.2.2.1 组织机构

部级运行维护组织机构为司法部监狱管理局信息化部门。

9.2.2.2 职能

职能应包括以下要求：
a） 起草和修订运行维护规范，并指导各省、监狱运行维护管理机构落实运行维护规范；
b） 外联各省、监狱运行维护管理机构做好运行维护管理工作；
c） 发布运行维护管理的相关信息和要求；
d） 从技术上、业务上指导各省、监狱运行维护管理机构开展相关工作；
e） 会同司法部网信管理部门做好司法部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。

9.2.2.3 管理架构

管理架构如图3所示：

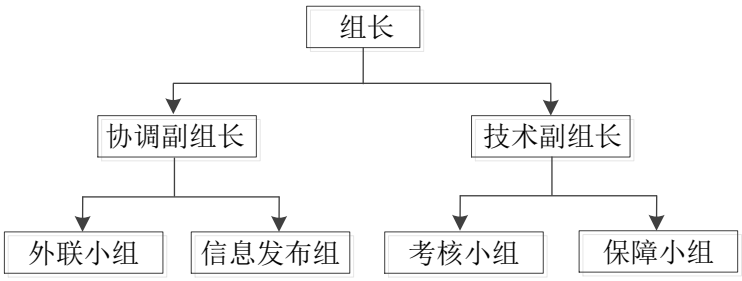

图3 部级运行维护组织管理架构

要求如下：
a） 组长宜由信息化部门的最高领导担任；
b） 协调副组长应主要负责日常事宜的协调、沟通和联系；
c） 技术副组长应主要负责相关技术问题的沟通、讨论和评估；
d） 外联小组应主要负责日常运行维护事宜的具体联系和处理；
e） 信息发布组应主要负责发布运行维护管理的相关要求、制度和预警信息等；
f） 考核小组应主要负责按照合同约定对运行维护服务的相关内容进行考核；
g） 保障小组应主要负责为运行维护过程提供技术支撑或保障。

9.2.3 省级运行维护组织机构、职能及管理架构

9.2.3.1 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。

9.2.3.2 职能

职能应包括以下要求：

a) 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；
b) 指导和监督所管辖监狱做好运行维护管理工作；
c) 发布运行维护管理的相关信息和要求；
d) 从技术和业务上指导所管辖监狱的运行维护管理工作；
e) 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。

9.2.3.3 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。

9.2.4 监狱运行维护组织机构、职能及管理架构

9.2.4.1 组织机构

监狱运行维护组织机构应为监狱信息化部门。

9.2.4.2 职能

职能应包括以下要求：

a) 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；
b) 组织开展本监狱运行维护管理工作；
c) 发布运行维护管理的相关信息和要求；
d) 从技术和业务上指导运行维护服务提供者落实相关工作；
e) 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。

9.2.4.3 管理架构

监狱运行维护管理架构可参照部级运行维护管理架构和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。

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。具体如下：

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)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1规定。

监狱可根据实际情况对表1中所有费率进行调整，总费率不低于表1的取费规则。

表1　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2规定。

表2　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	1.50

11　运行维护管理指标

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：

a)　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：

1)　监控类服务：异常报告及时率和异常漏报率等；

2)　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；

3)　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。

b)　内容信息服务的运行维护管理指标，包括：

1)　检索成功率；

2)　响应及时率。

c)　综合管理指标，包括：

1)　平均响应时间；

2)　问题解决比率等。

12　运行维护考核办法

运行维护考核办法要求如下：

a)　运行维护考核办法应量化打分细则，并在 SLA 中进行约定，并按照 SLA 的相关约定进行考核；

b)　运行维护考核应结合运行维护管理指标，把运行维护管理指标作为运行维护考核的重要数据支撑；

c)　运行维护考核应由运行维护管理者进行组织，用户单位审计、财务和监察等相关部门应参与考核；

d) 运行维护考核应包括运行维护例行考核和验收考核，运行维护例行进行考核应≥1 次/季度；

运行维护考核审查内容可包括运行维护团队基本情况审查、运行维护服务情况审查、运行维护资料文档情况审查和运行维护整改情况审查等方面，考核结果作为履约保证金退款、运行维护团队调整、合同续签和服务费用支付的重要依据。

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 29264—2012 信息技术服务 分类与代码
[6] SF/T 0008—2017 全国司法行政信息化总体技术规范
[7] SF/T 0028—2018 智慧监狱技术规范
[8] 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
[9] 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》