ICS 35.240.01
A16

SF

中华人民共和国司法行政行业标准

SF/T 0033—2019

公证数据中心建设和管理规范

Construction and management specification for notarization data center

2019-5-5 发布　　2019-5-20 实施

中华人民共和国司法部　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本标准由司法部公共法律服务管理局、中国公证协会提出。

本标准由司法部信息中心归口。

本标准起草单位：中国公证协会。

公证数据中心建设和管理规范

1 范围

本标准规定了公证数据中心建设的总体要求、总体架构及要求、机房建设要求、运维制度与安全管理制度。

本标准适用于司法行政公证管理部门、公证协会及各公证机构数据中心建设。

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 2589 综合能耗计算通则

GB/T 2887 计算站场地通用规范

GB/T 9361 计算站场地安全要求

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25070 信息安全技术 信息系统等级保护安全设计技术要求

GB 50174 电子信息系统机房设计规范

GB 50189 公共建筑节能设计标准

GB 50462 电子信息系统机房施工及验收规范

GB 51194 通信电源设备安装工程设计规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

机房使用率 used ratio of computer room

主机房、支持区、辅助区面积之和与机楼总建筑面积的比。

3.1.2

网络流量模型 network flow model

基于基本特征集合和组合特征集合两个层次的划分，实时从网络流量中提取的网络流量的基本特征数据。

示例：流量的大小、包长的信息、协议的信息、端口流量的信息和TCP标志位的信息等。

3.2 缩略语

下列缩略语适用于本文件。

API 应用程序编程接口 （Application Programming Interface）
CPU 中央处理器 （Central Processing Unit）
DNS 域名系统 （Domain Name System）
EVB 边缘虚拟桥 （Edge Virtual Bridging）
KVM 虚拟机 （Keyboard Video Mouse）
IaaS 基础设施即服务 （Infrastructure as a Service）
IDS 入侵检测系统 （Intrusion Detection Systems）
IP 互联网协议 （Internet Protocol）
IPS 入侵防御系统 （Intrusion Prevention System）
PaaS 平台即服务 （Platform as a Service）
PCI 外设组件互连标准 （Peripheral Component Interconnect）
SaaS 软件即服务 （Software as a Service）
SAN 存储区域网络 （Storage Area Network）
TCP 传输控制协议 （Transmission Control Protocol）
UPS 不间断电源 （Uninterruptible Power Supply）
VLAN 虚拟局域网 （Virtual Local Area Network）
VPN 虚拟专用网 （Virtual Private Network）

4 总体要求

4.1 规范化

选择设备应遵循EVB 802.1Qbg所要求的扩展支持能力，保证先进性。

4.2 可用化

可用化要求如下：

a) 在网络整体设计和设备配置上应采用双备份策略；
b) 在网络连接上应消除单点故障，提供关键设备的故障切换；
c) 关键设备之间的物理链路应采用双路冗余连接，按照负载均衡方式或双机热备方式工作；
d) 关键主机应采用双路网卡，应使用全冗余方式使系统达到99.999%的电信级可靠性。

