|  |  |
| --- | --- |
| ICS | 35.240.01 |
| CCS | L67 |

|  |
| --- |
| 3207 |

连云港市地方标准

DB3207/T XXXX—2025

政务云平台运行维护管理规范

Management Specification of Government Cloud Platform Operation and Maintenance

XXXX-XX-XX发布

XXXX-XX-XX实施

连云港市市场监督管理局  发布

目次

[前言 II](#_Toc190161978)

[1 范围 1](#_Toc190161979)

[2 规范性引用文件 1](#_Toc190161980)

[3 术语和定义 1](#_Toc190161981)

[4 基本要求 2](#_Toc190161982)

[5 运维制度 2](#_Toc190161983)

[6 运维服务 3](#_Toc190161984)

[7 应急保障 5](#_Toc190161985)

[8 评价与改进 5](#_Toc190161986)

1. 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。

本文件由连云港市数据局提出并组织实施与监督。

本文件由连云港市社会管理和公共服务标准化技术委员会归口。

本文件起草单位：连云港市数据局、中共连云港市委网络安全和信息化委员会办公室、连云港市大数据管理中心、连云港市标准化研究中心、中国电信股份有限公司连云港分公司、连云港市人力资源和社会保障局、中国联合网络通信有限公司连云港市分公司、江苏省连云港中等专业学校、连云港市连云区经济责任审计中心。

本文件主要起草人：徐毅、胡杰、徐周、李伟、董亮、陈群、王海港、朱伟、朱华华、张睿、李大柱、王建、徐茹、朱卫敏、季波、李敏、孙益龙、戴仁杰。

政务云平台运行维护管理规范

* 1. 范围

本文件规定了政务云平台运维制度、运维服务、应急保障等要求。

本文件适用于政务云平台运行维护管理。

* 1. 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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求

GB/T 28827.3 信息技术服务 运行维护 第3部分：应急响应规范

GB/T 28827.4 信息技术服务 运行维护 第4部分：数据中心服务要求

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 34077.3 基于云计算的电子政务公共平台管理规范 第3部分：运行保障管理

GB/T 37736 信息技术 云计算 云资源监控通用要求

* 1. 术语和定义

下列术语和定义适用于本文件。

政务云 government cloud

用于承载各级政务部门开展公共服务、社会管理的业务信息系统和数据，并满足跨部门业务协同、数据共享与交换等的需要，提供IaaS、PaaS和SaaS服务的政务云计算服务。

政务云用户 government cloud users

使用政务云计算基础设施开展电子政务业务和处理、存储数据的组织（或机构），主要指使用政务云的各级政务部门及相关事业单位，包括单位内部业务使用人员及负责云资源分配和管理的人员。

政务云指挥调度部门 government cloud command and dispatch department

政务云的指挥调度单位，负责政务云平台的规划、应用、监督、管理及对云服务方的考核，下达政务云指挥调度指令，审核政务云用户使用需求，受理政务云平台建设方案备案，审核政务云服务费用。

政务云运营维护部门 government cloud operation and maintenance department

为各级政务部门提供计算、存储、网络及安全等各类云计算基础设施资源、相关软件和服务的云服务方。负责执行云服务方业务运营和相关管理工作，运营、维护、管理云计算的计算基础设施及软件，通过服务方式将云计算的资源交付给政务云用户。

云管理平台 cloud management platform

为整个云计算基础设施提供资源管理和服务管理，能够对存储/计算/网络/系统等基础设施资源（IaaS）、应用/开发/数据平台（PaaS）和软件架构整合服务（SaaS）进行管理。一般情况下，由云计算基础设施服务方提供，也可由第三方提供云管理平台。

割接与升级 cutover and upgrade

对政务云资源池进行的调整网络结构、物理设备扩容、虚拟系统扩容、物理设备搬迁、软件升级等工作。

* 1. 基本要求
     1. 机构

政务云平台运维机构应当在数据主管部门授权下，设立专门的指挥调度部门和运营维护部门，明确职责分工，建立协同工作机制，准备充足的运维服务资源，配备专业的运维服务人员并提供 7×24h响应服务，确保运维工作高效开展。

