韶关市新区高创中心双创载体采购项目- 公共服务云平台采购项目

内容标准与管理规范手册

广东昆仑信息科技有限公司

2022 年 9 月

1. 范围

本文件规定了韶关市新区高创中心双创载体采购项目公共服务云平台服务管理规范的通用要求，描述了职责分工和资源、安全、迁移、运维服务等。

本文件适用于韶关市新区高创中心双创载体采购项目公共服务云平台的迁移管理和服务管理，各级云管理单位、建设单位及使用单位可参照执行。

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。

3. 术语和定义

GB/T 34078.1和DB/T 2845 所界定的以及下列术语和定义适用于本文件。

3.1. 公共服务云平台

韶关市新区高创中心双创载体采购项目公共服务云平台提供IaaS（基础设施即服务）、PaaS（平台即服务）、SaaS（软件即服务）三个层次的资源服务，本文件所称的公共服务云平台服务还包括安全、迁移、运维等服务内容。

4. 职责分工

4.1. 公共服务云平台管理部门的责任分工

负责公共服务云平台的统筹规划和建设管理，受理和审核云使用单位的资源需求。

4.2. 公共服务云平台监管部门的责任分工

负责公共服务云平台的日常监测工作，对公共服务云平台资源使用情况、云服务商服务能力和服务质量等进行监测和评价。

4.3. 公共服务云平台使用单位的责任分工

负责本部门应用系统的开发测试、迁移部署、运维管理和安全防护等工作。

4.4. 公共服务云平台服务商的责任分工

负责公共服务云平台建设、运行维护和安全保障工作，向云使用单位提供安全可靠的计算、存储、网络、安全和运维等服务。

4.5. 其他

若公共服务云平台管理部门和政务云监管部门为同一部门，则应履行两部门职责的总和。

5. 资源服务

5.1 公共服务云平台提供的服务资源包括 IaaS、PaaS、SaaS 三个层次，服务原则是统一管理、按需选择、弹性扩展、具有高安全性和高可靠性。

5.2 IaaS 层的服务模式：包括机房资源服务、计算资源服务、存储资源服务、网络资源服务和数据备份服务。云平台的管理资源、核心层的网络资源、边界安全资源由云服务商统一提供。

5.3 PaaS 层的服务模式：将云端基础设施部署和创建至客户端，用户借此获得编程语言、程序库的使用与服务。将软件研发的平台做为一种服务，以软件即服务模式交付给用户，为生成、测试和部署软件 应用程序提供开发和部署环境。

5.4 SaaS 层的服务模式：服务商将应用软件统一部署在平台的服务器上，用户

可以根据工作实际需求，通过网络向服务商订购所需的应用软件服务。

5.5 公共服务云平台监管部门应制定统一的云资源服务目录，公共服务云平台使用单位在申请使用云资源时，所需资源应从服务目录中选择。服务目录中没有的公共服务云平台资源应在目录中选择功能和性能相近的进行适配。

5.6 公共服务云平台服务商提供的软硬件产品归公共服务云平台服务商所有，原基础数据和使用电子公共服务云平台后产生的业务数据归公共服务云平台使用单位所有。

6. 安全服务

6.1 公共服务云平台监管部门对公共服务云平台进行实时安全监测，定期开展安全检查，发现安全风险、隐患和安全事件，督促公共服务云平台服务商和公共服务云平台使用单位进行整改。

6.2 公共服务云平台使用单位应加强应用系统日常安全监控，开展网络安全等级保护定级备案及测评工作，开展密码应用安全性评估。对应用系统产生的数据资源进行安全管理，涉及商业秘密、个人隐私等敏感数据的，应对隐私进行保护，并对数据进行脱敏处理。

6.3 应用系统运行过程中收集、产生和存储的数据资源归公共服务云平台使用单位管理。公共服务云平台服务商未经授权，不得访问、修改、披露、利用、转让和销毁公共服务云平台使用单位的数据和文档等资源。应用系统迁出或撤除时，公共服务云平台服务商要做好数据和文档等资源的移交和清除工作。

