合同编号：_____

贵州省残疾人联合会2025年政务信息化项目系统运维服务合同

项目名称：贵州省残疾人联合会2025年政务信息化运维项目（A包）

甲方：贵州省残疾人联合会

法定代表人：方胜

通信地址：贵州省贵阳市云岩区山林路2号

邮政编码：550003

乙方：贵州人和致远数据服务有限责任公司

法定代表人：罗磊

通信地址：贵州省贵阳市观山湖区林城西路摩根中心A座8层

邮政编码：550009

甲乙双方遵照《中华人民共和国民法典》及有关法律、行政法规，本着诚实信用、平等双赢、长期合作、共同发展的原则，经友好协商一致，就贵州省残疾人联合会2025年政务信息化运维项目（A包）签订本合同，以兹共同信守。

第一条 服务项目

1.1 服务类型

甲方通过招标方式确定由乙方向甲方提供贵州省残疾人联合会2025年政务信息化运维项目（A包）服务。

1.2 服务地点：贵州省贵阳市。

1.3 服务内容、服务期限及要求具体如下：

项目名称	服务范围和要求	总价（万元）	服务时间
一、贵州省残疾人大数据智慧服务云平台一期、二期、三期运维	**（一）运维内容** 对贵州省残疾人大数据智慧服务云平台一期、二期、三期的电脑端、移动端（app、微信小程序）各功能模块运维服务、数据运维服务。 **（二）运维指标** 7×24 小时电话或电子邮件服务，接收到服务请求后，在 10 分钟内给予响应， 1 小时内作出明确的响应安排，2 小时内处理完毕。2 小时内还未能处理完毕，影响到系统正常运行的，要及时书面报告残联办公室，以便采取应急措施。 **（三）运维服务方式** 驻场服务人员需求为中级产品经理 1 人，驻场人员要求具备本科以上文凭，计算机或相关专业毕业，具有 4 年以上相关项目维护经验。 **（四）运维团队人数**	76.22	2025 年 04 月 01 日—2026 年 3 月 31 日

	运维团队3人。其中驻场中级运维人员2人，产品运维人员1人；远程运维团队：项目经理1人，前端开发1人，后端开发2人，界面设计师1人，测试工程师1人。 **（五）数据处理** 本项目所含系统的数据，支持按用户需求进行导入、导出、比对，具体数据处理内容如下： 1、支持本系统与贵州省数据共享平台进行数据互通； 2、支持本系统与中国残联系统进行数据互通，包括数据的导出与导出； 3、支持与贵州省人社厅、贵州省残疾人联合会、贵州省扶贫办、贵州省医保局等单位数据比对和数据导入； 4、省残联与贵阳市残联每年需要更新残疾人动态更新基础数据。 **（六）远程及线上服务** 包括迁云技术支持；系统24小时保障；大规模调查期间，至少为2万名调查人员提供线上咨询服务。		
二、省残联电子政务协同办公平台（OA）统筹运维	**（一）服务范围** 1、提供系统日常运维，保障贵州省残疾人联合会电子政务协同办公平台（OA）、“数字机关”建设：5张表单个性化应用。 2、远程服务内容：设立呼叫中心，5×题咨8小时通过电话方式受理问询与解答，通过远程方式进行系统问题诊断与解决，每年12次远程巡检服务，检查应用系统、应用服务器、数据库运行指标，针对系统使用过程中出现的bug，合理需求进行服务器维护，服务器维护后对系统稳定、系统功能等进行测试，确保系统运行正常。 3、对移动办公OA系统进行重新授权，开通相应移动办公业务。 **（二）服务要求** 1、运维方式：账户运维，远程	6.35	2025年04月01日—2026年3月31日