4.3 性能化

纵向流量转换成复杂的多维度混合方式，应使整个系统具有较高的吞吐能力和处理能力。

4.4 开放接口

开放接口要求如下：

a) 应提供开放的API接口；
b) 应保证服务器存储、网络等资源能够通过API接口、命令行脚本实现对设备的配置与策略下发。

4.5 绿色节能

网络机房的整体能耗应遵循GB 50189和GB/T 2589的相关规定。采用低能耗的绿色网络设备。

4.6 安全可靠

公证数据中心安全防护等级应按照GB/T 22239-2008中第三级要求进行规划和建设。

5 总体架构及要求

5.1 总体架构

公证数据中心总体架构如图1所示：

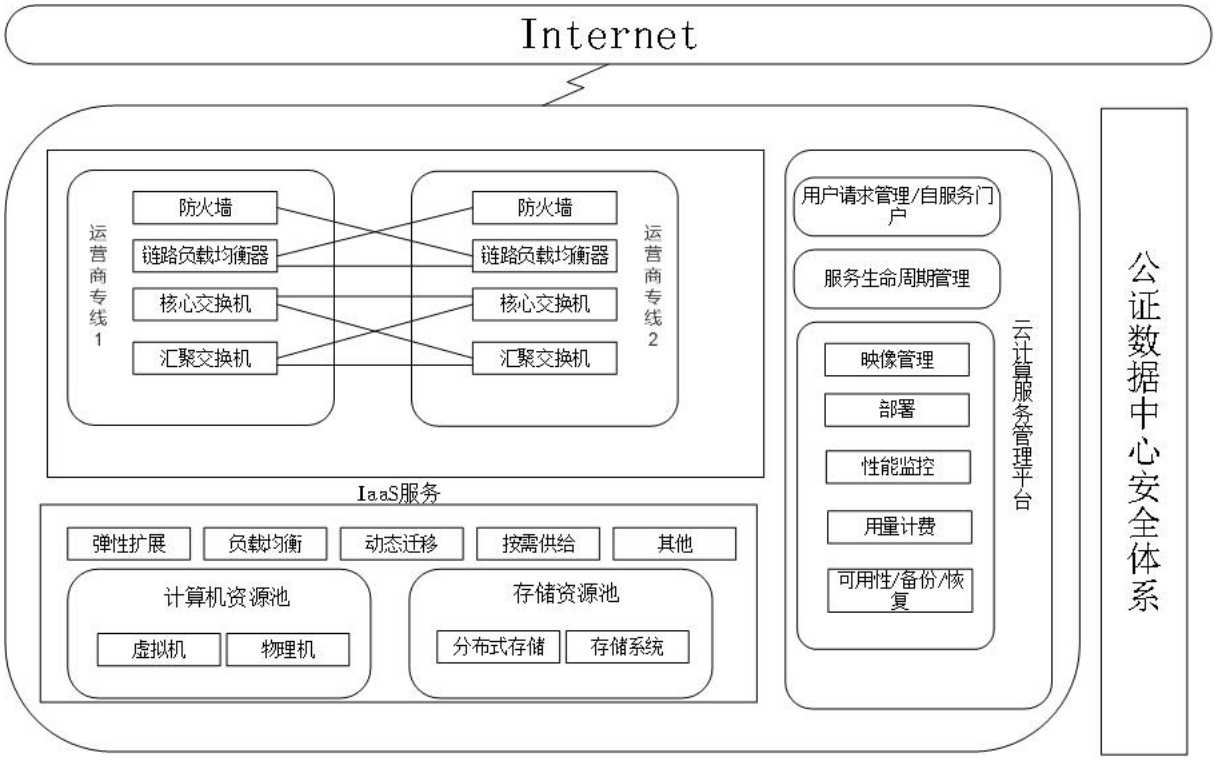

图1 公证数据中心总体架构

公证数据中心总体架构主要包括：资源池、云计算服务管理平台和公证数据中心安全体系。其中：

a) 资源池又包括：计算机资源池、存储资源池和网络资源池；
b) 云计算服务管理平台对资源池和应用进行管理调度及告警监控；
c) 公证数据中心安全体系保障公证数据中心的安全可靠运行。

5.2 计算机资源池设计要求

5.2.1 计算机资源池架构

计算机资源池的架构应由机架式服务器、刀片服务器构成，条件具备宜增加区块链资源，其中：

a) 刀片服务器应通过服务器虚拟化部署一般业务系统和web应用系统；
b) 机架式服务器应用于部署管理平台和高负载数据库服务器等；
c) 区块链资源用于部署区块链技术，应实现对数据的加密计算。

5.2.2 配置与选型

计算机资源池的配置与选型要求如下：

a) 根据实际业务发展情况应按需扩容、滚动建设；
b) 一台物理服务器应可虚拟多台虚拟机，应根据应用服务所需资源而定；
c) 刀片服务器虚拟化后的虚拟机可部署一般应用服务器，高性能服务器虚拟化后的虚拟机可部署重载数据库服务器；
d) 每台物理服务器要求配置应不少于 3 个千兆以太网电口，分别用于虚拟化平台管理口、应用系统对外提供服务、连接 NAS（网络附属存储）存储设备；
e) 如需连接 SAN 存储设备还应部署 HBA（主机总线适配器）卡和光纤交换机。