* + 1. 人员

政务云运维人员应具备质量管理体系、信息安全、信息技术服务、和人员证书等相关资质和技能，定期参加培训，熟悉政务云平台的技术架构和运维流程，提供可靠的运维技术支持。

* + 1. 设施设备

政务云平台应配备必要的硬件设施和软件工具，包括监控系统、备份设备、安全防护设备等，确保运维工作的顺利开展。

* + 1. 制度

政务云平台应建立完善的运维管理制度，包括但不限于人员管理、流程权限、绩效考核等，确保运维工作规范化、标准化。

* 1. 运维制度
     1. 指挥调度

政务云维护工作遵循在数据主管部门领导下“统一高效、集约运营、紧急优先、安全优先”的原则，下级应服从上级、局部须服从全局。

政务云运营维护部门应依据政务云指挥调度部门的相关规定或下达的指示开展运维管理工作，并在规定的时限内完成相关工作。

紧急情况下，政务云指挥调度部门可采用口头或电话方式下达指令，政务云运营维护部门应记录时间、地点、内容、授权人、受理人等内容，事后应补办文字手续，并进行存档备案。

所有业务的开放、关闭和撤销，以及所有政务云的调度、调整，应以政务云指挥调度部门的调度工单为准，严禁在未授权情况下修改政务云配置数据、调度电路或开放业务。

政务云运营维护部门可在所辖维护范围内进行紧急调度，确保政务云的应急和畅通能力。

政务云运营维护部门应按要求记录政务云调整、电路调度和业务开放等指令执行情况，以实现政务云调度的闭环管理。

* + 1. 驻场人员管理

政务云运营维护部门应建立运维团队管理制度，明确岗位职责，制定日常维护、备份恢复、安全防范等工作规程，通过实时监控、定期巡检、日志分析、系统优化等措施，确保系统稳定运行。

政务云运营维护部门应签订保密协议、重要岗位保密承诺书以及离岗离职人员安全保密承诺书，并实施相应的权限回收和审计措施。

政务云运营维护部门应严格控制对政务云资源的访问权限，并采取必要的安全措施，确保数据安全。未经授权的人员不得访问政务云资源，必要时应经过审批和监控。

* + 1. 流程权限

政务云运营维护部门应制定详细的操作规范和流程，包括系统升级、故障排查、数据备份等关键操作。

政务云运营维护部门应建立权限管理制度，通过分级授权、最小权限原则、定期审查等方式，严格管控对政务云资源的访问权限，并采取身份认证、访问控制等安全措施，确保数据安全。

* + 1. 绩效考核

政务云运营维护部门应建立绩效考核指标体系，通过定期评估、数据分析等方式，对约定的服务指标完成情况、用户满意度、维护服务完成度及质量、维护服务效率、维护对象故障率及故障处理时间等进行量化考核。

政务云运营维护部门应建立运行维护报告制度，通过周报、月报等形式，定期上报政务云运行维护工作情况，对政务云运行情况、事件、变更、资源使用、安全管理等进行系统分析，并提出改进建议。

政务云运营维护部门每季度开展服务质量评估，根据评估结果分析问题原因，持续改进运行维护服务。

* 1. 运维服务
     1. 运行监控

政务云运营维护部门应按照GB/T 28827.4和GB/T 37736的规定，使用监测系统等工具，结合现场人工巡检，对政务云机房资源、云资源池硬件、网络、云平台、虚拟化资源、相关软件系统等进行实时监测、记录、分析和告警，具体要求如下:

a） 实时监控政务云平台与设备的告警；

b） 实时监控政务云平台用户数量变化情况；

c） 实时监控政务云平台的业务流量流向；

d） 实时监控政务云平台与网管、台账等运营支撑系统之间接口状态；

e） 实时监控政务云平台网络出口流量情况；

f） 实时监控政务云平台质量关键指标数据；

g） 监控政务云基础设施资源量使用情况及预警；

h） 机房动力、环境及安防等配套设施监控系统的关键指标等。

* + 1. 维护作业

政务云运营维护部门应按照GB/T 28827.1和GB/T 28827.4的规定组织维护作业，具体要求如下：

a） 实施维护作业时，应优先考虑远程操作和自动化技术，以减少现场作业和人工操作，政务云运营维护部门应持续优化网管平台及其他辅助支撑手段，提高维护作业的执行效率和自动效率；

b） 维护作业计划分为天、周、月、季度、半年以及年度等执行周期；

c） 日常现场巡检每天至少安排两次，巡检期间，应对资源池设备运行的机房环境、配套基础设施进行细致全面监视和检查。

* + 1. 割接升级

割接升级应符合GB/T 31168的相关规定。具体要求如下：

a）政务云运营维护部门基于业务需求发起割接升级申请，同时组织制定割接升级方案并与工程部门、设备厂商及其他相关部门和人员共同制定实施计划；

b）割接升级实施前须事先进行严格的测试验证，确保业务安全，制定完整的技术方案。及时评估割接带来的影响，并通知受影响单位部门，技术方案应包括回退方案；

c） 割接升级操作原则上均应安排在夜间业务闲时执行，一般在凌晨0点以后操作，操作过程应严格按照既定方案实施执行。在操作过程中若出现意外情况，且无法在预定时间内解决，原则上都应回退，若无法回退，则应立即启动应急预案；

d） 调整割接工作完成后须及时进行业务测试和验证，加强值班监控，密切注意调整割接后的业务和网络的运行情况，做好相关记录的归档工作及割接情况总结，并按相关规定上报结果。

