“陕西智慧教育综合服务平台”
工程服务项目

招 标 文 件

项目编号：SNJZ-2022-188

陕西教育招标有限责任公司

2022 年 11 月 29 日

目　录

第一章 招标公告

项目概况

“陕西智慧教育综合服务平台”工程服务项目招标项目的潜在投标人应在陕西教育招标有限责任公司业务一部（地址：西安市太白南路 181 号 西部电子社区 A 座 B 区 401）获取招标文件，并于 2022 年 12 月 20 日 14 时 30 分 （北京时间）前递交投标文件。

一、项目基本情况：

项目编号：SNJZ-2022-188

项目名称：“陕西智慧教育综合服务平台”工程服务项目

采购方式：公开招标

预算金额：3,100,000.00 元

采购需求：

合同包 1(“陕西智慧教育综合服务平台”工程服务):

合同包预算金额：3,100,000.00 元

合同包最高限价：3,100,000.00 元

品目号	品目名称	采购标的	数量（单位）	技术规格、参数及要求	品目预算(元)	最高限价(元)
1-1	其他运行维护服务	“陕西智慧教育综合服务平台”工程服务	1	详见采购文件	3100000.00	3100000.00

本合同包接受联合体投标

合同履行期限：在采购人规定的时间段内完成各项服务内容，详见《招标文件》。

二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定;

2.落实政府采购政策需满足的资格要求：

合同包 1(“陕西智慧教育综合服务平台”工程服务)落实政府采购政策需满足的资格要求如下:

本项目非专门面向中小企业采购，依据《中华人民共和国政府采购法》和《中华人民共和国政府采购法实施条例》等有关规定，落实政府采购“优先购买节能环保产品、扶持小微企业、监狱企业、福利企业” 等相关政策。

（1）《政府采购促进中小企业发展暂行办法》（财库〔2020〕46 号）；（2）《财政部　司法部关于政府采购支持监狱企业发展有关问题的通知》(财库〔2014〕68 号）；（3）《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）；（4）《节能产品政府采购实施意见》（财库[2004]185 号）；（5）《环境标志产品政府采购实施的意见》（财库[2006]90 号）；（6）《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51 号）；（7）《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》--（财库〔2019〕9 号）；（8）《关于印发环境标志产品政府采购品目清单的通知》--（财库〔2019〕18 号）；（9）《关于印发节能产品政府采购品目清单的通知》--（财库〔2019〕19 号）；（10）《市场监督总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》—2019 年第 16 号；（11）《关于运用政府采购政策支持乡村产业振兴的通知》（财库〔2021〕19 号）；（12）陕西省财政厅关于印发《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23 号），相关政策、业务流程、办理平台（详见 http://www.ccgp-shaanxi.gov.cn/zcdservice/zcd/shanxi/）；（13)《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15 号）；（14）《关于进一步加强政府绿色采购有关问题的通知》（陕财办采〔2021〕29 号）；（15）《陕西省财政厅　陕西省工业和信息化厅关于运用政府采购政策支持首台（套）及创新产品有关事项的通知》(陕财办采〔2021〕17 号）；（16）其他需要落实的政府采购政策。若享受以上政策优惠的企业，提供相应声明函或品目范围内产品有效认证证书。

3.本项目的特定资格要求：

合同包 1(“陕西智慧教育综合服务平台”工程服务)特定资格要求如下:

（1）具有独立承担民事责任能力的法人、其他组织或自然人，提供营业执照/事业单位法人证书/非企业专业服务机构执业许可证/自然人身份证。（2）法定代表人参加投标时，提供法定代表人证明书；授权代表参加投标时，提供法定代表人授权书；非法人单位参照执行。（3）财务状况报告：提供 2021 年度的财务报告，或提交投标文件截止时间前六个月内银行资信证明，或政府采购信用担保机构出具的投标担保函。（4）税收缴纳证明：提供投标文件递交截止时间前六个月内至少一个月已缴纳的纳税凭据或完税证明，依法免税的投标单位应提供相关文件证明。（5）社会保障资金缴纳证明：提供投标文件截止时间前六个月

内已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明,依法不需要缴纳社会保障资金的单位应提供相关证明材料。(6)提供具有履行本合同所必需的设备和专业技术能力的承诺。（7）提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。（8）投标单位不得为“信用中国”网站（www.creditchina.gov.cn）中列入失信被执行人和重大税收违法案件当事人名单的投标单位，不得为中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的投标单位。（9） 单位负责人为同一人或者存在直接控股、管理关系的不同投标单位，不得参加同一合同项下的政府采购活动；投标人投标时须提供投标人企业关系关联承诺书。

三、获取招标文件

时间：2022 年 11 月 29 日至 2022 年 12 月 06 日，每天上午 08:00:00 至 11:30:00，下午 13:30:00 至 16:00:00（北京时间）

途径：陕西教育招标有限责任公司业务一部（地址：西安市太白南路 181 号 西部电子社区 A 座 B 区 401）

方式：现场获取

售价：500 元

四、提交投标文件截止时间、开标时间和地点

时间：2022 年 12 月 20 日 14 时 30 分 00 秒（北京时间）

提交投标文件地点：陕西教育招标有限责任公司会议室（西安市雁塔区太白南路 181 号西部电子社区 A 座 B 区 401）

开标地点：陕西教育招标有限责任公司会议室（西安市雁塔区太白南路 181 号西部电子社区 A 座 B 区 401）

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

1.携带有效的单位介绍信、经办人身份证原件、经办人身份证复印件加盖单位公章；售后不退。

2.报名成功投标单位须按照《陕西省财政厅关于政府采购投标单位注册登记有关事项的通知》的要求，通过陕西省政府采购网（http://www.ccgp-shaanxi.gov.cn/）注册登记加入陕西省政府采购投标单位

库。

七、凡对本次采购提出询问，请按以下方式联系。

1.采购人信息

名称：陕西省教育厅财务处

地址：西安市长安南路563号

联系方式：侯老师029-88668695

2.采购代理机构信息

名称：陕西教育招标有限责任公司

地址：西安市太白南路181号西部电子社区A座B区401

联系方式：029-88224929

3.项目联系方式

项目联系人：鲁方方、崔斌、李宝宝、程钰

电话：029-88224929

第二章 投标人须知

一、总则

本次招标依据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》等国家现行有关法律法规执行。

1.采购人、采购代理机构、监督管理机构

1.1 采购人：陕西省教育厅。

1.2 采购代理机构：陕西教育招标有限责任公司。

1.3 招标采购单位：采购人及采购代理机构的统称。

1.4 监督管理机构：陕西省财政厅。

2.合格的投标人

2.1 符合《中华人民共和国政府采购法》第二十二条规定，有能力提供本项目所需服务的投标单位；接受联合体投标。

2.2 投标人在投标文件中须提供以下资格证明文件以便资格审查：

（1）具有独立承担民事责任能力的法人、其他组织或自然人，提供营业执照/事业单位法人证书/非企业专业服务机构执业许可证/自然人身份证。

（2）法定代表人参加投标时，提供法定代表人证明书；授权代表参加投标时，提供法定代表人授权书；非法人单位参照执行。

（3）财务状况报告：提供2021年度的财务报告或提交投标文件截止时间前六个月内银行资信证明；或政府采购信用担保机构出具的投标担保函。

（4）税收缴纳证明：提供投标文件递交截止时间前六个月内至少一个月已缴纳的纳税凭据或完税证明；依法免税的投标人应提供相关文件证明。

（5）社会保障资金缴纳证明：提供投标文件递交截止时间前六个月内已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。

（6）提供具有履行本合同所必需的设备和专业技术能力的承诺。

（7）提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。

（8）单位负责人为同一人或者存在直接控股、管理关系的不同投标单位，不得参

加同一合同项下的政府采购活动；投标人投标时应提供投标人企业关系关联承诺书。

上述资格证明文件第（2）、（6）、（7）、（8）项必须在投标文件正本中附纸质原件，其他资格证明文件必须在投标文件正本中附复印件（或扫描件）并加盖投标人公章（原件备查）。

以上资格要求均为必备资格，资格审查时，缺少其中任何一项或某项达不到投标文件要求的，其响应文件视为无效文件。

2.3 根据《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125 号）的规定，对列入失信被执行人、重大税收非法案例当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的投标单位，拒绝其参与政府采购活动。