5.2.3 服务器选型

服务器选型要求如下：

a) 标准机架式服务器可选择典型的是 2U 或 4U 的型号，包含 2 到 4 个 CPU 插座，2 到 8 个 PCI—E 或 PCI—X 插槽，4 到 6 个硬盘托架；
b) 刀片式服务器应考虑刀片式架构中的每个刀片所包含 CPU 数及最大内存。应考虑对于每个宿主机服务器用于支持一定数量的客户机所需的网络和存储 I/O，保证刀片上运行的每个宿主机服务器和刀片底盘自身能够提供支持。

5.3 存储资源池设计要求

5.3.1 存储资源池配置应采用存储虚拟化技术，搭建支撑云计算中心高效运行的存储保障环境。

5.3.2 存储虚拟化环境应不少于 2 组存储虚拟化硬件设备，每组配置 2 个以上控制器，72G 以上高速缓存，并提供相应的存储资源虚拟化管理软件。

5.3.3 高速 SAN 存储网应不少于 2 台高速 SAN 光纤交换机。

5.4 网络资源池设计要求

5.4.1 物理拓扑

网络资源池组网物理拓扑图如图2所示。

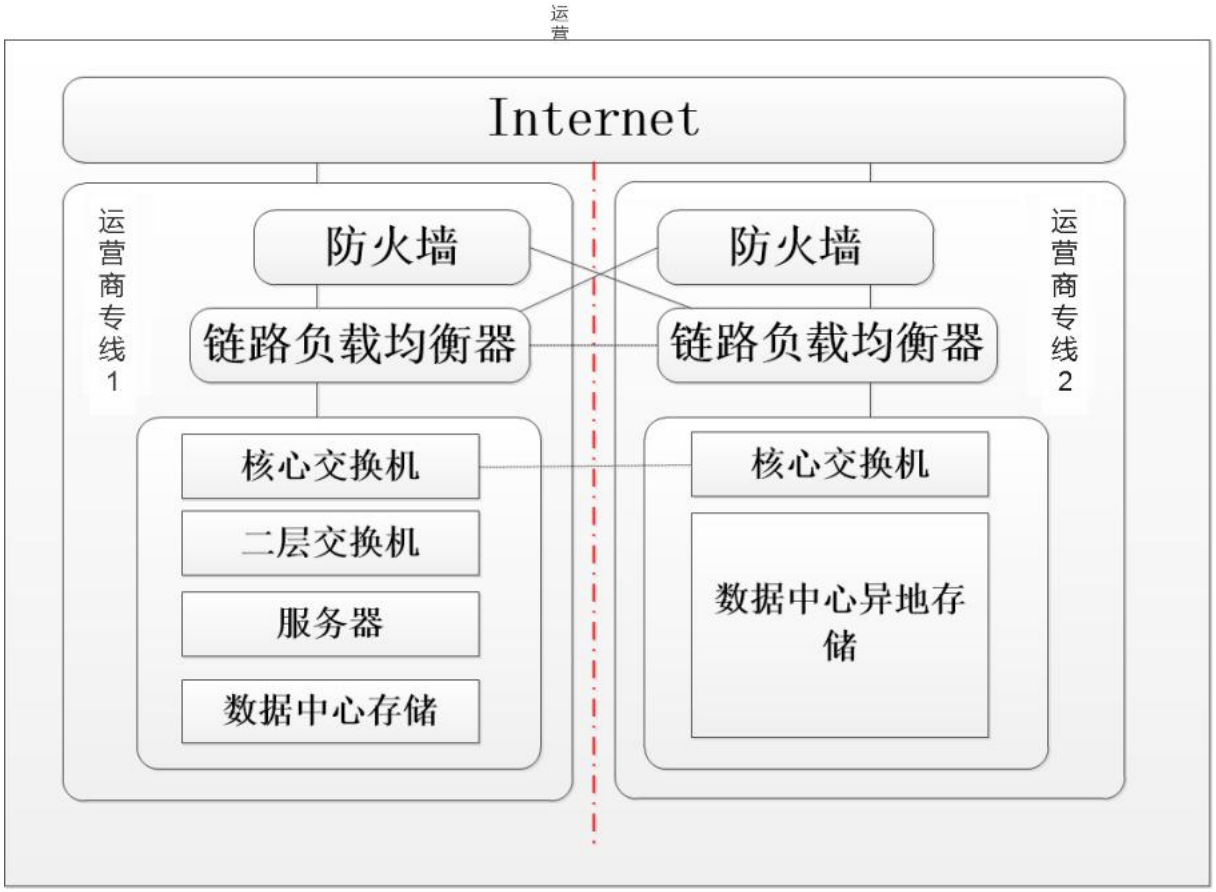

图 2　网络资源池组网物理拓扑图

5.4.2　设计结构

网络资源池设计结构要求如下：

a)　应满足双网双平面结构，网络接口、网络链路以及关键网络设备均配置冗余部件；
b)　网络接口上每台物理服务器至少配置 2 张网卡，分别用于业务服务、虚拟化平台宿主机管理、IP 存储系统互联；
c)　业务服务网络根据业务属性不同，通过 VPN 划分为公用网络区、互联网接入区、专用网络区；
d)　虚拟化计算资源可在不同的网络区域中自由迁移。

5.4.3　结构安全

网络资源池结构安全要求如下：

a)　应设置防火墙、隔离网闸、运维审计、数据库审计系统等安全设备；
b)　防火墙应用于实现同一网络区域中不同业务系统的之间的安全隔离；
c)　隔离网闸应用于在 VPN 隔离的不同网络区域之间进行安全数据交换，同时用于电子公证之间的数据安全交换。

5.4.4　存储安全

网络资源池存储安全要求如下：

a) 宜采用区块链资源实现区块链计算资源部署，该区块链资源接入在核心交换机设备上，与其他服务器资源形成局域网；