* + 1. 故障排查

安全管理应符合GB/T 22239和GB/T 31168的相关规定。具体要求如下：

a） 政务云运营维护部门应对政务云平台进行常态化漏洞扫描，发现服务器、网络设备、云主机、数据库、中间件等软硬件存在的漏洞，应立即采取预防、加固等整改措施，并形成整改报告。同时，进一步做好安全审计、渗透测试、监控异常活动等保障工作；

b） 政务云运营维护部门应制定明确的身份验证、强制密码策略，引入多因素身份验证机制，根据最小权限原则为政务云平台内用户制定特定访问权限，并定期审查与更新访问控制列表，监控和审计访问活动；

c） 政务云运营维护部门根据政务安全监测结果，结合常态化威胁情报信息开展安全策略优化；

d） 政务云运营维护部门应定期开展隐患排查，针对发现的隐患，及时进行预警，按照政务云操作规范，制定整改和规避技术措施。

* + 1. 数据备份和恢复
       1. 数据备份

数据备份是政务云运营及安全的重要工作，包括但不限于虚拟化管理平台配置数据、网络配置数据、存储配置数据、安全设备配置数据以及各类设备账号密码、网络资源数据、运行质量数据和软件数据等。

* + - 1. 数据备份要求

政务云运营维护部门应按照GB/T 34077.3的规定做好数据和应用系统日常备份和恢复。数据备份责任单位应以满足业务使用需求、发生重大数据安全事件时可实现业务快速恢复为目标，根据政务云数据重要性及恢复成本制定具体备份方案，明确备份的数据类型、备份方式、备份周期、备份执行方式、数据存储方式、数据存储周期、验证周期、负责人员等。具体要求如下：

a） 数据备份应定期执行，一般按月或季度执行备份操作。如果涉及政务云升级、割接及数据变动等风险操作，则必须在变动前后各进行一次数据备份操作；

b） 数据备份工作应在不影响政务云安全运行及生产操作的情况下进行。数据备份期间如遇异常情况，维护人员应及时处理，并向主管汇报；

c） 数据备份工作原则上应以远程操作方式实施，定期将所需备份的数据传送到外部文件系统或外部存储介质；

d） 各类备份数据应明确是否要求脱敏或加密传输及存储，需加密的数据应严格执行加密要求。数据备份相关人员应与企业签订数据保密承诺协议；

e） 数据备份方式包括增量备份和全量备份。各类备份数据应明确存储周期，超过时限的数据可予以删除，释放资源。各类备份数据应明确验证周期，维护人员应对备份数据进行定期验证，确保备份数据的准确、有效。数据备份后，应定期检查存储体上的文件是否齐全，文件大小是否和设备上的文件一致，做好检查结果记录；

f） 对系统和数据的备份应有备份日志（自动或手工记录），备份运行人员每周复核备份日志，如发现备份错误或其它异常现象，应于3日内跟进解决。

* 1. 应急保障
     1. 故障处理

政务云资源池故障根据影响业务的范围、持续时间以及性质严重程度，通常分为特别重大故障、重大故障、较大故障和一般故障。

政务云运营维护部门应对主动发现的故障或各政务云用户上报的故障及时进行处理，并应按照要求进行故障上报。对于主动发现的故障，需做好故障通知，及时告知可能受影响的政务云用户。

制定应急响应流程，流程应包括事件发现、事件接报、事件类型判断、应急预案启动、事态控制、应急恢复、应急结束等环节，并按照预先制定的应急处置流程处置突发事件，应急响应结束后，及时进行总结，同步优化、调整和完善应急预案。

* + 1. 应急演练

政务云运营维护部门应按照 GB/T 28827.3的规定，根据实际情况制定政务云应急预案，并负责定期组织开展预案演练，规范应急演练操作规程，确保故障发生时能够及时启动应急预案并恢复业务。

* + 1. 重大保障

在重要活动、重大会议、重要节假日时期，政务云运营维护部门为政务云平台提供安全检查，积极防御，实时检测，响应处置等安全服务。

* 1. 评价与改进
     1. 评价机制

政务云运营维护部门应建立运行维护服务评价机制，明确评价主体、评价内容、评价周期和评价方法，确保评价工作的科学性和公正性。

评价主体应包括政务云指挥调度部门、政务云用户及第三方评估机构，评价内容应涵盖服务指标完成情况、用户满意度、故障处理效率、安全管理水平等。

评价周期分为月度、季度和年度，月度评价以运行维护报告为基础，季度评价以服务质量评估为依据，年度评价应进行全面总结和综合考核。

* + 1. 评价内容

服务指标完成情况：包括系统可用性、故障处理时间、备份恢复成功率等关键指标的达成情况。

用户满意度：通过问卷调查、用户反馈等方式收集政务云用户对运维服务的满意度评价。

故障处理效率：包括故障发现及时性、故障处理时长、故障恢复成功率等。

安全管理水平：包括漏洞修复及时性、访问控制有效性、数据备份完整性等。

* + 1. 改进措施

政务云运营维护部门应根据评价结果，分析问题原因，制定改进措施，并明确责任人和完成时限。

改进措施应包括技术优化、流程完善、人员培训等方面，确保运维服务质量的持续提升。

政务云运营维护部门应定期跟踪改进措施的落实情况，并将改进效果纳入下一轮评价内容，形成闭环管理。

* + 1. 评价结果应用

评价结果应作为政务云运营维护部门绩效考核的重要依据，与运维团队的奖惩机制挂钩。

评价结果应及时向政务云指挥调度部门和政务云用户反馈，增强透明度和信任度。

评价结果应作为优化政务云平台资源配置和服务策略的参考依据，推动政务云平台的持续改进和发展。