	服务，本地服务、系统培训。 2、运维指标：提供7×24小时服务；0.5小时内响应服务；一般故障2小时内恢复，重大故障8小时内恢复。 3、运维服务方式：采用远程+现场服务方式。		
三、省残联机关办公区宽带租赁	**（一）服务范围** 运维内容：租用1条500M的互联网专线。 **（二）服务要求** 1、运维指标：提供7×24小时服务；0.5小时内响应服务；一般故障2小时内恢复，重大故障8小时内恢复。 2、运维服务方式：采用远程+现场服务方式。	1.07	2025年04月01日—2026年3月31日
四、省残联门户网站运维	**（一）服务范围** 保障贵州省残疾人联合会官网正常运行 **（二）服务要求** 1、运维内容：支持远程巡检和运维，支持故障处理和恢复，保障贵州省残疾人联合会官网正常运行。 2、运维指标：7×24小时电话或电子邮件服务，接收到服务请求后，在10分钟内给予响应，1小时内作出明确的响应安排，2小时内处理完毕。2小时内还未能处理完毕，影响到系统正常运行的，要及时书面报告残联办公室，以便采取应急措施。 3、运维服务方式：采用远程+现场服务方式。	4.10	2025年04月01日—2026年3月31日
五、省残联电子政务协同办公平台安全服务	**（一）服务范围** 1、渗透测试：通过模拟恶意黑客可能使用的攻击技术和漏洞发现技术，对受测网络及应用系统进行深入探测，发现信息系统最薄弱的环节，充分了解网络及应用当前存在的安全隐患。 2、代码审计：以发现程序错误，安全漏洞和违反程序规范为目标	5.37	2025年04月01日—2026年3月31日

	的源代码分析，寻找系统中存在的薄弱环节和业务逻辑问题、漏洞等。代码审计采取自动化工具或者人工审查的方式，通过对编程项目中源代码的全面分析，旨在发现错误，安全漏洞或违反编程约定的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方。代码审计过程需要对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞。防御性编程范例的一个组成部分，能够试图在软件发布之前减少错误。提供代码修订措施和建议，提供代码审计报告。 3、网站监测：全方位的对网站可用性进行监控，敏感词监测、网页防篡改监测、木马暗链等监测。 **（二）服务要求** 1、运维内容：省残联电子政务协同办公平台安全服务。 2、运维指标：7×24 小时电话或电子邮件服务，接收到服务请求后，在 10 分钟内给予响应，1 小时内作出明确的响应安排，2 小时内处理完毕。2 小时内还未能处理完毕，影响到系统正常运行的，要及时书面报告残联办公室，以便采取应急措施。		
六、省残联门户网站安全服务	**（一）服务范围** 1、渗透测试：通过模拟恶意黑客可能使用的攻击技术和漏洞发现技术，对受测网络及应用系统进行深入探测，发现信息系统最薄弱的环节，充分了解网络及应用当前存在的安全隐患。 2、代码审计：以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析，寻找系统中存在的薄弱环节和业务逻辑问题、漏洞等。代码审计采取自动化工具或者人工审查的方式，通过对编程项目中源代码的全面分析，旨在发现错	5.67	2025 年 04 月 01 日—2026 年 3 月 31 日

	误，安全漏洞或违反编程约定的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方。代码审计过程需要对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞。防御性编程范例的一个组成部分，能够试图在软件发布之前减少错误。提供代码修订措施和建议，提供代码审计报告。 3、网站监测：全方位的对网站可用性进行监控，敏感词监测、网页防篡改监测、木马暗链等监测。 **（二）服务要求** 1、运维内容：省残联门户网站安全服务。 2、运维指标：7×24 小时电话或电子邮件服务，接收到服务请求后，在 10 分钟内给予响应，1 小时内作出明确的响应安排，2 小时内处理完毕。2 小时内还未能处理完毕，影响到系统正常运行的，要及时书面报告残联办公室，以便采取应急措施。		
七、省残联智慧服务云平台安全服务	**（一）服务范围** 1、下一代防火墙 （1）具备传统防火墙、入侵防御、入侵检测、防病毒、应用防护、流量管控、抗 DDOS 攻击、IP SEC VPN、SSL VPN、DMVPN 等安全防护功能； （2）为了简化安全配置的高效、便捷、安全性，产品必须支持通过一条安全策略实现协议控制、用户认证、URL 过滤、入侵防御、病毒防护、流量控制、并发、新建限制、垃圾邮件过滤、审计等安全功能； （3）支持同一个地址对象中可以包含 IP、IP 段、IPrange、排除地址等多种类型； 支持针对策略中的源、目的地址进行新建限制，可以针对单 IP(或地址范围)进行新建控制； （4）支持 web 界面下对攻击流量进行抓包分析，支持自定义抓包参	30.74	2025 年 04 月 01 日—2026 年 3 月 31 日

