# 《政务云数据中心安全运维技术规范》
# （征求意见稿）
# 编制说明

## 一、工作简况

（一）任务来源

本文件由天翼云科技有限公司和北京交通大学联合提出，经中国技术市场协会批准，正式列入2024年团体标准制修订计划，标准名称为《政务云数据中心安全运维技术规范》。

（二）项目背景

随着数字政府建设的深入推进，政务云数据中心已成为支撑国家治理体系和治理能力现代化的核心基础设施。然而，云计算环境下面临的网络安全威胁日益复杂，传统运维模式难以应对新型攻击手段和严格的合规要求。当前政务云数据中心存在以下挑战：

1. **资产暴露面扩大**：互联网化部署导致资产数量激增，未知资产和脆弱性管理难度加大；
2. **防御体系分散**：安全设备策略缺乏联动，数据全生命周期防护存在盲区；
3. **应急能力不足**：威胁监测实时性不足，故障切换与容灾恢复机制尚未标准化；
4. **合规压力升级**：需满足《GB/T 20984》《GB/T 20986-2023》等国家标准对资产分级、事件响应的强制要求。

为此，亟需建立一套覆盖"识别-防御-监测-响应"全链条的政务云数据中心安全运维技术体系，以系统性方法应对安全风险，保障政务业务连续性和数据主权安全。

（三）目的意义

本标准的制定旨在实现以下目标：

**1.规范安全运维全流程**

精准资产管理：通过资产台账动态更新、关联图谱绘制和暴露面收敛，夯实安全防护基础；

纵深防御构建：统一安全设备运维标准，强化网络/系统/数据层加固措施，形成多层级防护屏障；

智能监测预警：依托流量分析与异常行为检测技术，实现威胁实时感知和风险趋势预判。

**2.提升业务连续性保障能力**

（1)容灾体系完善：通过同城多活、异地灾备等架构设计和年度故障演练，确保RTO/RPO达标；

(2)应急响应提速：明确事件处置流程（准备→诊断→根除→恢复），配套溯源取证机制，缩短MTTR（平均修复时间）。

**3.驱动运维模式智能化转型**

(1)技术工具融合：推动安全产品、AI分析平台与运维流程深度集成，实现风险处置自动化；

(2)数据价值释放：基于安全日志、设备告警等多源数据分析，支撑主动防御决策。

本标准实施后，将有效提升政务云数据中心的风险抵御能力，为数字政府建设提供符合等保2.0/关基保护条例要求的安全底座，助力国家网络安全战略落地。

（四）起草单位及起草人名单

本文件起草单位：XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX。

本文件主要起草人：XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX。

（五）主要起草过程

1.文本调研

于2025年1月启动了文本的调研工作，并与2025年10月完成了相关资料的收集和分析工作。

2.标准立项

翼云科技有限公司向中国技术市场协会标准化委员会提出申请，于2024年9月获得中国技术市场协会标准化工作委员会批准立项。

3.组建标准起草工作组

2025年1月7日，召开项目启动会。

2025年1月7日，成立了翼云科技有限公司、北京交通大学等组成的标准起草工作组，并讨论标准调研工作事项。

4.形成标准草案

2025年1月8日，起草组对资料收集情况进行汇报，并对进行了线上讨论。

2025年2月25日，开展组内讨论，确定了标准框架和主要内容。

2025年4月10日，对翼云科技有限公司起草的标准初稿进行讨论，并提出修改意见。

2025年6月17日，起草组根据修改意见进行修改，形成标准草案。

5.形成征求意见稿

2025年9月15日，对标准草案进行讨论，起草组对草案内容进行了修改，形成标准征求意见稿。

## 二、确定标准主要内容的论据

（一）编制原则

1）合规性原则

论据支撑：

全文引用GB/T 20984（风险评估）、GB/T 20986（事件分

级）等 12 项国家标准，确保与《网络安全法》《数据安全法》形成技术衔接。

继承 YD/T 4570-2023《政务云安全能力要求》对租户隔离、安全资源池的强制性条款。

2）全生命周期覆盖

论据支撑：

参照 GB/T 36626-2018《信息系统安全运维管理指南》，建立"预防-监控-处置-改进"闭环机制。

涵盖物理设施（GB/T 34982）、虚拟化平台、业务应用三层防护体系。

（二）标准主要内容及适用范围

1）核心内容框架

| 模块 | 技术要点 | 引用依据 |
| --- | --- | --- |
| 资产安全管理 | 动态资产台账、CMDB 基线管理、暴露面收敛策略 | GB/T 25069 术语体系 |
| 安全防护体系 | 东西向流量微隔离、数据加密（国密 SM4）、WAF 策略联动 | YD/T 4570 第 6 章 |
| 监测预警机制 | 全流量威胁分析、异常行为 AI 建模、风险态势可视化 | GB/T 20984 风险评估模型 |
| 应急响应流程 | 事件分类（7 大类）、处置 SOP（含取证溯源）、灾备切换演练 | GB/T 20986 事件分级标准 |