查询渠道：“信用中国”（www.creditchina.gov.cn/）；“中国政府采购网”（www.ccgp.gov.cn/）等。

查询截止时间：投标文件递交截止时间后 1 小时。

2.4 投标人必须向采购代理机构购买招标文件并登记备案，任何未从采购代理机构购买招标文件并登记备案的潜在投标人均无资格参加投标。

3.合格的货物和服务

3.1 投标所用货物及服务，均应来自上述第 2 条所规定的合格投标人。

3.2 投标人应按招标文件要求提供符合招标文件货物及服务所需的相关证明文件。

3.3 货物系指投标人按招标文件规定，向采购人提供的符合招标文件要求的相关货物。

3.4 服务系指招标文件规定的，投标人须承担的与投标货物有关的辅助服务,如包装、运输、保险、安装、调试、技术培训、售后服务以及其他类似的义务。

4.投标费用

4.1 投标人应承担所有与准备和参加投标有关的费用。不论投标的结果如何，招标采购单位均无义务和责任承担这些费用。

二、招标文件

5.招标文件构成

5.1 招标文件包括下列内容：

第一章　招标公告

第二章　投标人须知

第三章　商务条款

第四章　合同格式

第五章　合同条款

第六章　附件（投标文件格式）

第七章　服务内容及要求

6.招标文件的澄清

6.1 投标人对招标文件若有澄清要求，应在政府采购法定时间内，以书面形式通知采购代理机构，采购代理机构对投标人的澄清要求均以书面形式予以答复，并将根据澄清要求涉及的范围以书面答复告知相关的每一个购买招标文件的投标人。

7.招标文件的修改

7.1 在投标截止期十五（15）日前，招标采购单位有权根据需求对招标文件进行必要澄清或者修改。更正公告将以书面形式通知所有招标文件收受人，并在陕西省政府采购网上发布。该澄清或者修改的内容为招标文件的组成部分。

7.2 为使投标人准备投标时有充分时间对招标文件的修改部分进行研究，招标采购单位有权适当延长投标截止时限。延期公告将以7.1所述方式通知所有招标文件收受人。

7.3 投标人在收到上述通知后,应在通知规定的时间内向采购代理机构回函确认。

7.4 招标文件的解释权归采购代理机构。

三、投标文件的编制

8.投标文件编制要求

8.1 投标人应认真阅读招标文件的所有内容，严格按照招标文件的要求编制和提供投标文件,并保证所提供的全部资料的真实性,使投标文件对招标文件做出实质性响应。如果投标人在投标文件中没有按照招标文件要求提交必备资料或者投标文件没有对招标文件在各方面都做出实质性响应，其投标文件视为无效文件。

8.2 投标人提交的投标文件以及投标人与采购代理机构就有关投标的所有来往函电均应以中文书写。

9.投标文件构成和格式

9.1 投标人须按招标文件第六章附件（投标文件格式）提供的相应格式及顺序编制投标文件，并编制目录，双面打印，逐页标注连续页码，胶装成册,不得缺少或留空任

何招标文件要求必须填写的表格或提交的资料,否则其投标文件视为无效文件。投标文件书脊处应有项目名称、项目编号、投标人名称（可手写）。

10.投标文件的制作和签署

10.1 投标人应准备 **1 份**投标文件正本、**4 份**副本。每套投标文件须清楚地标明“正本”、“副本”。一旦正本和副本不符，以正本为准。

10.2 投标文件的正本需打印，并由投标人的法定代表人或其授权代表按招标文件要求在投标文件指定的页面落款处加盖公章和签字。投标文件的副本可以采用正本的复印件。

10.3 除投标人对投标文件错处做必要修改外，投标文件不得行间插字、涂改和增删。如有修改，必须由投标人的法定代表人或其授权代表在修改处签字并盖公章后方可视为有效。

10.4 投标文件因表述不清所引起的后果由投标人负责。

11.投标报价

11.1 投标人必须采用本招标文件第六章附件（投标文件格式）中提供的投标报价一览表及分项报价表进行报价。

11.2 投标人必须对本项目招标文件载明的系统建设所有服务要求进行完整报价,招标采购单位拒绝只对部分服务进行报价的投标。投标人应在投标文件的投标分项报价表中标明对本次招标拟提供服务的单价和总价。任何有选择的报价将不予接受。

11.3 投标报价：本项目“报价表”所报价格为本项目涉及的所有内容的一切费用。

11.4 所有根据合同或其它原因应由投标人支付的税款和其它应交纳的费用都要包括在投标人提交的投标报价中。

11.5 招标采购单位要求投标人按投标分项报价表标明拟提供服务的报价构成和总价，只是为了方便对投标文件进行比较，但在任何情况下并不限制采购人以上述任何条件订立合同的权力。

11.6 投标人所报的投标价在合同执行过程中是固定不变的，不得以任何理由予以变更。任何包含价格调整要求的投标，将被认为是非响应性投标而予以拒绝。

11.7 最低报价不是中标的唯一依据。

11.8 投标人不得以低于成本的报价参加投标。评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响服务质量或者不能诚信履约的，可要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会可将其作为无效投标处理。

11.9 凡因对招标文件阅读不深、理解不透、误解、疏漏或因对市场行情了解不清而造成的后果和风险均由投标人自负。

11.10 报价精确到元，投标人提供的服务一律以人民币报价。

12.投标保证金

12.1 投标保证金金额：**人民币陆万元（60000.00 元）。**

12.2 投标保证金必须按招标文件规定的数额全额交纳，投标保证金应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交，投标人可以任选其一：

（1）采用支票、汇票、本票、银行转账等非现金形式交纳。交纳的保证金必须从投标人的账户转出，并备注项目编号，投标保证金必须在提交投标文件截止时间前到账。

保证金交纳账户：

开户行：浙商银行西安长安路支行

开户名称：陕西教育招标有限责任公司

银行行号：316791000065

开户账号：7910000410120100071552

财务电话：029-88224928

（2）金融机构、担保机构投标担保方式。须在提交投标文件截止时间前将《政府采购投标担保函》正本递交至采购代理机构。

12.3 凡没有根据第 12.1 条、第 12.2 条规定提交投标保证金的投标，将被视为无效投标。

12.4 投标保证金退还

（1）投标人在投标截止时间前撤回已提交的投标文件的，代购代理机构将在收到投标人撤回通知之日起五个工作日内退还至投标人的银行账户。

（2）未中标人的投标保证金，采购代理机构将在对中标人发出《中标通知书》后五个工作日内退还至投标人的银行账户。

（3）中标人的投标保证金，将在中标人与采购人签订供货合同，中标人持《保证金退还申请书》（格式详见本章“八、保证金退还申请书”）随合同送至采购代理机构备案后，五个工作日内退还至中标人的银行账户。

（4）若招标终止，采购代理机构将在发布招标终止公告后五个工作日内退还投标保证金。

12.5 投标人若要办理发票相关事宜，请在开标之日起 2 个月内办理，逾期不再办理。

12.6 投标人发生下列情况之一时，其投标保证金将不予退还：

（1）在投标有效期内，投标人撤回其投标的；

（2）中标后不按本须知规定交纳招标代理服务费的；

（3）中标后不按本须知规定签订供货合同的；

（4）符合本招标文件规定的其他不予退还条件的。

13.投标有效期

13.1 投标有效期为开标之日起九十（90）个日历日（中标人的投标文件有效期与合同有效期一致）。投标人的投标有效期不足招标文件规定的将被视为非响应性投标而予以拒绝。

13.2 从投标截止期始至招标文件确定的投标有效期期满这段时间内，投标人不得撤回其投标，否则其投标保证金将不予退还。

四、投标文件的密封和递交

14.投标文件的密封和标记

14.1 为方便开标唱标，投标人应将“开标一览表（报价表）”单独密封递交，并在封面上标明“开标一览表（报价表）”字样。同时应保证投标文件正、副本中仍有“开标一览表（报价表）”，且与唱标的“开标一览表（报价表）”一致。当出现不一致的情况时，以唱标内容为准。

14.2 投标人应将投标文件正本、所有的副本密封。

14.3 密封与标记要求

(1) 标记要求：标明招标项目名称、项目编号、投标人全称等内容。

(2) 密封要求：加封条密封，密封条加盖投标人公章。

14.4 如果投标文件未按要求密封，采购代理机构将拒绝接收。

15.投标截止时间

15.1 投标人应在不迟于“招标公告”中规定的投标截止时间，在开标地点将投标文件递交至采购代理机构。

15.2 采购代理机构可以按本须知第 7 条规定，通知因修改招标文件而适当延长投标截止时间。在此情况下，招标采购单位和投标人受投标截止时间制约的所有权利和义务均应延长至新的截止时间。