	数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；支持根据协议、源目的 IP、端口等参数进行数据报文过滤； （5）产品具备日志分发能力，支持按照不同类型的日志进行分发，并具备不少于 3 个 Syslog 服务器，用于发送流量、系统或默认 3 类型日志到不同服务器； （6）支持 FTP、SMTP、POP3、NNTP 等不少于 8 种协议及应用的弱口令检测、支持基于弱口令字典及弱口令识别算法的多方位检测、支持协议及应用的暴力破解防护、支持暴力破解事件的日志合并及日志生成频率设置； （7）支持区域地址所属查询，能针对国外地址进行有效防护和管理； 2、堡垒机 （1）对资产运维进行管控，提供账号管理、身份认证、自动改密、资源授权、实时阻断、同步监控、审计回放等能力，增强运维管理的安全性，具备强大的输入输出审计能力； （2）为了便于后期运维保障升级扩容，需具备添加一台或多台协议代理服务器，分担堡垒机主服务器性能压力，便于提高整体性能； （3）具备 NAT 地址映射部署，通过映射后的 IP 地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境； （4）具备自动改密功能，密码策略支持随机生成不同密码 、随机生成相同密码、手工指定相同密码，随机密码支持自定义密码强度； （5）具备通过应用发布实现数据库操作的命令级审计和图形审计的双重审计效果， 命令级审计便于重现真实的完整		

	操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句关键字定位审计回放； （6）具备实时监控当前连接发生的所有会话信息，发现高危操作可实时切断会话；具备在线和离线视频回放方式重现维护人员对服务器的所有操作过程，具备倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作；具备通过搜索操作关键字定位回放。 3、SSL/VPN （1）提供通用安全套件，确保传输数据的机密性及完整性。实现安全.快速接入； （2）为满足当前终端接入环境，客户端需支持龙芯、兆芯、飞腾、鲲鹏等国产化 CPU 平台，支持中标麒麟，银河麒麟、普华、深度 OS、优麒麟、UOS 统信、中科方德等国产化操作系统客户端； （3）支持多数据库，根据用户规模的大小，可以灵活切换 SQLite 和 Mysql 数据库，支持数据库备份和还原操作； （4）支持对在线用户的实时监测，包括 VPN 用户信息、程序名称、会话 ID、客户端名称和用户类型； （5）支持用户 IE 配置一键复制，提高部署效率，可以复制各种 IE 插件设置、cookie 设置、权限设置等； （6）支持用户将文件存储在服务器端私人文件夹当中，具有用户私人属性，仅允许用户访问到自己私人文件夹的方法； （7）支持通过磁盘映射方式，进行客户端本地磁盘的物理映射，满足从应用导出数据到本地磁盘或者从本地磁盘选择文件导入到应用上的需求。 4、漏洞扫描 （1）通过对系统进行安全脆弱性		

	深度检测，发现可被利用漏洞，并提供漏洞修复方法及建议； （2）具备对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、深度、红旗、中标麒麟等；具备扫描 IPv6 环境中的设备、系统； （3）具备对主流数据库的识别与扫描，包括：Oracle、Sybase、GBASE、GaussDB、达梦、人大金仓、优炫等，能够扫描的数据库漏洞扫描方法不小于 2600 种； （4）具备多种协议口令猜测，包括 SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、 DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、 ActiveMQ、WebLogic、WebCAM 等； （5）具备 35 种以上默认扫描策略模板，如常规安全扫描、中高危漏洞扫描、高危漏洞扫描、web 服务组件扫描、网络设备扫描、云平台漏洞扫描、虚拟化扫描、主机信息收集、攻击性扫描、SQLSERVER 数据库扫描、Apple 类扫描、视频监控类扫描等等，同时针对市场应急响应的漏洞提供应急响应策略模板； （6）具备以 txt、csv、dat、xls 等格式进行资产列表的导入；具备每个资产历史扫描的风险趋势图显示，缺省显示最后 24 次扫描结果的趋势显示； （7）控制台功能可以通过控制台对系统进行操作和设置，例如重启和关闭系统、修改系统和网络配置、查看漏扫引擎状态并提供网络诊断工具； 5、数据库审计 （1）以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的		