b) 应在高性能服务器部署软件区块链技术解决方案。

5.4.5 网络虚拟化

网络虚拟化要求如下：

a) 应在云计算平台的汇聚层部署汇聚交换机、防火墙、IPS、负载均衡器等设备，实现网络服务虚拟化；
b) 虚拟化技术模拟汇聚层交换机，每个模拟出的交换机应拥有它自身的软件进程、专用硬件资源（接口）和独立的管理环境，不同物理端口分配给不同的虚拟交换机，且虚拟交换机之间不应共享端口；
c) 采用网络虚拟化技术，对不同设备进行虚拟化分区，应包括安全审计虚拟化、负载均衡虚拟化、IPS/IDS 虚拟化、防火墙虚拟化四个方面。

5.4.6 IP 地址及 DNS

IP地址及DNS要求如下：

a) IP 地址规划应遵循国信办和国家外网工程办有关规定和指导意见；
b) 公证数据中心的网络带宽应不低于 100MB。

5.5 云计算服务管理平台要求

云计算服务管理平台应包括以下内容：

a) IT 基础架构中的物理资源和虚拟资源的管理；
b) 宿主机的管理接口（统一设置宿主机上某一个单独物理网卡用于云计算管理平台对虚拟机的管理通讯）应进行统一 VLAN 规划，实现不同分区的虚拟机在同一个资源组中迁移，实现云计算平台对 3 个区的统一管理。

5.6 公证数据中心安全系统要求

5.6.1 概述

公证数据中心安全系统要求包括IaaS、PaaS、SaaS、云安全服务、安全防护等级五个内容，具体要求见5.6.2、5.6.3、5.6.4、5.6.5和5.6.6。

5.6.2 IaaS 要求

IaaS 要求如下：

a) 机房、电源、监控等场地设施和周围环境及消防安全，应严格按照国家相关标准，并满足 24 小时不间断运行的要求进行设计建设。其具体安全措施应遵循 GB/T 9361 和 GB/T 2887 的相关规定；
b) 通信线路应采用铺设或租用专线方式建设；
c) 通信线路应远离强电磁场辐射源，埋于地下或采用金属套管；
d) 通信线路应定期测试信号强度，确定是否有非法装置接入线路,在线路附近有新的网络架设、电磁企业开工时，可请专业机构负责检测；
e) 通信线路应定期检查接线盒及其他易被人接近的线路部位，防止非法干扰；
f) 骨干线路应在骨干线路或重要的节点设置冗余线路和环形路由；