15.3 采购代理机构拒绝接收投标截止时间后送达的任何投标文件。

五、开标与评标

16.开标

16.1 招标采购单位将在“招标公告”规定的时间和地点组织开标大会。开标大会邀请所有投标人派代表参加。

16.2 开标时，由大会主持人现场宣读开标工作纪律；投标人或者其推选的代表检查投标文件的密封情况，经确认无误后，由采购代理机构工作人员当众拆封。

16.3 拆封后，采购代理机构公开宣读投标人“开标一览表（报价表）”中的内容，“开标一览表（报价表）”规定内容以外的文字、数据等不予宣读。

16.4 采购代理机构将在开标大会现场做开标记录，开标记录包括按本须知第16.3条规定的在开标时宣读的全部内容。唱标结束后，各投标人的授权代表必须审核开标记录，无误后签字确认。

17.投标人资格审查

17.1 开标结束后，采购人和代理机构将根据招标文件要求对各投标人资格（含信用记录）进行审查，资格审查未通过的投标人其投标将被拒绝。

18.评标

18.1 评标委员会

18.1.1 采购代理机构将按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条列》、《政府采购货物和服务招标投标管理办法》等有关规定组建评标委员会。

18.1.2 评标委员会由采购人代表及有关经济、技术等方面的专家组成。专家评委从政府采购专家库中随机抽取产生。

18.1.3 评标委员会负责评标工作，对投标文件进行符合性审查（商务、技术审查和评估），并向招标采购单位提交书面评审意见。

18.2 评标过程的保密性

18.2.1 开标后，直至发布中标公告时止，凡与审查、澄清、评价和比较投标的有关资料以及授标意见等，均属保密范围，评标委员会及招标工作人员不得向投标人及与评标无关的其他人透露。除本须知第18.3.1条规定的情形外，从开标之日起，直至授予合同期间，投标人不得就与其投标有关的事项与采购人、采购代理机构和评标委员会成员私下接触。

18.2.2 在评标过程中，如果投标人试图在投标文件的审查、澄清、比较及授予合

同方面向评标委员会或招标采购单位施加任何影响，其投标将被拒绝。

18.3 投标文件的澄清

18.3.1 评标期间，为有助于对投标文件的审查、比较和评价，评标委员会可要求投标人对其投标文件进行澄清或说明，有关澄清或说明的要求和答复应以书面形式递交。要求澄清和说明的内容及其答复不得超出投标文件的范围或改变投标文件实质性内容。

18.4 投标文件的初审（符合性检查）

18.4.1 符合性审查：评标委员会将审查投标文件签署是否合格、是否实质上响应了招标文件的要求。

18.4.2 评标委员会将审查每份投标文件是否实质上响应了招标文件的要求。实质上响应的投标应该是与招标文件要求的全部条款、条件和规格相符，没有重大偏离或保留的投标。对关键条文的偏离、保留或反对将被认为是实质上的偏离。重大偏离或保留是指实质上影响供货范围、质量和性能；或者实质上与招标文件不一致，而且限制了采购人的权利或投标人的义务。纠正这些偏离或保留将会对其他实质上响应要求的投标人的竞争地位产生不公正的影响。对于投标文件中不构成实质性偏差的不正规、不一致或不规则，招标采购单位可以接受，但这种接受将影响投标人的综合得分。评标委员会只根据投标文件本身的内容确定投标文件的响应性，而不寻求外部的证据。

18.4.3 如果投标文件实质上没有响应招标文件的要求，评标委员会将予以拒绝，投标人不得通过修正或撤销不合要求的偏离从而使其投标成为实质上响应的投标。

18.4.4 如发现下列情况之一的，其投标无效：

（1）提供的必备资格证明文件不全、无效或达不到招标文件规定要求的；

（2）投标人未按照招标文件要求提交投标保证金的；

（3）投标文件未按照招标文件要求的格式编制的；

（4）投标文件中应签字盖章处未按招标文件要求盖章或签字的；无法定代表人签字或签字人无法定代表人有效授权书的；

（5）投标有效期不足的；

（6）投标报价低于成本或高于招标文件公布的采购预算的；

（7）不满足第三章 商务条款的；

（8）投标分项报价表出现漏项；

（9）投标人在同一份投标文件中,对同一服务有两个或多个报价的；

（10）投标文件附有招标采购单位不能接受的条件的；

（11）投标人不接受18.4.6条规定的；

（12）投标人在政府采购或其它重大项目履约过程中有不良记录，且造成重大影响的；

（13）投标人提供虚假证明，开具虚假业绩，除按无效标处理外，还将按照政府采购法有关规定进行相应处罚；

（14）符合招标文件中其他有关拒绝投标或无效投标文件条款的。

18.4.5 评标委员会将只对确定为实质上响应的投标文件进行审核，查看其是否有计算上和累加上的算术错误，修正错误的原则如下：

（1）单独密封的开标一览表（报价表）内容与投标文件正本内容不一致的，以单独密封的开标一览表（报价表）为准；

（2）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

（3）大写金额和小写金额不一致的，以大写金额为准；

（4）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

（5）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

18.4.6 同时出现两种以上不一致的，按照前款第 18.4.5 条规定的顺序修正。修正后的报价按照前款第 18.3.1 条的规定经投标人确认后产生约束力，投标人不确认的，其投标无效。

18.5 投标文件的详细评审

18.5.1 评标委员会将按照本须知第 18.4 条要求，只对确定为实质上响应招标文件要求的投标文件进行详细评审。

18.5.2 政府采购政策评审依据：

依据国家政府采购相关政策，对符合《政府采购促进中小企业发展暂行办法》（财库〔2020〕46 号）规定的小微企业报价给予 10%的扣除，用扣除后的价格参与评审。监狱企业、福利企业等参照小微企业执行。（投标人须根据本项目招标公告所列政府采购政策文件，提供相对应的声明文件（或证明材料），出具者在评审时予以考虑，未出具者不予考虑。）

18.5.3 评标办法：综合评分法

（1）对于投标文件中不构成实质性偏差的不正规、不一致或不规则内容，评标委员会可以接受，但这种接受将影响投标人的综合得分。

（2）评价和比较以招标文件为依据，对所有实质上响应的投标按下述“评分细则”

进行综合评分。

赋分项	赋分标准		满分
价格评审（满分 10 分）	评分方法：P=10*Pmin/ Pn 其中：Pmin：所有有效投标的最低投标报价。 Pn：第 n 个投标人的投标报价。 计算分数时四舍五入取小数点后两位。 评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。		10
服务方案（满分 80 分）	备份系统与备份服务	根据投标单位提供的服务方案是否完整、科学、合理赋分： 方案科学、合理，且完全满足服务需求的，得 17-10 分；方案基本满足服务需求的，但存在瑕疵的，得 9-0 分。	17
	咨询服务	根据投标单位提供的服务方案是否完整、科学、合理赋分： 方案科学、合理，且完全满足服务需求的，得 11-6 分；方案基本满足服务需求的，但存在瑕疵的，得 5-0 分。	11
	等级保护服务	根据投标单位提供的服务方案是否完整、科学、合理赋分： 方案科学、合理，且完全满足服务需求的，得 17-9 分；方案基本满足服务需求的，但存在瑕疵的，得 8-0 分。	17
	密码应用服务	根据投标单位提供的服务方案是否完整、科学、合理赋分： 方案科学、合理，且完全满足服务需求的，得 10-6 分；方案基本满足服务需求的，但存在瑕疵的，得 5-0 分。	10
	项目管理服务	根据投标单位提供的服务方案是否完整、科学、合理赋分： 方案科学、合理，且完全满足服务需求的，得 15-8 分；方案基本满足服务需求的，但存在瑕疵的，得 7-0 分。	15
	人员团队	投标人提供项目团队配置方案及团队人员的职称、专业证书证件等赋分： 人员配置满足项目需求，分工合理，可确保项目顺利完成，得 5-1 分。未提供 0 分；	10

		投标人团队人员的职称证书证件等情况赋分，5-0 分；（提供相关证明材料，未提供或提供不予认可的不得分）。	
履约能力（满分 10 分）	业绩	根据投标人提供近五年与本项目有关的省级类似项目业绩,以合同为准，由评委按份数赋分，每份 2 分，满分 10 分。	10

19.推荐中标候选投标人名单

19.1 评标委员会对进入详细评审的投标人进行综合评分，根据得分由高到低进行排序，并推荐排序第一的投标人承担供货任务，如果综合评分出现二个投标人得分相同的情况，按下列顺序排列：

（1）投标价格低的；

（2）技术评审得分高的。

20.编写评标报告

20.1 评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告，采购代理机构将评审结果报送采购人审核，采购人根据评标报告中评标委员会的中标候选单位推荐顺序确定中标人。