	风险行为进行实时告警。 （2）支持对 Oracle 数据库状态的自动监控，可监控会话数、连接进程、CPU 和内存占用率等信息。 （3）支持国产数据库人大金仓、达梦、南大通用、神通、高斯、瀚高、巨杉、Oce anBase 、AnalyticDBMySql 、AnalyticDBMySql 、AnalyticDBPostgreSQL、RDSMySql、RDSPostgreSQL 等数据库的审计。 （4）支持 MongoDB、redis 数据库的审计。 （5）支持对针对数据库的 SQL 注入、CVE 高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。 （6）系统支持数据库中存储过程自动学习，可学习存储过程中涉及的操作并与审计事件中的存储过程名进行关联，方便确认存储过程是否存在风险。 6、日志审计 （1）对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月； （2）提供网络设备、安全设备与系统、主机、中间件、数据库、存储、应用和服务在内的多种审计数据源的日志采集，并且提供日志过滤归并功能提高日志采集能力；支持针对日志的查询，告警，审计，报表，报告等功能； （3）为适应网络环境中的各类设备日志采集，需具备 SNMPTrap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC 等多种方式完成日志收集功能； （4）具备显示告警状态雷达图，日志趋势曲线图；最近事件览图；最近一段时间不同日志分类的日志数量，不同等级的日志的数量，		

	事件 EPS 曲线； （5）具备日志审计外发联动安全管理平台/态势感知类产品，日志可加密压缩传输，具备加密压缩方式转发，定时转发；支持日志源管理功能，对断点日志源可以产生告警； （6）提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表； 7、主机防病毒 （1）支持可疑文件检测，支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型病毒查杀； （2）支持勒索病毒专项检测防护能力；支持挖矿病毒专项检测防护能力。 （3）支持首页声音告警，有新事件及时提醒管理人员关注。 （4）支持 windows 与 linux 策略进行差异化配置与维护。 （5）支持终端基础资产清点，包括：IP、连接 IP、MAC、资产名称、操作系统版本、内核版本、处理器、内存、硬盘大小和型号、网卡型号、首次在线时间、最后在线时间等。 （6）支持详细记录终端进程每一次变动信息，包括：进程 ID、进程名、动作（启动、退出）、进程路径、父进程 ID、父进程名、进程命令行参数、启动或退出时间。 8、基线核查加固 根据国际、国内、行业相关标准，建立各主流操作系统、数据库、中间件、虚拟设备等相关资产的安全基线要求，核查加固安全运维服务人员所维护的安全设备系统安全基线情况。根据漏洞扫描报告进行有效修复、减少系统中存在的高、中危漏洞，降低安全漏洞和隐患带		

	来的安全风险，提升系统自身的安全防护能力，最大程度保障系统的持续、安全、稳定运行。一年 4 次。 9、渗透测试 通过模拟恶意黑客可能使用的攻击技术和漏洞发现技术，对受测网络及应用系统进行深入探测，发现信息系统最薄弱的环节，充分了解网络及应用当前存在的安全隐患。 10、风险评估 从风险管理角度，依据有关信息安全技术与管理标准，对信息资产所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估。基于全面的风险评估，准确了解信息安全现状，明晰信息安全需求。基于风险评估结果，针对性制定信息系统安全策略和风险解决方案。结合技术与管理，指导未来的信息安全建设和投入，建立自身的信息安全管理框架。1 年 1 次。 11、安全培训 安全问题“三分技术、七分管理”，作为安全管理的主要执行者/人员，在面临信息安全威胁的严峻挑战时，提高安全意识和安全技能，成为了一项必要的工作。提供信息安全意识培训、信息安全技能教育培训，从而真正提升受训人员的安全技术和实际动手能力。提升相关人员的信息安全意识、保密意识；落实网络安全法对信息安全教育培训的要求；提升参训的人员的信息安全技能、了解和掌握基本的信息安全知识。1 年 2 次； 12、网站监测 全方位的对网站可用性进行监控，敏感词监测、网页防篡改监测、木马暗链等监测。 13、预警通告 通告内容包括安全事件、安全公		