2）适用范围

适用对象：各级政务云服务商、政府部门自建数据中心。

约束边界：不适用于涉密信息系统（需遵循分级保护标准）。

（三）确定标准主要内容的论据

1. 问题导向论据

- 现实痛点：据国家信息安全漏洞库（CNNVD）统计，2023年政务云相关漏洞同比增长47%，其中配置错误类占63%
- 标准对策：增设"安全配置基线"章节，明确200+项加固条目（如禁用TLS 1.0、强制双因素认证）。

2. 最佳实践论据

- 案例借鉴：广州某组委会灾备项目，通过800+TB数据实时备份，保证数据持续可用；通过系统日志实时分析，发现潜在风险；通过设定容灾架构，指定应急相应和处理方案。
- 技术移植：引入金融行业已验证的"零信任访问控制"模型，适配政务云跨部门协作场景。

3. 法规符合性论据

- 等保2.0衔接：第三级系统要求映射表，满足通用要求+云计算扩展要求。
- 关基保护：针对核心系统、重点数据等关键业务，增加冗余度指标（RTO<15分钟，RPO=0）。

4. 技术演进论据

- AI赋能：基于大模型的日志分析算法，实现未知威胁检出率＞85%（对比传统规则引擎提升40%）。
- 云原生适配：容器运行时保护、Service Mesh安全审计等新技术要求。

**三、主要试验[或验证]情况分析、技术经济论证、预期经济效果**

1、某卫星通信案例

1）业务连续性保障

要求核心关键业务可以持续提供服务，严格执行“1-5-10”的标准要求，即：“问题 1 分钟发现- 5 分钟定位 - 10 分钟恢复”。要求 RTO 不超过 10 分钟，RPO≈0，以确保在紧急情况下能够迅速恢复业务。

2）数据安全与备份

为保障数据安全与业务连续性，需实施全生命周期防护：传输环节采用 SSL/TLS 加密，存储环节使用 AES 加密与权限管控并定期校验完整性。备份策略构建实时、增量及全量多层次机制，其他数据依重要性分级处理。容灾中心内实行多副本存储，并规划“两地三中心”异地冗余架构，防范区域性灾难导致数据丢失，全面提升可靠性与恢复能力。

3）系统高可用性

采用模块化基础架构支持资源横向扩展，灵活应对业务增长。应用层实施集群部署与负载均衡，结合自动重试和故障转移确保高可用；基础设施层配置冗余设备及热插拔技术提升容错能力。同时，建立实时监控体系，持续追踪 CPU、内存、网络等指标，及时预警潜在故障，保障系统稳定运行，避免业务中断。

4）应急响应与演练

制定全面云容灾应急预案，覆盖自然灾害、人为故障及网络攻击等场景，定期更新优化。每季度至少开展一次容灾演练（含切换、数据恢复及流程测试），检验系统有效性并提升团队熟练度。

2、案例实现

用户需按两地三中心架构部署核心业务系统，通过业务架构改造、故障演练及容灾切换机制保障高可用性与灾备能力。业务架构改造实施无状态化重构，消除单点依赖，实现快速故障迁移；构建同城双活中心（负载均衡动态分配流量，互为实时热备）

和异地灾备中心（定时备份与异步复制，应对同城全故障接管）。故障演练机制定期模拟网络中断、数据库故障等场景，结合脚本任务、人工干预与系统工具编排复杂测试，验证应急预案有效性并优化风险点。容灾切换流程支持智能自动/手动触发（基于监控阈值），通过预编排模板实现跨中心流量快速切换；灵活编排自定义步骤，融合脚本自动化、人工审批及系统校验任务，确保操作精准高效。全面提升系统故障恢复速度与业务连续性，满足高可用性要求。

**四、采用国际标准和国外先进标准的程度**

本文件为首次自主制定，本文件不涉及国际国外标准的采标情况。

**五、重大分歧意见处理经过及依据**

本文件在制定过程中未出现重大分歧意见。

**六、与现行相关法律、法规及相关标准的协调性**

参考了 GB/T 20984—2022 、GB/T 20986—2023、GB/T 25069—2022 等国家标准相关内容要求。《政务云数据中心安全运维技术要求》在内容上与《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《密码法》等现行法律、法规高度协调，同时与《GB/T 20984-2022》《GB/T 20986-2023》《GB/T 36626-2018》《YD/T 4570-2023》等标准的技术要求一致。标准不仅满足了国家对政务云数据中心安全运维的基本要求，还通过引用和整合多个相关法规和标准，构建了完整的安全运维体系，确保其在实际应用中的合规性和可操作性。

因此，该标准在内容上完全符合现行法律、法规及标准的要求，具有良好的协调性和适用性。

**七、知识产权情况说明**

无。

## 八、其他应予说明的事项

无。

《政务云数据中心安全运维技术规范》

团体标准起草组

2025 年 9 月 9 日