六、授予合同

21.中标通知书

21.1 采购代理机构接到采购人的中标确认函后，将中标结果在陕西省政府采购网上进行公告。向中标人发出中标通知书。

21.2 中标通知书是合同的组成部分。

21.3 未中标人的评审情况，采购代理机构将以电子邮件形式告知。

22.授予合同

22.1 采购代理机构将在中标通知书发出之日起三十（30）个日历日内，组织采购人与中标人签订合同。

23. 招标代理服务费

23.1 中标人在收到中标通知书后十(10)个日历日内，按照原国家计委《招标代理服务收费管理暂行办法》(计价格[2002]1980 号)及发改办价格[2003]857 号文件规定的收费标准，向陕西教育招标有限责任公司交纳招标代理服务费,招标代理服务费采用现金、

电汇或银行转账方式交纳，不得采用投标保证金抵扣。

服务费交纳账户：

开户行：中国光大银行陕西自贸试验区西安唐延路支行；

开户名称：陕西教育招标有限责任公司；

银行行号：303791000136

开户账号：78580188000058925

财务电话：029-88224928

23.2 中标人应在交纳采购代理服务费后 2 个月内领取服务费发票，逾期不再办理。

七、其他

24.其他

24.1 开标后，如果发生有效投标人不足三家，本项目废标。

24.2 如果中标人没有按照上述第 22.2 条或第 23.1 条规定执行，招标采购单位将有充分理由取消该中标决定。在此情况下，招标采购单位可将合同授予评标排序下一名的投标人，或重新招标。

24.3 拒绝商业贿赂

24.3.1 政府采购中的采购人、采购代理机构、投标人和评标专家都要签订相应的《拒绝商业贿赂承诺书》，并对违反承诺的行为承担全部责任。

24.3.2 投标人必须按招标文件要求填写一份拒绝政府采购领域商业贿赂承诺书（格式见第六章 附件）原件编制在投标文件正本中，否则其投标文件视为无效文件。

25.质疑、投诉

25.1 投标人认为招标文件、招标过程和中标结果使自己的权益受到损害的，可在法定时间内，按照政府采购质疑和投诉办法（财政部令第 94 号）一次性针对同一采购程序环节向招标代理机构提出质疑，联系方式：

接收质疑函的方式：书面形式

联系单位：陕西教育招标有限责任公司

联系人：鲁方方

联系电话：029-88224929

通讯地址：西安市太白南路 181 号 西部电子社区 A 座 B 区 401

25.2 投标人对采购代理机构的答复不满意，或采购代理机构未在规定的期限作出答复的，可在法定时间内，按照政府采购质疑和投诉办法（财政部令第 94 号）向采购人

同级财政部门提出投诉。

26.融资

26.1 中标人有融资需求的，可参照《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23 号）执行。

27.履约保证金

成交单位在与采购人签订合同后五日内，应向采购人指定账户提交履约保证金，保证金额为成交总金额的百分之十（10%）。履约保证金在终验合格后无息退还。履约保证金退还后，成交人承诺的服务仍须按原有承诺承担相关义务，否则采购人将追究成交人的相关法律责任。

八、保证金退还申请书

陕西教育招标有限责任公司保证金退还申请书（模板）

陕西教育招标有限责任公司：

我单位_____（中标/成交投标人名称）_____，是_____（项目名称、项目编号）_____中标/成交单位，目前已与采购人完成合同签署，现特此申请退还该项目投标保证金。

投标人名称：_____

开户银行：_____

账　　号：_____

附：经济合同_____份

申请单位（公章/财务章）：

申请日期：

第三章　商务条款

1.交货期及地点：

1.1 交货（完工）时间：合同签署后，按照省教育厅工作安排完成相关工作。

1.2 交货（完工）地点：采购人指定地点。

2.验收

2.1 初验：按照省教育厅工作安排，交付采购人后进行初验。检查合格的视为初验合格，收货单位签发“初验合格单”。

2.2 终验：初验合格后 30 天可进行终验，终验合格后，采购人签发“终验合格单”。

2.3 若验收不合格的，中标人必须在接到通知后 5 个日历日内保证所开发系统的正常运行。验收过程中，若发现严重质量问题，且在规定时间内整改无效，采购人将进行严肃处理，并将其列入“不良行为记录名单”。

2.4 验收依据

合同文本，招标文件，投标文件，国内相应的标准、规范。

3.款项结算

3.1 款项结算：

（1）合同签订后，支付合同总额 40％货款；

（2）终验合格后，投标单位持“终验合格单”办理支付合同总额 60％货款的手续。

3.2 货款支付时，中标单位须按采购方要求提供正式发票等付款所需的材料。

3.3 货款支付单位为：陕西省教育厅。

发票开具的“购货单位（人）名称”为：采购人指定名称。

4.实施要求

4.1 投标人应结合项目研究、开发、实施、测试、验收的相关标准的要求，提供详细的项目技术研究、软件开发以及工程的实施方案。项目实施方案中应包括详细工作流程图、工程计划等。

4.2 投标人应设置合理可行的团队人员，并为此安排具有较高专业水平、认真负责的技术骨干和项目管理人员，以确保工程按期、按质完成。

4.3 投标人应负责所有系统软件的安装、部署以及整体平台联调和运行期间的

改进、保障工作。

5.质量保证

5.1 质量保证期从终验合格之日起计算。

5.2 质量保证要求：

5.2.1 系统的质保期为验收合格后不少于 36 个月。投标人承诺的质保期超过以上规定时间的，按其承诺时间质保。

5.2.2 投标人应承诺在质量保证期内免费提供系统维护、软件升级换代等服务；质量保证期后以优惠价提供上述服务。

5.2.3 投标人应保证所提供的产品，在现有 Internet 网络及专有网络条件达到产品要求条件下均应可靠运行，否则由此引起的一切费用、产品及后果由中标单位承担。

5.2.4 投标人应在系统开发建设及质保期内，因采购单位业务需求发生变化时，无条件配合做好变更梳理和系统调整优化，确保系统满足业务变化需求。

5.3 质量保证期技术服务:

5.3.1 质量保证期内，应常驻 2 人在用户现场，负责对运行中可能出现的故障进行处理。

5.3.2 运行中出现故障时，在收到通知后的 24 小时内，通过上门服务、远程支持、电话/传真支持等方式，解决故障。

6.售后服务

6.1 中标人的责任包括从项目开发到整个系统的交付使用和维护。

6.2 中标人必须对中标产品提供质保期内的免费修改、维护服务。

6.3 中标人必须提供所开发软件数据库模型说明，并提供系统安装及部署说明、系统操作说明、系统维护说明、程序模块调用关系说明、程序运行流程说明等技术文档。

6.4 中标人应提供数据库和系统超级用户密码，采购人管理员可对其进行修改。中标人应按照采购人要求对数据库关键字段进行校验位加密、对数据库对象单元（函数、程序包等）和后台软件加密，并提供加密解密算法。

6.5 中标人必须提供本地化服务支持，售后服务与技术支持至少应包含：电话支持、远程维护、现场服务三种方式；在接到采购人维护要求后应立即做出回应，并在 24 小时内指导维护。

6.6 承诺提供长期技术服务的，需在售后服务方案中明确售后服务方式、计费标准；若质量保证期内技术标准、规程发生变更，中标人须提供系统的免费升级服务。

6.7 在项目质保期后，如果因国家标准改变，中标人应该根据国家标准进行必要的调整。

6.8 若出现因软件缺陷所引发的系统故障，采购人有权要求中标人及时免费维护并做相应的处理。

6.9 质保期内中标人免费为采购人提供项目的日常管理和应用操作等有关内容的培训。

6.9.1 方案应对培训的时间、地点、人员、培训内容、培训机制等进行说明，培训内容包含该项目的每一个功能点，参训人员必须熟练掌握该软件的使用及基本维护方法。

6.9.2 培训方案还应包括维保期内升级改造后的再培训。

7.知识产权

7.1 中标人应保证投标产品及服务不会出现因第三方提出侵犯其专利权、商标权或其它知识产权而引发法律或经济纠纷，否则由中标人承担全部责任。

7.2 任何被中标人用于未经授权的商业目的行为所造成的违约或侵权责任由中标人承但。

7.3 根据采购人需求开发的信息系统，其知识产权归采购人所有，中标人如需在产权局进行备案或进行二次销售，必须获得采购人的书面许可。

8.违约责任

8.1 按《中华人民共和国民法典》中的相关条款执行。

8.2 未按合同要求提供产品或服务质量不能满足技术要求，采购人有权终止（或解除）合同，并对中标人违约行为进行追究。

8.3 如果中标人在合同履行过程中有违约行为的，应按照以下约定向采购人承担违约责任：

(1)中标人不能按期完成合同成果的，每逾期一周（7天）按照合同总金额的1 %向采购人承担违约责任，逾期 30 日以上的，采购人有权随时解除合同；合同解除后，采购人不再向中标人支付任何合同价款，采购人已经支付的合同价款，中标人应予以退还。