	告、病毒信息、漏洞信息，以便第一时间得到漏洞的修补办法，防止安全事件的发生。有效的预防安全事故发生，并可以及时做出针对措施，1 年实时预警通告。 14、应急演练 针对单位整体安全状态保障的服务，该项服务形式多样，可根据实际情况进行调整。行业、单位或部门通过采取安全演练的方式，反思、整改，吸取教训弥补不足，总结经验推动工作，进一步完善网络信息安全工作方案及应急预案，提高工作能力。通过应急演练活动，行业、单位或部门建立健全应用系统和网络运行应急工作机制，验证相关组织、人员对应用系统及网络运行突发事件的组织指挥能力和应急处置能力，同时验证单位现有应急预案的可行性，并对应急预案进行及时更新完善，进一步提高应对突发紧急安全事件的能力。1 年 2 次应急演练。 15、应急响应 应急响应服务提供 7*24 小时的电话支持安全服务，根据网络管理员或系统管理员的初步判断和相关安全事件，通过电话咨询安全服务人员，服务人员会根据客户信息提供电话支持服务，在客户和安全服务人员同时确认需要信息安全专家或安全服务队伍现场支持后，根据客户安全事件级别进行应急响应。1 年应急响应。 16、网站云防护 提供网站云防护能力，包含：云抗 DDOS 防护能力、云 WAF 服务、WEB、SHELL 防护、云 DNS 服务、网站加速服务、端口隐藏服务、地域访问控制、邮件通知、防护报告：月报、人工专家服务、1 年 2 个系统的网云防护，防护时段：7×24。 **（二）服务要求** 1、运维内容：省残联智慧服务云		

	平台安全服务。 2、运维指标：7×24 小时电话或电子邮件服务，接收到服务请求后，在 10 分钟内给予响应，1 小时内作出明确的响应安排，2 小时内处理完毕。2 小时内还未能处理完毕，影响到系统正常运行的，要及时书面报告残联办公室，以便采取应急措施。		
总计：含税金额为¥1295200.00 元整（大写：壹佰贰拾玖万伍仟贰佰元整）。			

第二条 价款及划转方式

2.1 本项目合同总金额：人民币（大写）壹佰贰拾玖万伍仟贰佰元整，（小写）¥1295200.00 元整，该费用为含税价。费用包含：乙方应承担提供技术服务和技术支持的费用、技术培训费用（包括教材、课程费等），以及乙方为全面履行合同义务所需支付的所有其他费用。

2.2 付款方式：

第一次付款：甲乙双方签订合同后的 30 日内，乙方向甲方开具全额增值税普通发票，甲方收到乙方发票后的 15 个工作日内，甲方向乙方支付合同总金额的 60%，即人民币（大写）柒拾柒万柒仟壹佰贰拾元整，（小写）¥777120.00 元整。

第二次付款：乙方人员入驻且正常运维 90 日内，甲方再次向乙方支付合同总金额的 30%，即人民币（大写）叁拾捌万捌仟伍佰陆拾元整，（小写）¥388560.00 元整。

第三次付款：乙方人员入驻且正常运维 180 日内，甲方再次向乙方支付合同总金额的 5%，即人民币（大写）陆万肆仟柒佰陆拾元整，（小写）¥64760.00 元整。

第四次付款：项目根据本合同第五条通过甲方或甲方委托的第三方组织验收通过后 30 天内，甲方向乙方支付项目合同金额的 5%，

即人民币（大写）陆万肆仟柒佰陆拾元整，（小写）¥64760.00元整。

第三条 甲方的权利义务

3.1 甲方的权利

3.1.1 甲方有权随时向乙方了解项目进度，并要求乙方提供项目相关资料。

3.1.2 甲方有权按照本合同约定或有关法律法规规定，对本项目进行监督和检查，如乙方未按照本合同约定提供服务，或乙方提供的服务违反法律法规的强制性规定的，甲方有权要求乙方按照监督检查情况制定相应措施并对违反法律法规的行为加以整改。甲方不因行使该监督和检查权而承担任何责任，也不因此减轻或免除乙方根据本合同约定或相关法律法规 规定应承担的任何义务或责任。

3.1.3 甲方有权在乙方履行合同过程中出现损害公共利益、公共安全情形时终止本合同。

3.1.4 甲方有权将乙方履行合同情况及不符合政府购买服务相关法律规定情况，向相关部门报告并主张纳入不良信用记录、年检（报）、评估、执法等监管体系中。

3.2 甲方的义务

3.2.1 甲方应按照合同约定向乙方支付本合同价款。

3.2.2 甲方应积极协调、组织原运维服务团队在合同签订后 7 日内与乙方开展运维服务交接，确保运维服务工作交接完成。若甲方未按照约定协调或经甲方协调后，原运维服务未在前述期限内与乙方开展运维服务完成交接，由此产生的全部损失及责任由甲方承担，导致乙方迟延开始运维服务的，乙方不承担违约责任。