g) 骨干线路应设置冗余电源配置；
h) 骨干线路应在重要部门重要业务系统所属的相关线路设置冗余或环形路由；
i) 主机安全应采取的措施和技术手段包括身份认证、主机安全审计、主机入侵防御、主机防病毒系统；
j) 网络安全应采取的安全措施和技术包括防火墙、IPS、网络安全审计系统、防病毒、防病毒网关、强身份认证；
k) 在互联网环境下应将 SAN 存储分隔为两个数据区，分别作为中心应用数据区和社会公众数据区，进行存储区域划分实现数据隔离。

5.6.3 PaaS 要求

PaaS要求如下：
a) 公证数据中心应配备运维安全审计系统，通过防火墙、IPS、漏洞管理、网页防篡改等安全技术手段保障由外部发起的攻击，实现对应用运行安全的全方位防护；
b) 应安装 PKI（公钥基础设施）应用服务器，结合 CA（认证机构）中心，实现对接口的强用户认证，接口数据加解密和有效接口的访问控制。

5.6.4 SaaS 要求

SaaS要求如下：
a) 应保障应用安全，对应用程序或工具在使用过程中可能出现计算、传输数据的泄露和失窃，通过其他安全工具或策略来消除隐患；
b) 应保障数据安全，经过网络传输和交换的数据不应发生增加、修改、丢失和泄露等；
c) 应通过加密和密钥管理，保障安全；
d) 应建立身份识别和访问管理，确保用户身份及其所归属的某项定义组来限制用户对某些信息项的访问；
e) 应建立安全事件管理，对发生的安全事件进行分析，提高安全保障；
f) 应保障业务连续性。

5.6.5 云安全服务要求

云安全服务要求如下：
a) 云平台应进行上线检测、监控服务以及 2 个月一次的远程巡检和现场巡检服务；
b) 应定期远程巡检、定期现场巡检；
c) 应有远程安全值守服务；
d) 应有安全加固服务。

5.6.6 安全防护等级要求

安全防护等级应遵循GB/T 22239-2008中第三级要求进行规划和建设。

6 机房建设要求

6.1 基本要求

公证数据中心机房建设基本要求如下：
a) 应按照数据中心机房 B 级以上标准进行建设；

b) 应配置网络 KVM，实现“无人机房”；
c) 网关和集成服务器应在专门的网管控制中进行设备管理、软件调试工作，人机分离，应提供统一、集中的访问权限管理，管理员按照用户权限分配专门的账号给网管人员和集成服务商技术人员。

6.2 布线系统

布线系统要求如下：
a) 机房内通信电缆及电力电缆应在走线架上布放，布线距离应尽量短而整齐；
b) 通信电缆与电力电缆应分别按不同路由敷设，如相互间距离较近，则应保持不低于 100mm；
c) 应预留 1 个机架作为配线架专用机架，每个设备机架配置一套不少于 24 口配线架。

6.3 机房系统

6.3.1 机房环境

机房环境要求如下：
a) 应遵循 GB 50174 与 GB 50462 相关要求；
b) 所有设备应放在计算机房环境里，室内清洁无尘；
c) 温度应介于（15～30）℃，每小时变化<10℃；
d) 湿度应介于（40～70）%，不结露、霜；
e) 机房荷载要求：主机房楼面等效均布活荷载标准值应为 6kN/㎡；控制室楼面等效均布活荷载标准值应为 4.5 kN/㎡；
f) 机房照明方式应采用一般照明，水平面（距地 0.8m）照度应为（200～450）LX，直立面（距地 1.4m）照度应为（30～50）LX；
g) 现有机房地板应具有足够的强度，应是难燃材料或非燃材料，同时耐油、耐腐蚀、柔光、不起尘；新建机房不应采用活动地板；
h) 建筑物的接地应采用联合接地系统，接地电阻值应小于 1Ω。