(2) 中标人未按照合同约定履行合同义务或有其他违约情形的，中标人应按照合同总金额的20%向采购人承担违约责任。

第四章　合同格式

合 同

“‘陕西智慧教育综合服务平台’ 工程服务项目”（项目编号：SNJZ-2022-　），在陕西省财政厅的全程监督管理下，由陕西教育招标有限责任公司组织招标采购。经评标委员会评审推荐，　（采购人）　(以下简称“甲方”)确定　中标单位名称　（以下简称“乙方”）为本项目中标单位。

依据《中华人民共和国民法典》和《中华人民共和国政府采购法》，经双方协商，于　年　月　日按下述条款和条件签署本合同。

甲方通过公开招标方式采购，接受了乙方以总金额　大写（￥　）　(以下简称“合同价”)提供合同条款附件所述的服务。

本合同在此声明如下：

1.本合同中的词语和术语的含义与合同条款中定义的相同。

2.下述文件是本合同的一部分，并与本合同一起阅读和解释：

⑴ 合同通用条款；

⑵ 合同条款附件；

⑶ 中标通知书；

⑷ 招标文件；

⑸ 投标文件。

3.考虑到甲方将按照本合同向乙方支付合同款，乙方在此保证全部按照合同的规定向买方提供产品和服务，并修补缺陷。

4.考虑到乙方将按照本合同向甲方提供产品和服务并修补缺陷，甲方在此保证按照合同规定的时间和方式向乙方支付合同价或其他按合同规定应支付的资金。

5.本合同一式　份，其中，买方　份，卖方　份，招标代理　份。

甲方名称:	乙方名称:
甲方地址:	乙方地址:
电　　话:	电　　话:
传　　真:	传　　真:
邮　　编:	邮　　编:
	开户银行:
	帐　　号:
甲方代表签字:	乙方代表签字:
甲 方 盖 章:	乙 方 盖 章:

第五章　合同草案条款

1.定义

本合同下列术语应解释为：

(1)“合同”系指甲乙双方签署的、合同格式中载明的甲乙双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

(2)“合同价”系指根据合同规定乙方在正确地完全履行合同义务后甲方应支付给乙方的价格。

(3)“服务”系指乙方根据合同规定须向甲方提供的服务。

(4)“服务地点”系指本合同项下服务场地。

(5)“天”指日历天数。

2.适用性

2.1 本合同条款适用于没有被本项目招标文件规定条款、投标文件承诺条款所取代的范围。

3.标准

3.1 本合同下提供的服务应符合招标文件技术规格与要求所述的标准。如果没有提及适用标准，则应符合中华人民共和国有关机构发布的最新版本的标准。

4. 验收

按招标文件第三章相关内容执行。

5.履约保证金

乙方在与甲方签订合同后五日内，应向甲方指定账户提交履约保证金，保证金额为成交总金额的百分之十（10%）。履约保证金在终验合格后无息退还。

6.质量保证

6.1 质量保证期从终验合格之日起计算。

6.2 质量保证要求：

6.2.1 系统的质保期为验收合格后　　个月。

6.2.2 乙方承诺在质量保证期内免费提供系统维护、软件升级换代等服务；质量保证期后以优惠价提供上述服务。

6.2.3 乙方保证所提供的产品，在现有 Internet 网络及专有网络条件达到产品要求条件下均应可靠运行，否则由此引起的一切费用、产品及后果由乙方承担。

6.2.4 乙方应在系统开发建设及质保期内，因甲方业务需求发生变化时，无条件配合做好变更梳理和系统调整优化，确保系统满足业务变化需求。

6.3 质量保证期技术服务:

6.3.1 质量保证期内，应常驻 2 人在用户现场，负责对运行中可能出现的故障进行处理。

6.3.2 运行中出现故障时，在收到通知后的 24 小时内，通过上门服务、远程支持、电话/传真支持等方式，解决故障。

7.款项结算

7.1 按招标文件第三章相关内容执行。

8.转让

8.1 未经甲方事先书面同意，乙方不得部分转让或全部转让其应履行的合同义务。

9.乙方履约延误

9.1 乙方应按照本项目招标文件中规定的服务期提供产品及服务。

9.2 在履行合同过程中，如果乙方遇到妨碍提供产品及服务的情况时，应及时以书面形式将拖延的事实、可能拖延的时间和原因通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意，以及是否收取误期赔偿费。延期应通过修改合同的方式由双方认可。

10.违约责任

10.1 如果乙方在合同履行过程中有违约行为的，应按照以下约定向甲方承担违约责任：

(1) 中标人不能按期完成合同成果的，每逾期一周（7天）按照合同总金额的 1 %向采购人承担违约责任，逾期 30 日以上的，采购人有权随时解除合同；合同解除后，采购人不再向中标人支付任何合同价款，采购人已经支付的合同价款，中标人应予以退还。

(2) 中标人未按照合同约定履行合同义务或有其他违约情形的，中标人应按照合同总金额的20%向采购人承担违约责任。

11.违约终止合同

11.1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可向乙方

发出书面违约通知书，提出终止部分或全部合同：

⑴ 如果乙方未能在合同规定的期限内或甲方根据合同条款第8.2条的规定同意延长的期限内提供服务。

⑵ 如果乙方未能履行合同规定的其它任何义务。

⑶ 如果甲方认为乙方在本合同的竞争和实施过程中有腐败和欺诈行为。为此目的，定义下述条件：

“腐败行为”是指提供、给予、接受或索取任何有价值的物品来影响甲方在采购过程或合同实施过程中的行为。

“欺诈行为”是指为了影响采购过程或合同实施过程而谎报或隐瞒事实，损害甲方利益的行为。

11.2 如果甲方根据上述第11.1条的规定，终止了全部或部分合同，甲方可以依其认为适当的条件和方法购买类似的服务，乙方应承担甲方因购买类似服务而产生的额外支出。但是，乙方应继续执行合同中未终止的部分。

12.不可抗力

12.1 签约双方任何一方由于不可抗力事件的影响而不能执行合同时，履行合同的期限应予延长，其延长的期限应相当于事件所影响的时间。不可抗力事件系指甲乙双方在缔结合同时所不能预见的，并且它的发生及其后果是无法避免和无法克服的事件，诸如战争、严重火灾、洪水、台风、地震等。

12.2 受影响一方应在不可抗力事件发生后尽快用书面形式通知对方，并于不可抗力事件发生后十四（14）天内将有关当局出具的证明文件用特快专递或挂号信寄给对方审阅确认。一旦不可抗力事件的影响持续一百二十天（120）天以上，双方应通过友好协商在合理的时间内达成进一步履行合同的协议。

12.3 因合同一方迟延履行合同后发生不可抗力的，不能免除迟延履行方的相应责任。

13.因破产而终止合同

13.1 如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方，提出终止合同而不给乙方补偿。该合同的终止将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权力。

14.因甲方的便利而终止合同

14.1 甲方可在任何时候出于自身的便利向乙方发出书面通知全部或部分终止合同，

终止通知应明确该终止合同是出于甲方的便利，并明确合同终止的程度，以及终止的生效日期。

14.2 对乙方收到终止通知后三十（30）天内完成的服务，甲方应按原合同价格和条款予以接收，对于剩下的产品及服务，甲方可：

⑴ 仅对部分产品及服务按照原来的合同价格和条款予以接受；

⑵ 取消对所剩产品及服务的采购，并按双方商定的金额向乙方支付部分完成服务的费用。

15.争议的解决

15.1 因执行本合同所发生的或与本合同有关的一切争议,双方应通过友好协商解决，协商不成的，任何一方均可向甲方所在地的人民法院提起诉讼。

16.适用法律

16.1 本合同应按照中华人民共和国的现行法律进行解释。

17.通知

17.1 本合同一方给对方的通知应用书面形式送到合同专用条款中规定的对方的地址。传真要经书面确认。

17.2 通知以送到日期或通知书的生效日期为生效日期，两者中以晚的一个日期为准。

18.税款

18.1 按照中华人民共和国税法和有关部门的规定，甲方需交纳的与本合同有关的一切税费均应由甲方负担。

18.2 按照中华人民共和国税法和有关部门的规定，乙方需交纳的与本合同有关的一切税费均应由乙方负担。

19.合同生效

19.1 本合同应在甲乙双方共同签字并加盖公章后生效。

第六章 附件（投标文件格式）

投标人应认真阅读招标文件中所有内容，按照招标文件的要求编制和提供投标文件，并保证所提供的全部资料的真实性，使投标文件对招标文件作出实质性响应。

投标人编写投标文件时，请按本章节提供的相应格式及顺序编排。并应编制目录，逐页标注连续页码，胶装成册,不得缺少或留空任何招标文件要求填写的表格或提交的资料。

投标文件书脊处应有项目名称、项目编号、投标人名称（可手写）。

（正本或副本）

项目编号：SNJZ-2022-

“陕西智慧教育综合服务平台”
工程服务项目

投 标 文 件

投标单位：_____（公章）

时　间：　年　月　日

1.投标函（格式）

投 标 函

致：陕西教育招标有限责任公司

根据贵方为“陕西智慧教育综合服务平台”工程服务项目的招标公告SNJZ-2022- ，签字代表（姓名、职务）经正式授权并代表投标人（投标人名称、地址），提交投标文件正本 1 份、副本 4 份。