3.2.3 甲方应及时向乙方提供与履行本合同相关的且甲方有权提

供的必要文件、资料，包含但不限于完整且正确的系统源代码、运维日志、系统设计文件、网络拓扑设计文件及系统安装部署手册等资料等系统相关资料。

3.2.4 甲方应为乙方履行本合同过程中与相关政府部门、原运维服务团队及其他第三方的沟通、协调提供必要的协助。

3.2.5 甲方应向乙方提供系统相关源代码授权。

3.2.6 甲方应向乙方现场运维人员提供良好的工作环境和工作条件。

第四条 乙方的权利义务

4.1 乙方的权利

4.1.1 乙方有权按照本合同约定向甲方收取本合同价款。

4.1.2 乙方有权自甲方处获得与提供本合同项下服务相关的所有必须的文件、资料，如甲方未能合理提供服务所需的相关文件、资料及工作环境或工作条件，因此导致乙方服务不符合合同相关约定的，乙方不承担相应责任。

4.1.3 乙方有权要求甲方协调、组织原运维服务团队在内的其他第三方为乙方履行本合同项下的服务提供必要协助。

4.2 乙方的义务

4.2.1 乙方应接受甲方的监督管理。

4.2.2 乙方应建立安全管理制度和措施，按照《中华人民共和国网络安全法》等法律法规以及政务信息系统安全管理等有关规定实施。

4.2.3 乙方应建立健全服务应急处置机制，保障系统日常稳定运行。

4.2.4 如乙方工作过程中造成他人安全事故，由乙方承担全部责任。

第五条 服务标准、过程管理及验收

5.1 服务标准

服务标准依照本合同条款“1.3 服务内容及要求”及《信息技术软件维护》（GB/T20157-2006）、《信息技术服务运行维护第 1 部分：通用要求》（GB/T28827.1-2012）、《信息技术服务运行维护第 2 部分：交付规范》（GB/T28827.2-2012）、《信息技术服务运行维护第 3 部分：应急响应规范》（GB/T28827.3-2012）、《信息技术服务质量评价指标体系》（GB/T33850-2017），以及《贵州省省级政务信息系统建设管理办法》（黔府办函〔2023〕2 号）等文件的规定执行。

5.2 验收

5.2.1 验收主体

甲方或甲方委托的第三方组织对乙方提供的服务进行验收。

5.2.2 验收方式和验收标准

验收方式和验收标准依照本合同条款“1.3 服务内容及要求”及“5.1 服务标准”的规定执行。

5.2.3 验收流程

乙方在 2026 年 3 月 31 日完成项目合同约定服务内容后的【10】个工作日，按照《省级政务信息化项目服务验收细则（试行）》相关要求乙方向甲方提出项目验收申请。甲方在收到验收申请后应在【10】个工作日内受理项目验收申请，由甲方或甲方委托的第三方在【10】个工作日组织相关专家进行验收，若甲方或甲方委托的第三方机构未

在上述期限内组织验收、审核，则视为本项目验收合格。

验收通过：由甲方或甲方委托的第三方组织相关专家出具验收意见验收通过，由甲方或甲方委托的第三方组织相关专家出具验收意见书，乙方按照相关意见优化完善相关服务，持续做好后续工作；服务验收不通过，甲方有权要求乙方采取更换、修复、维护等必要措施，乙方收回相关验收材料，限期完成相关整改后重新提交服务验收申请。

5.3 资料移交

在项目通过验收后的一个月内，乙方须向甲方完成项目资料移交。并配合甲方完成验收报告等材料报省大数据局备案，同时资料移交纸质版和电子版各一份，移交纸质资料应为原件，移交电子版资料可阅且不可篡改。

第六条 知识产权

乙方保证对所提供的技术资料、知识产权等具有合法产权或已取得合法授权，不存在侵犯他人合法权利的情形。由于乙方的原因侵犯第三人权利的，由乙方承担因此给甲方所造成的一切损失（包括但不限于赔偿费、调查取证费、差旅费、律师费等）。

第七条 保密条款

7.1 各方应遵守国家有关保密的法律法规和行业规定，并对甲方、乙方提供的资料及商业秘密负有保密义务。未经甲方、乙方同意，不得将承接本项目获得的政府、公民个人等各种信息和资料提供给其他无关的单位和个人。如发生以上情况，违反相关法律法规者应当承担有权索赔并追究违约法律责任。

