

附件

内蒙古公共信息资源开放服务管理平台软件和安全运维服务考核表

内蒙古公共信息资源开放服务管理平台软件和安全运维服务项目考核评分表					
一级指标	二级指标	三级指标	评 价 标 准	分值	评价得分
运维服务	1. 基础软件运维服务（6分）	面向操作系统	对基础软件的功能修改完善、性能调优、以及常规的例行检查和状态监控、响应支持等服务。	2	
		面向数据库	根据数据库运行状态进行数据库服务性能调优	2	
		面向中间件	每三个月进行更换中间件东方通密码；根据运行状态进行中间件服务性能调优；	2	
	2. 应用软件运维服务（38分）	开放平台首页	配合部门开通数据源与开放平台网络策略	2	
			开放门户网站功能运维，包括但不限于登录、注册、下载、搜索、查看等功能，保障数据的准确性、及时性，保障门户正常访问；根据要求发布相关资讯。	4	
		目录和资源管理系统	目录管理系统功能运维，包括但不限于目录注册、目录发布、生成文件配置、资源挂载等功能，并协助部门编制开放目录。	3	
			资源管理系统功能运维，包括但不限于资源审核、资源发布、资源变更等功能；维护前置机的连通性；维护文件、库表、接口类资源；协助部门挂接开放资源。	3	
		运行管理系统	运行管理系统功能运维，包括但不限于用户管理、栏目管理、互动交流管理、用户行为日志、统计分析等功能，定期梳理互动交流信息，保障各功能组件正常使用。	3	
		方案报告	编写项目周报、月报、工作总结等文档，统计开放平台已发布目录数、已挂接资源目录数、已发布资源数、部门数据总量、接口调用次数等，并对问题进行排查、分析	3	
			定期梳理平台运行中的问题，针对国家检查报告中的问题进行各类整改，并出具整改报告	3	
		数据归集与开放	定期对平台挂接的库表资源、接口资源进行拨测和检查	1	
			新增开放数据目录50条，对50条新增开放数据目录进行数据梳理与来源确认	10	
			实施跨网域数据物理隔离归集作业。按照资源交换需求，在互联网端建立同结构库表，对已获得授权库表配置交换任务，并制定任务更新策略；每周定期检查库表资源跨网交换情况，排查错误，保证数据一致性。	1	
			按照开放平台资源格式要求，对库表结构数据进行结构化切片与拆分处理	1	
			依据开放规则将库表数据批量转换为 CSV、JSON、XML 等标准文件资源	1	
			建立开放数据定期更新机制，制定更新策略并配	1	

			置自动任务		
			完成开放目录与平台资源的一一映射挂接，实现目录与文件资源关联绑定	1	
			对挂接目录进行目录查询功能校验，对关联资源进行文件调取可用性校验	1	
	3. 安全运维服务（10分）	系统和数据安全	定期对备份数据进行恢复测试	1	
			定期备份应用包，进行本地备份，对备份计划进行巡检	1	
			安全巡检：包括但不限于操作系统运行安全及日志巡检，中间件安全及日志巡检，数据库运行及日志巡检，组件支撑服务安全及日志巡检，插件服务安全及日志巡检，服务器的容量状况巡检，服务器的性能状况巡检，数据备份巡检等	2	
			参加重点节假日、重点工作期间重保工作	1	
			参加国家和自治区组织的攻防演练	1	
			配合第三方做等保测评、渗透测试，对暴露问题整改	1	
			运用云中心安全组件，定期提供安全分析报告，对日常检查暴露安全问题进行整改	1	
			定期对组件漏洞库进行更新升级	1	
			接受云中心、安全处等安全检查，对暴露问题整改	1	
	4. 人员管理（10分）	出勤管理	严格执行请销假制度，不得擅自离岗。驻场项目经理1天及以上假期需向运维负责人请假，驻场技术人员3天及以上假期需向运维负责人请假。	3	
			按时上下班，工作时间不得迟到早退。	3	
		人员保证	一线运维团队离岗离职须通知甲方，并征得甲方取得同意，经同意后三日之内替换人员必须到岗，且为同等级以上技术资质人员。	1	
		岗位要求	运维人员具备独立运维本项目的岗位能力，掌握运维本项目的专业技能。运维人员需不断提升业务能力和服务能力，不得产生服务厅局或服务对象对大数据中心或运维团队的投诉。明确运维团队所在公司高层投诉渠道、联系人及联系电话，因工作态度和业务能力产生的问题，大数据中心有权向所在公司进行投诉。	1	
		办公环境 人员素质	运维人员保持办公场所保持整洁。不得在办公室、楼道、卫生间、机房等公共场所吸烟、吐痰、大声喧哗。运维人员接听办公电话或值班电话、向相关领导汇报工作、其它做相关会议工作，应使用文明语言。原则上不得采用远程在线方式运维，确需采用时，须向负责人报告，并做好相关审批登记、访问控制、在线监测、日志审计等安全工作。经负责人同意后，可通过VPN方式开展运维工作。上班时间不得使用终端电脑和手机玩游戏、上网浏览与工作无关的内容。运维人员上班应穿着整洁大方，不得穿拖鞋等不合时宜衣着，必要时需统一服装（如：应急演练、其它单位参观、上级视察工作等）。	2	
	5. 保密要求（6分）	保密协议签署	一线运维团队与大数据中心签署保密承诺书，运维公司与大数据中心签署保密协议。	2	
		资产信息保密	未经甲方允许不准外借，运维人员（包括离岗离职	2	