6.3.2 消防安全

消防安全要求如下：
a) 机房的电源线与信号线的孔洞、管道应分开设置，机房内的走线除设备的特殊要求外，一律应采用不封闭走线架；交流线应采用绝燃材料加护套，并用金属套管；
b) 机房建筑材料应采用非易燃或阻燃材料；
c) 主机房应同时设计安装消防报警系统；
d) 施工中应把电力线与信号线分架分孔洞敷设。确实需同槽同孔敷设或交叉的，应采取可靠的隔离措施；
e) 机房设备的排水管不应与电源线同槽敷设或交叉穿越。确实需同槽或交叉的，应采取可靠的防渗漏防潮措施；
f) 机房空调隔热层应采用不燃或阻燃材料；
g) 施工完毕应将竖井和孔洞用不燃或阻燃材料封堵。

6.3.3 设备供电

设备供电要求如下：

a) 遵循 GB 50174 与 GB 50462 相关要求；

b) 交流：电压应是 220V 单相，变化小于±15%；
c) 频率：50Hz 变化应小于±5%；
d) 电源波形：正弦波畸变应不大于±3%；
e) 直流：电压应是 48V±15%；
f) 交流电力系统应配有交流调整装置或不间断的电源来滤除脉冲干扰；
g) 供电应尽可能地应用两路市电和油机系统，平时市电输入经转换开关任一路供电；当两路均断时，由油机供电。

6.3.4 环境保护与设备节能

环境保护与设备节能要求如下：

a) 应遵循 GB 50189、GB/T 2589 的相关要求；
b) 公证数据中心对周围环境应无电磁辐射、无粉尘、无噪声、无污染物产生。

6.4 UPS 配置要求

UPS应遵循GB 51194的相关要求进行设计配置。

7 运行维护与安全管理

7.1 总体安全方针与安全策略

总体安全方针与安全策略应具备以下特性：

a) 安全策略紧紧围绕行业的发展战略，符合实际的信息安全需求，保障与促进信息化建设的顺利进行，避免过于理想化或不可操作性；
b) 明确阐述所有信息化建设项目在规划设计、开发建设、运行维护等各阶段应遵循的总体原则和要求；
c) 安全策略应经过安全决策机构批准，具备指导和规范信息安全工作的效力；
d) 安全策略中应规定其自身的时效性，当信息系统运行环境发生重大变化时，及时对总体安全策略进行必要的调整，并将调整后的策略提交安全决策机构批准。

7.2 安全管理机构

安全管理机构应包括以下内容：

a) 根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；
b) 设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；
c) 成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；
d) 制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求；
e) 建立授权与审批制度；
f) 建立内外部沟通合作渠道；
g) 定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

7.3 人员安全管理

人员安全管理应包括以下内容：

a) 主要内容：人员录用、离岗、考核、教育培训等；
b) 关键岗位要求：应对关键岗位人员进行的以安全为核心的管理，包括对关键岗位的人员采取在录用或上岗前进行安全审查和技能考核，与关键岗位人员签署保密协议，对离岗人员撤销系统账户和相关权限等措施；
c) 安全培训：应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。培训的内容包括单位的信息安全方针、信息安全方面的基础知识、安全技术、安全标准、岗位操作规程、最新的工作流程、相关的安全责任要求、法律责任和惩戒措施等；
d) 具体应遵循 GB/T 22239-2008 与 GB/T 20269 的相关要求。

7.4 系统建设管理

应遵循GB/T 22239-2008的相关要求。

7.5 系统运维管理

7.5.1 系统运维管理的内容

系统运维管理包括环境和资产安全管理、设备和介质安全管理、日常运行维护、集中安全管理、事件处置与应急响应、灾难备份、安全监测和其他要求在内的八项内容。具体要求见7.5.2、7.5.3、7.5.4、7.5.5、7.5.6、7.5.7、7.5.8。