7.2 本合同保密条款长期有效，无论本合同是否生效、被撤销、

变更、解除或终止，各方仍应执行本合同保密条款。

第八条 违约责任

8.1 甲方在监督检查过程中发现乙方存在以下问题的，乙方应按要求及时整改：

（1）与相关法律法规不符合的。

（2）甲方对乙方未能在合理时间内整改或经多次整改后仍不符合合同约定的，甲方有权终止合同，待乙方整改完成后重签合同。

8.2 因乙方原因出现运维服务中断的情况，乙方应从逾期之日起每日按具体未完成项目服务费的 0.1‰的数额向甲方支付违约金，并赔偿甲方的损失。但因甲方需求变更等非乙方原因造成的服务无法进行或按期完成的，乙方不承担逾期违约责任。

8.3 甲方应严格按照合同约定期限支付合同约定费用，逾期一日的，应按中国人民银行公布同期同类贷款市场报价利率计算向乙方支付违约金，超过【60】日的，乙方有权解除合同，并要求甲方承担相应的违约责任。

8.4 任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件发生后 2 日内向另一方书面通报，以减轻可能给另一方造成的损失，在取得有关机构的不可抗力证明或谅解确认后，允许相应延期履行或修订合同，并可根据具体情况部分或全部免于承担违约责任。由于不可抗力导致合同不能履行的，任意一方均有权终止合同。

8.5 发生其他违约情形，违约方应赔偿由此给守约方造成的一切损失及为维护合法权益而支出的一切费用，包括但不限于诉讼费、保全费、律师费。尽管合同中有任何其他规定，乙方承担的全部合同责

任及与合同履行相关责任的赔偿总额不得超过合同金额的100%，若对方公司违约导致贵会损失超过合同金额，则按实际损失计算不受违约金上限的限制。该责任上限适用于违约、侵权、过失等乙方应承担的全部法律责任。

8.6 甲、乙双方应遵循诚实信用原则，按照合同约定充分履行合同义务，保障合同顺利履行完毕。若因非可归责于双方的原因导致项目提前终止，双方另行商定解决方案，防止国有资产投资风险及损失。

第九条 合同终止

1. 合同期满，双方未续签的。

2. 合同双方协议终止本合同履行。

3. 本合同终止并不影响各方应有的权利和应承担的义务。

4. 本合同的权利义务终止后，甲方和乙方应当遵循诚实信用原则，履行通知、协助、保密等义务。

第十条 争议解决

本合同在履行过程中发生的任何争议，如各方不能通过友好协商解决，任何一方均可通过甲方所在地人民法院诉讼处理。除有关争议的条款外，在争议的解决期间，不影响本协议其他条款的继续履行。

第十一条 通知与送达

11.1 根据本合同需要发出的全部通知，均须采取书面形式，以（1）专人递送，（2）特快专递，（3）传真，或（4）挂号信件发出。特快专递或挂号信件的交寄日以邮戳为准。上述书面通知均须标明合同各方为收件人。

11.2 上述书面通知按对方在本合同中所列的地址发出，如任何一方的地址有变更时，须在变更前10日以书面形式通知对方。因迟延通知而造成的损失，由过错方承担责任。

11.3 甲乙双方将按如下规定确定通知被视为正式送达的日期;

11.3.1 以专人递送的，接收人签收之日视为送达;

11.3.2 以传真方式发出的，以发件方发送后打印出的发送确认单所示时间视为送达;

11.3.3 以特快专递形式发出的，发往本市内的，发出后第3日视为送达。

11.3.4 以挂号方式发出的，发往本市内的，邮寄后第3日视为送达。

11.3.5 上方约定的送达方式同样适用于司法程序的相关送达。

第十二条 其他

12.1 本合同自甲乙双方加盖公章之日起生效。

12.2 本合同一式六份，具有同等法律效力，甲乙双方各执叁份。

12.3 本合同未尽事宜，由甲乙双方另行签订补充协议，与本合同具有同等法律效力。补充协议条款与本合同不一致的，以补充协议为准。(以下无正文)

（本页无正文，为《贵州省残疾人联合会2025年政务信息化运维项目（A包）》的签章页）

甲方（盖章）

单位名称：贵州省残疾人联合会

法定代表人或授权代表（签字）：

2025年 6月 26日

乙方（盖章）

单位名称：

法定代表人或授权代表（签字）：

2025年 6月 26日