在此，签字代表宣布同意如下：

1.若中标，我方将按招标文件的规定履行合同责任和义务。

2.我方已详细审查全部招标文件，完全理解并同意放弃对这方面有不明及误解的权力。

3.本投标有效期为自开标日起___个日历日（若中标，投标文件有效期与合同有效期一致）。

4.我方完全理解并同意招标文件中有关不予退还投标保证金和拒绝投标的条款。

5.我方同意提供按照贵方可能要求的与其投标有关的一切数据或资料，完全理解贵方不一定接受最低投标报价的投标或收到的任何投标。

6.若我方获得中标资格，我方保证按有关规定向贵方支付招标代理服务费。

7.与本投标有关的一切正式往来信函请寄：

投标人名称（公章）：_____

详　细　地　址：_____

邮　政　编　码：_____

电　　话：_____

传　　真：_____

电子邮件地址：_____

开　户　银　行：_____

帐　　号：_____

投标人代表签名：_____

电　　话：_____

传　　真：_____

手　　机：_____

年　　月　　日

2.开标一览表（报价表）（格式）

开标一览表（报价表）

投标人名称：_____ 项目编号：SNJZ-2022-188

总 报 价	完工期	质保期
￥：		
（大写）		

注：1.本表价格应按投标总价填写，须单独密封随投标文件一同提交。同时应保证投标文件的正、副本中仍有此表且一致。
2.投标报价精确到元。

投标人代表签字：_____（投标人公章） 日期：_____

3.投标分项报价表（格式）

投标分项报价表

投标人名称：_____ 项目编号：SNJZ-2022- 188

序号	内容	数 量	单价（人民币/元）	金额（人民币/元）	备 注
1					
2					
3					
4					
5	税费				
6	其他				
…	…				
总 计（人民币/元）		（大 写）			￥：

注：①按货物需求与技术要求中填写本表。投标分项报价表之和须与报价一览表金额一致。

②该表可扩展。

③如果不提供详细分项报价将视为没有实质性响应招标文件。

投标人代表签字：_____（投标人公章） 日 期：_____

4.4.资格证明文件

4-1 具有独立承担民事责任能力的法人、其他组织或自然人，提供营业执照/事业单位法人证书/非企业专业服务机构执业许可证/自然人身份证。（复印或扫描件加盖公章）

4-2 法定代表人参加投标时，提供法定代表人证明书；授权代表参加投标时，提供法定代表人授权书；非法人单位参照执行。（原件编制在投标文件正本中）

4-3 财务状况报告：提供经审计的 2021 年度的财务报告或提交投标截止时间前六个月内银行资信证明；或政府采购信用担保机构出具的投标担保函。（复印或扫描件加盖公章）

4-4 税收缴纳证明：提供投标提交截止时间前六个月内至少一个月已缴纳的纳税凭据或完税证明；依法免税的投标单位应提供相关文件证明。（复印或扫描件加盖公章）

4-5 社会保障资金缴纳证明：提供投标提交截止时间前六个月内已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。（复印或扫描件加盖公章）

4-6 提供具有履行本合同所必需的设备和专业技术能力的承诺。（原件编制在投标文件正本中）

4-7 提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。（原件编制在投标文件正本中）

4-8 单位负责人为同一人或存在直接控股、管理关系的不同单位，不得同时参加本项目，未对本采购项目提供过整体设计、规范编制或者项目管理、监理、检测等服务的投标单位，提供企业关联关系承诺书。（原件编制在投标文件正本中）

4-9 投标人拒绝政府采购领域商业贿赂承诺书。（原件编制在投标文件正本中）

4-2-1 法定代表人证明书（格式，原件编制在投标文件正本中）

法定代表人证明书

<table>
<tr><td colspan="5">致：</td></tr>
<tr><td rowspan="6">企
业
法
人</td><td>企业名称</td><td colspan="3"></td></tr>
<tr><td>地址</td><td colspan="3"></td></tr>
<tr><td>邮政编码</td><td colspan="3"></td></tr>
<tr><td>工商登记机关</td><td colspan="3"></td></tr>
<tr><td>税务登记机关</td><td colspan="3"></td></tr>
<tr><td>统一社会信用代码</td><td colspan="3"></td></tr>
<tr><td rowspan="3">法定代表人</td><td>姓名</td><td></td><td>性别</td><td></td></tr>
<tr><td>职务</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td colspan="3"></td></tr>
<tr><td rowspan="2">法定代表人身份证复印件</td><td colspan="2" rowspan="2">（粘贴处）</td><td colspan="2">法定代表人（签字或盖章）</td></tr>
<tr><td colspan="2">（投标单位公章）

年　月　日</td></tr>
</table>

注：法人投标时提供。

4-2-2 法定代表人授权书（格式，原件编制在投标文件正本中）

法定代表人授权书

本授权书声明：注册于中华人民共和国的_____（投标人名称）_____的在下面签字的_____（法定代表人姓名、职务）_____代表本公司授权的在下面签字的_____（被授权人的姓名、职务）_____为本公司的合法代理人，就项目编号为（项目编号）的_____(项目名称)_____的投标，以本公司名义处理一切与之有关的事务。

本授权书于_____年_____月_____日签字生效，特此声明。

法定代表人签字或签章：　　被授权人签字：

公　　章：　　职　　务：

附：法定代表人、被授权人身份证复印或扫描件。

法人代表身份证	被授权人身份证

4-6 提供具有履行本合同所必需的设备和专业技术能力的承诺。（原件编制在投标文件正本中）

承诺函

项目名称：_____

项目编号：_____

致：陕西教育招标有限责任公司

_____（投标人名称）_____郑重声明，我公司具有履行合同所必需的设备和专业技术能力，在合同签订前后随时愿意提供相关证明材料，符合法律法规规定的资格条件。我方对以上声明负全部法律责任。

特此声明。

投标人名称：_____(投标人公章)

投标人代表：_____(签字)

地　　址：_____

邮　　编：_____

电　　话：_____

日　　期：_____

4-7 提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明（格式，原件编制在投标文件正本中）

声　明

项目名称：_____

项目编号：_____

致：陕西教育招标有限责任公司

_____（投标人名称）_____郑重声明，我公司在参加本项目采购活动前三年内无重大违法活动记录，符合法律法规规定的资格条件。我方对以上声明负全部法律责任。

特此声明。

投标人名称：_____(投标人公章)

投标人代表：_____(签字)

地　　址：_____

邮　　编：_____

电　　话：_____

日　　期：_____

4-8 单位负责人为同一人或存在直接控股、管理关系的不同单位，不得同时参加本项目，未对本采购项目提供过整体设计、规范编制或者项目管理、监理、检测等服务的投标单位，提供企业关联关系承诺书。(格式，原件编制在响应文件正本中)