			人员)禁止向非本项目人员透露IP、网络拓扑、用户名、密码、设备资产情况等本项目的信息。本项目各种图纸、资料、文件(含电子文档)。		
		离职(离岗)安全管理	离职(离岗)人员不得将本项目涉及网络安全、应用系统安全、数据安全的资料信息带走或者透露给他人,包括但不限于:设备及系统的用户名密码、门禁密码、网络安全配置策略、系统数据等。	2	
	6. 办公安全(6分)	禁止网络混连	互联网笔记本电脑、互联网台式电脑、互联网平板电脑等终端设备必须独立使用在互联网上,(非运维需要或经甲方同意)禁止专网和互联网共用一个终端设备、禁止使用双网卡终端或安装外置网卡,或其他违规外联的情况。	2	
		禁止存储无关数据	运维人员自有电脑离开办公环境禁止存储涉及厅局的业务数据。给运维人员配备的电脑和运维的自有电脑禁止存储和自身运维无关的业务数据。	2	
		禁止关键信息存入外设	运维人员U盘、硬盘、云端、网盘等存储端,禁止存储相关红头文件、涉及厅局的业务数据、配置数据、程序代码等关键信息,上述信息禁止带出办公场所以外的场所。	2	
	7. 培训内容(2分)	应用系统培训	每年至少举办一次应用系统培训工作。	2	
	8. 二次开发指标要求(20分)	用户中心快捷入口访问链接改造	对快捷入口的访问链接进行改造,实现链接访问的身份认证与数据传输加密,保障用户访问过程的安全性。	1	
		网站服务入口访问链接改造	对主服务入口的访问链接实施改造,集成密码算法实现访问身份验证和传输数据加密,防止链接被篡改或劫持。	1	
		网站资料中心已发布资料访问链接改造	对已发布的各类资料访问链接进行改造,通过密码技术确保资料访问的授权控制和传输数据完整性,防止未授权访问。	2	
		用户信息安全管理	对基础信息实施改造,实现信息的加密存储、安全传输和访问权限控制,保障用户数据机密性。	1	
		登录接口服务	对系统登录接口服务进行改造,集成密码认证机制实现用户登录身份的强验证,防止登录信息被窃取或伪造,保障登录过程安全。	1	
		用户信息查询服务	对信息查询接口实施改造,通过密码技术确保用户信息查询过程的安全性和数据完整性。	1	
		历史数据处理	对历史数据进行合规处理,确保历史数据符合安全要求。	1	
		数据源管理改造	对数据源管理功能实施改造,保障数据源管理过程的安全性和数据机密性。	1	
		资源管理改造	对资源管理模块进行改造,全面提升资源管理的安全等级。	1	
		数据源服务改造	对数据源服务接口实施改造,保障数据源服务的安全性。	1	
		历史数据处理	对历史数据进行合规处理,确保历史数据安全合规。	1	
		服务代理改造	对服务代理模块进行改造,保障服务代理过程安全。	1	
		服务appkey信息改造	对服务appkey信息实施改造,防止appkey被窃取或滥用,保障服务访问安全。	1	
		服务动态令牌	对动态令牌信息进行改造,确保动态令牌的安全	1	

		信息改造	性和有效性，防止令牌被伪造。		
		服务调用流水	对调用流水记录实施改造，防止调用流水被篡改或泄露，保障服务调用过程可追溯。	1	
		调用情况分析	对服务调用情况分析功能进行改造，确保调用情况分析的准确性和数据安全性。	1	
		历史数据处理	对历史数据进行合规处理，确保历史分析数据安全合规。	1	
		数据交换机密性改造	对数据交换过程实施机密性改造，防止数据在交换过程中被未授权获取或泄露。	1	
		数据交换完整性改造	对数据交换过程实施完整性改造，保障交换数据的真实性和可靠性。	1	
	9. 服务满意度（2分）	用户对象满意度	服务对象发放问卷调查表，根据用户满意率评价。	2	