7.5.2 环境和资产安全管理要求

环境和资产安全管理要求如下：

a) 环境安全管理：包括计算机、网络机房环境以及设置有网络终端的办公环境，应明确环境安全管理的责任部门或责任人，加强对人员出入的控制，对有关物理访问、物品进出和环境安全等做出规定。对重要区域设置门禁控制手段或使用视频监控等措施；
b) 资产安全管理：包括介质、设备、设施、数据、软件、文档等，应从安全和信息系统角度对资产进行管理，将资产作为信息系统的组成部分，按其在信息系统中的作用进行管理。应明确资产安全管理的责任部门或责任人，对资产进行分类、标识，编制与信息系统相关的软件资产、硬件资产等资产清单；
c) 具体应遵循 GB/T 22239-2008 和 GB/T 20269 的相关要求。

7.5.3 设备和介质安全管理要求

设备和介质安全管理要求如下：

a) 应明确配套设施、软硬件设备管理、维护的责任部门或责任人，对信息系统的各种软硬件设备采购、发放、领用、维护和维修等过程进行控制，对介质的存放、使用、维护和销毁等方面做出规定，加强对涉外维修、敏感数据销毁等过程的监督控制；
b) 具体应遵循 GB/T 22239-2008 中系统运维管理，同时可参照 GB/T 20269 等。

7.5.4 日常运行维护要求

日常运行维护要求如下：

a) 应明确系统日常运行维护的责任部门或责任人，对运行管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理；
b) 应制订设备操作管理、业务应用操作管理、变更控制和重用管理、信息交换管理相应的管理制度；

c) 制定与信息系统安全管理相配套的规范和操作规程并落实执行；
d) 正确实施为信息系统可靠运行而采取的各种检测、监控、审计、分析、备份及容错等方法和措施，对运行安全进行监督检查；
e) 具体应遵循 GB/T 22239-2008 和 GB/T 20269 的相关要求。

7.5.5 集中安全管理要求

集中安全管理要求如下：

a) 信息系统应按照统一的安全策略、安全管理要求，统一管理信息系统的安全运行，进行安全机制的配置与管理，对设备安全配置、恶意代码、补丁升级、安全审计等进行管理，对与安全有关的信息进行汇集与分析，对安全机制进行集中管理；
b) 具体应遵循 GB/T 22239-2008 中系统运维管理部分，同时可参照 GB/T 25070 和 GB/T 20269 的相关要求。

7.5.6 事件处置与应急响应要求

事件处置与应急响应要求如下：

a) 应按照国家有关标准规定，确定信息安全事件的等级；
b) 应结合信息系统安全保护等级，制定信息安全事件分级应急处置预案，明确应急处置策略，落实应急指挥部门、执行部门和技术支撑部门的工作，建立应急协调机制；
c) 应落实安全事件报告制度，信息系统发生较大、重大、特别重大安全事件时，运营使用单位按照相应预案开展应急处置，并及时向受理备案的公安机关报告；
d) 应组织应急技术支撑力量和专家队伍，按照应急预案定期组织开展应急演练；
e) 具体应遵循 GB/T 22239-2008 的相关要求。

7.5.7 灾难备份要求

灾难备份要求如下：

a) 应对信息系统采取灾难备份措施，防止重大事故、事件发生。识别需要定期备份的重要业务信息、系统数据及软件系统等，制定数据的备份策略和恢复策略，建立备份与恢复管理相关的安全管理制度；
b) 具体应遵循 GB/T 22239-2008 的相关要求，同时可参考 GB/T 20988 的相关要求。

7.5.8 安全监测要求

安全监测要求如下：

a) 应开展信息系统实时安全监测，对物理环境、通信线路、主机、网络设备、用户行为和业务应用等的监测和报警，及时发现设备故障、病毒入侵、黑客攻击、误用和误操作等安全事件，及时对安全事件进行响应与处置；
b) 具体应遵循 GB/T 22239-2008 的相关要求。

7.5.9 其他要求

其他要求如下：

a) 应对系统运行维护过程中的其它活动，如系统变更、密码使用等进行控制和管理；
b) 应按国家密码管理部门的规定，对信息系统中密码算法和密钥的使用进行分级管理。

7.6 安全管理制度

安全管理制度要求如下：

a) 应遵循 GB/T 22239-2008 的相关要求，同时可参照 GB/T 20269 的相关要求；

b) 应制定安全检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善；

c) 应定期对信息系统安全状况进行自查。经自查，信息系统安全状况未达到安全保护等级要求的，应进一步开展整改。