投标单位企业关系关联承诺书

一、我单位在本项目投标过程中，不存在与其它投标人负责人为同一人，有控股、管理等关联关系承诺。

1.管理关系说明：

我单位管理的具有独立法人的下属单位：_____(没有填无)。

我单位的上级管理单位 _____ (没有填无)。

2.股权关系说明：

我单位控股的单位_____(没有填无) 。

我单位_____(没有填无)被____（控股单位全称）___单位控股。

3.单位负责人：_____ (没有填无)。

4.其他与本项目有关的利害关系说明。_____ (没有填无)。

二、我单位_____（是或否） 为本采购项目提供过整体设计、规范编制或者项目管理、监理、检测等服务的投标单位。

我单位承诺以上说明真实有效，无虚假内容或隐瞒。

投标人名称：_____（投标人公章）

投标人代表签字：_____

日　　期：

4-9.投标人拒绝政府采购领域商业贿赂承诺书

陕西省政府采购投标人
拒绝政府采购领域商业贿赂承诺书

为响应党中央、国务院关于治理政府采购领域商业贿赂行为的号召，我单位在此庄严承诺：

1.在参与政府采购活动中遵纪守法、诚信经营、公平竞标。

2.不向政府采购人、采购代理机构和政府采购评审专家进行任何形式的商业贿赂以谋取交易机会。

3.不向政府采购代理机构和采购人提供虚假资质文件或采用虚假应标方式参与政府采购市场竞争并谋取中标、成交。

4.不采取“围标、陪标”等商业欺诈手段获得政府采购定单。

5.不采取不正当手段低毁、排挤其他投标单位。

6.不在提供商品和服务时“偷梁换柱、以次充好”损害采购人的合法权益。

7.不与采购人、采购代理机构政府采购评审专家或其它投标单位恶意串通，进行质疑和投诉，维护政府采购市场秩序。

8.尊重和接受政府采购监督管理部门的监督和政府采购代理机构招标采购要求，承担因违约行为给采购人造成的损失。

9.不发生其他有悖于政府采购公开、公平、公正和诚信原则的行为。

投标人名称：_____（投标人公章）

投标人代表：_____（签字）

地　　址：_____

邮　　编：_____

电　　话：_____

年　　月　　日

5.商务条款响应偏离表（格式）

商务条款响应偏离表

投标人名称：_____ 项目编号：SNJZ-2022-188

序号	招标文件 条目号	招标文件商务条款内容	投标文件承诺内容	偏离情况	说明

1.本表须按“第三章 商务条款”中所列商务条款进行比较和响应；

2.该表必须按照招标文件要求逐条如实填写，根据投标情况在“偏离情况”项填写正偏离或负偏离或无偏离，在“说明”项填写正偏离或负偏离原因。

3.该表可扩展。

投标人代表签字：_____(投标人公章) 日期：_____

6. 技术服务方案

投标人根据既定的评分办法，按顺序编制投标文件（**证明材料应清晰可辨，否则视为无效**）

7.履约能力及售后服务证明材料

投标人根据既定的评分办法，按顺序编制投标文件（**证明材料应清晰可辨，否则视为无效**）

8.其他证明文件

投标单位认为有必要提供的其他证明材料。

第七章　服务内容及要求

一、项目背景情况

陕西智慧教育综合服务平台（一期）建设内容以业务应用为核心，满足陕西省教育厅当前业务对信息化需要，以系统整合为本期项目工作重点，以微服务技术搭建全新平台架构，为省教育厅业务整合、资源共享以及未来教育数字化全面转型打下坚实基础。本期建设内容重点是构建技术支撑平台和数据支撑平台，为统一用户、统一认证、数据融合以及系统集成做好支撑。构建教育内部工作门户，将目前已建、新建等业务应用进行整合，实现统一的用户访问入口和基于用户角色的应用级授权，提供个性化的服务定制，构建系统集成框架。同时基于门户的对外公共服务要求完善陕西教育线上办事大厅，围绕办事大厅服务功能构建基于移动端的陕西教育“秦教通”APP，全面打造全方位、多终端的陕西教育公共服务功能。在业务应用方面，围绕业务需求采用新建和升级等方式建设业务应用系统，同时实现与“秦政通”“秦务员”的对接。在安全方面本项目基于陕西政务云平台安全支撑体系，重点完善应用安全和数据安全。

陕西智慧教育综合服务平台总体统筹规划了“1211N”架构，即“1 基础、2 平台、1 门户、1 保障和 N 应用”建设。

“1 基础”。即信息基础设施，是本项目建设的基础环境支撑。本项目运行需要的网络、计算、存储、灾备、安全等基础支撑体系完全依托陕西省政务云平台提供服务，充分考虑安可信创安全、密码应用安全，达到集约化、自主化建设和降本增效的目的。

“2 平台”。建设教育技术支撑平台和数据支撑平台，为教育信息化的相关业务应用提供基础且核心的平台支撑，让业务应用只关注业务流程和业务实现。技术支撑平台的主要功能是为上层业务应用提供统一用户管理、统一授权管理、统一身份认证、单点登录、安全审计等服务，将省教育厅已有且成熟的业务组件或流程组件进行抽取和规范化改造后作为微服务功能为上层应用提供统一服务支撑。数据支撑平台依托统一数据标准，实现全省教育体系各层级、各业务数据的汇聚整合、集中管理，解决教育基础数据中存在的数据标准化、一致性以及同

一数据多源出现等问题，提升对数据“进、存、治、管、用”各环节的管理和服务能力，实现数据的全生命周期管理。

“1 门户”。建设陕西省智慧教育综合服务平台门户，将教育体系的各类资源进行聚合，挂接到统一的服务门户上，打造服务及业务的统一交付窗口，用户只需登录到统一门户就可访问各类服务或开展业务，包括默认门户、个人门户、线上办事大厅、分类检索、跨机构链接等服务功能。

“1 保障”。围绕教育信息化体系，建立统一的管理制度、标准规范等体系，围绕网络和信息安全建立统一的安全保障体系，全面保障教育信息化的建设和实施，并建立长效管理和运行机制。

“N 应用”。业务应用建设是教育信息化建设的核心，围绕教育管理、教学管理、公共服务三大类核心业务需求，采用“统一规划、统筹共需、急用先行、分期建设”的思路，规划梳理 400 余项业务流程，以微服务架构的形式，汇总融合形成支撑各项业务职能的 30 个业务域。

平台建设成后部署在西咸信创云数据中心，依托省级政务云开展平台和数据备份工作、开展信息系统等保测评、开展密码应用等相关工作，并为省教育厅提供项目管理、网络安全和信息化咨询服务与支撑等相关服务工作。

二、备份系统与备份服务

1.环境概述

陕西省政务云平台目前的承载环境如下：

西咸信创云数据中心是省级政务云的生产数据中心，11 号楼信息中心为同城灾备中心，延安云计算数据中心为异地灾备中心，信创云数据中心和 11 号楼信息中心通过双 200G 的电信裸光纤连接，信创云数据中心和 11 号楼信息中心通过租用电信双 10G 的 OTN 链路实现与延安云计算数据中心的连接，实现“两地三中心”的省级政务数据中心布局。

陕西省智慧教育综合服务平台（一期）项目依托陕西省政务云平台进行部署运行，平台的整体容灾备份体系依托省政务云灾备体系开展。

在政务云平台容灾备份体系基础上，本项目重点考虑应用与数据的备份设计。

2.备份目标

2.1 国家标准要求

国家《信息系统灾难恢复规范》GB/T 20988—2007 中对灾难备份等级有明确要求，备份的等级主要分为六个等级。

同时对各等级中 RPO（数据恢复的时间点）和 RTO（数据恢复的时间）都有详细要求，如下表所示：

灾难恢复能力等级	RTO	RPO
1	2 天以上	1 天至 7 天
2	24 小时以上	1 天至 7 天
3	12 小时以上	数小时至 1 天
4	数小时至 2 天	数小时至 1 天
5	数分钟至 2 天	0 至 30 分钟
6	数分钟	0

2.2 灾难备份技术

灾难备份系统实施主要分为业务容灾和数据备份两大类。

数据备份的关注点在于数据，当灾难发生后可以确保用户原有的数据损失降到最小。业务容灾是在数据级容灾的基础上，同时提供应用接管能力，保证业务的连续性。

数据备份技术主要有灾备软件、数据库备份软件、异构存储虚拟化等。业务容灾技术主要有专有厂商软硬件结合、数据同步复制和虚拟化结合、数据容灾软件和持续业务保护系统结合等。

2.3 技术和可用性目标

从省教育厅目前的业务系统分析，因电子政务外网与互联网的复杂性，业务平台保护变得异常复杂，所以，从系统的设计目标而言，简单统一就变得非常重要，总的设计目标如下：

双中心主备模式：构建基于西咸信创云数据中心和 11 号楼信息中心的双中心主备模式，实现在 11 号楼信息中心拥有西咸信创云数据中心所有业务系统备机的结构，数据通过实时复制方式从 11 号楼信息中心向西咸信创云数据中心复

制，并提供当西咸信创云数据中心的业务系统由于发生故障需要恢复时，11 号楼信息中心可进行反向复制能力，从物理上排除单点故障。

实现多备份域：在西咸信创云数据中心、11 号楼信息中心及延安云计算数据中心都建设备份域，将西咸信创云数据中心的数据备份传输到 11 号楼信息中心和延安云计算数据中心实现备份及保护。

业务系统的结构及平台会随着业务需求的变化而不断变化，只有具备灵活弹性的系统架构和统一的管理，才能实现真正意义上的业务保护手段随时调整。

当陕西省智慧教育综合服务平台（一期）各业务系统一旦出现问题，从系统的恢复和业务的连续性上考虑，不确定的因素很多，根据省教育厅具体业务特点，业务系统在容灾备份建设完成后，应能达到以下目标：