6.4 公共服务云平台服务商应按照网络安全等级保护第二级安全有关要求，对公共服务云平台进行安全等级保护测评和风险评估。按照密码管理有关要求，定期开展密码应用安全性评估。按照公共服务云平台计算服务安全评估有关规定，进行云计算服务安全评估。

6.5 公共服务云平台服务商应制定安全控制策略并实施安全控制措施，提升公

共服务云平台安全防护能力。制定应急响应预案、重大安全事件处理方案，定期发布安全公告，并开展应急演练。

7. 迁移服务

7.1. 迁移原则

7.1.1. 稳定性原则

公共服务云平台迁移首先要保障应用系统运行的稳定性。迁移之前，应进行详细的评估论证、测试验证，通过技术和管理手段，保障应用运行的稳定性。

7.1.2. 安全性原则

公共服务云平台迁移需要保障平台的安全性，包括网络安全、应用安全和数据安全。公共服务云平台服务商应确保业务数据的完整性、可靠性，降低迁移风险，为公共服务云平台使用单位提供完善的安全管理机制，保障数据安全。

7.1.1 访问方式一致性原则

公共服务云平台迁移应最大限度的保持系统访问的方式不变，避免由于平台的迁移导致访问方式发生变化而给用户带来不便。根据用户的访问方式，公共服务云平台服务商迁移时应制定合理的迁移方案，保障系统迁移前后访问方式的一致性。

7.2. 迁移流程

7.2.1. 申请和审核

公共服务云平台服务商迁出或撤除应用系统时，应向公共服务云平台管理部门提出申请，审批通过后，公共服务云平台服务商使用单位和公共服务云平台服务商共同完成应用停止、数据备份、数据消除和资源回收等工作。

7.2.1 部署和运行

审核通过后，公共服务云平台服务商组织开展系统部署、测试和安全风险预评估等工作。测试通过后，应用系统正式运行，同时将服务协议、测试报告和安全风险评估报告报送公共服务云平台管理部门，由公共服务云平台管理部门存档。

7.2.2. 资源变更

7.2.3.1 公共服务云平台服务商的应用系统需要进行云资源调整时，应向公共服务云平台管理部门提出申请，经审核同意后方可实施。公共服务云平台监管部门提供的云资源使用情况报告为审核的主要依据。

7.2.3.2 公共服务云平台监管部门通过对公共服务云平台使用情况进行监测，对资源利用率明显偏低的应用系统提出资源调整建议，公共服务云平台服务商应根据建议及时调整。

7.2.3. 项目退出

公共服务云平台迁出或撤除应用系统时，应向公共服务云平台管理部门提出申请，审批通过后，公共服务云平台使用单位和公共服务云平台服务商共同

完成应用停止、数据备份、数据消除和资源回收等工作。

8. 运维服务

8.1 公共服务云平台监管部门通过监测公共服务云平台运行维护情况，定期对公共服务云平台服务商的服务质量和满意度进行评价，并公布评价结果。

对监测和评价过程中发现的问题，负责督促公共服务云平台服务商及时整改。

8.2 公共服务云平台服务商负责应用系统的日常运行维护工作。建立健全运维管理制度和应急处置预案，支持并参与公共服务云平台的应急演练、服务评估等活动，发现问题及时向公共服务云平台监管部门通报，确保本部门应用系统安全稳定运行。

8.3 公共服务云平台服务商应建立健全运维管理制度和实施标准，提供 7*24 小时的运行监控。运行维护工作主要包括：资源监测、配置和优化、服务监控、事件处理、流程管理、日常巡检、备份恢复、灾备管理、执行应急预案和配合应急演练等服务。

8.4 公共服务云平台服务商对公共服务云平台实施升级、优化和调整等重大变更前，应书面告知公共服务云平台监管部门，并进行安全影响分析、测试和验证。经评估确保变更不影响公共服务云平台和公共服务云平台使用单位应用系统的正常运行后方可实施。