1.20 分钟内的故障切换能力

当西咸信创云数据中心业务系统发生停机故障时，11 号楼信息中心在 20 分钟内完成业务系统启动及投运，以保证业务连续性。

2.事务级的数据丢失

采用实时复制技术，根据平台 10000MB/天的数据增量测算，传输需求为：10000MB/3600S/24H＝约 115KB/S，远小于采用 10MB 链路复制时链路提供的约 1MB 数据通讯能力，基本无数据丢失。如果存在丢失，有可能是在复制过程中，复制突然中断造成的几个未处理完成的事务级丢失。

3.快速数据恢复重构

当系统发生逻辑错误时，会造成西咸信创云数据中心和 11 号楼信息中心实时复制的系统数据同时不可信，需要采用备份恢复方式恢复生产数据，在备份过程中，通过针对操作系统和业务数据的备份，在恢复时可以实现故障当天恢复业务系统的快速恢复目标。

总体预期目标具体分述如下表所示：

业务系统恢复目标表

业务高可用实现结果		
服务器故障，导致该服务器系统崩溃	采用复制技术手动切换到热备服务器。	应用中断时间<20 分钟； 数据丢失时间约为 0 分钟；
逻辑错误(例如误删除等)导致生	采用备份恢复。	依据设定的备份频度：

业务高可用实现结果		
产数据丢失或混乱		应用中断时间<2-8 小时； 数据丢失时间<1-2 小时；
西咸信创云数据中心不可用	启用 11 号楼信息中心业务平台。	应用中断时间<20 分钟； 数据丢失时间约为 0 分钟；

3.建设内容

本项目本期规划建设的业务应用系统如下：

- 陕西教育资源公共服务业务域（一期）
- “秦教通”业务域（一期）
- 陕西省教育厅协同办公业务域（一期）
- 校园安全管理业务域（一期）
- 陕西教育扶智平台业务域（一期）
- 陕西教育事业统计管理业务域（一期）
- 技术支撑平台
- 数据支撑平台

根据本项目总体数据量预测，本期所建应用系统的一年数据存储总量预计为336.3TB，其中333TB为教育资源数据，变化不频繁，业务应用数据量每年为3.3T。针对应用系统的建设情况，具体如下：

应用系统本地灾备：利用西咸信创云数据中心已有的数据灾备系统，实现现有应用系统的本地灾备。

应用系统数据异地灾备：在延安云计算数据中心建设数据灾备系统，实现应用系统数据的异地灾备。

4.容灾技术选择

在构建容灾系统所涉及的要素中，数据备份系统是基础，只有保证了数据和应用系统的安全可用，业务的恢复才有可能。数据备份系统采用的技术主要有传统的数据备份和新兴技术数据复制两种。

选择技术路线在整个容灾建设尤其重要。技术路线基本决定了投入成本、所需技术支持力量、后期运营和维护工作量等。传统的数据备份技术不适合重要业务的容灾，实时数据复制是构建容灾的基石。依据本项目特点，采用数据实时复制技术。

数据复制技术主要集中在数据库、操作系统和存储硬件三种技术上，每种技术都有其适用的范围，下面针对这几种容灾技术进行分析并根据应用需求作出技术选择。

4.1 容灾技术选择原则

（1）满足不同应用需求的容灾数据损失（RPO）及应用恢复时间（RTO），数据一致性等具体要求。

（2）支持本地的系统加固以及本地系统的弹性构架。而弹性构架是对 IT 系统的长期发展至关重要，主要是指 IT 系统横向、纵向的扩展性。比如异构环境的支持、扩展。而系统本地加固与远程容灾的技术必须是互不冲突的。

（3）在能够满足以上两项要求的同时，最经济。

（4）支持容灾系统各层的总体切换。

4.2 性能分析

考察容灾系统对业务系统性能的影响，主要从两个方面衡量：一是 CPU 资源的消耗；二是 I/O，特别是写操作的延迟效应。

（1）CPU 资源消耗

采用主机端的软件镜像技术，对 CPU 资源的损耗，实际上是微乎其微的。具体的体现可以通过简单的测试得到：

①在测试系统上，往一个没有镜像的逻辑卷复制一个大文件，查看 CPU 使用率；

②在测试系统上，往一个有镜像的逻辑卷上复制一个大文件，查看 CPU 使用率。

主机 CPU 的处理速度更是在千兆的水平（ns 级），所以 I/O 对主机 CPU 的消耗往往都是可以忽略不计的，如果需要关心的话，也主要针对像 RAID-5 这样的技术（需要大量计算，从而消耗主机的 CPU 资源），而像镜像这样的技术，是几乎不需要消耗 CPU 时间的。

（2）I/O 的延迟效应（特别是写操作的延迟效应）

采用像技术构建容灾系统，其对系统 I/O 的延迟效应要小于任何一种数据复制技术，不管是基于磁盘系统的硬件数据复制技术，还是基于主机软件的数据复制技术，前面的部分已经做了阐述。

（3）复制效果分析

分析项目	数据库复制	存储硬件复制	存储管理软件方案
数据级容灾效果	同步方式对生产中心的性能影响极大。因此基本采用非同步方式，RPO、RTO 都不为零，需要停机时间，数据损失量为一个归档日志的数据损失量。	RPO 接近零。 RTO 不为零，应用会中断，需要手工切换存储。切换时间较短，但由于应用中断以及复制机制都可能导致数据不一致性，因此停机时间可能远远大于存储切换时间。	RPO、RTO 为零。 无应用中断、无数据损失。
数据容灾性能消耗	消耗系统整体（阵列、主机）性能，因此性能开销极大。	消耗磁盘阵列上的 CPU、内存的性能。	消耗主机上的 CPU、内存的性能，由于卷操作不需要内存缓冲，镜像也不是复杂计算，因此对主机的性能消耗小于 3%。
风险	1、采用异步复制，灾难出现后，没有被复制的归档日志的数据将丢失； 2、采用同步复制，数据库性能将大幅下降。	1、数据从主存储复制到从存储时，链路中断，可能导致数据不一致，数据库无法启动，丢失； 2、存储 Cache 出现错误，将复制远端，导致两个存储都不可用。	无

5.容灾架构设计

本次项目容灾备份系统建设，采用存储管理软件容灾解决方案，实现同城容灾，另外根据需要可以很容易扩展到异地容灾。

6.同城容灾系统设计

同城容灾中心的建设是以业务容灾为目标，保证系统在容灾中心有实时的数据冗余，应用系统冗余，及硬件处理能力。当区域性灾难发生时，容灾中心能够及时接管业务，保持业务系统的连续性。

6.1 同城容灾实施方案分析

关键应用同城容灾实施方案对比分析如下表所示：

方案对比表

方案	主要软硬件	IP 链路要求	RPO(理论)	RTO(理论)	建设难易	投资大小	可靠度
专有厂商软硬件结合	1、专用软硬件、集群及操作系统 2、灾备两中心同构存储专有复制技术	≥1Gbps	≈0	≤3~5 分钟	难	高	较高
数据库同步复制和虚拟化结合	1、数据库自身软件同步复制数据 2、特殊的虚拟化平台软件	≥1Gbps	≈0	≤3~5 分钟(应用需 3~5 分钟 Vmware 的 SRM)	中	中	较低
数据容灾软件和持续业务保护系统结合	1、数据容灾软件 2、应用容灾保护系统	≥10Mbps	≤1~10 分钟	≤30 分钟	易	低	中

从上表综合分析可以看出：

（1）基于“专有厂商软硬件结合”的同城容灾方案：中心两端软硬件设备要求严格，链路要求高，这样投资就很高。

（2）基于“数据库同步复制和虚拟化结合”的同城容灾方案：中心两端数据库、操作系统要求严格，且需要特殊的虚拟化平台软件做应用容灾。

（3）基于“数据容灾软件和持续业务保护系统”的同城容灾方案：在中心两端主要软硬件使用要求低，符合现有应用环境实现容灾，对其它如链路、RTO、RPO 值等方面相对于前两个方案都比较适中。

6.2 同城容灾备份规划实施

基于“数据容灾软件和持续业务保护系统”的同城容灾方案的实施实际包括数据库和应用两个方面，要求两者相互配合、共同协作，来完成陕西省智慧教育综合服务平台（一期）同城容灾功能。

7.异地容灾系统设计

异地灾备中心的建设是以数据级灾备为目标，保证系统在异地灾备中心有完整的数据备份，应用系统备份，及相应的硬件处理能力。异地灾备中心一般是在 300 公里以外建立应急指挥中心的灾备中心，一旦应急指挥中心现场发生灾难，

各业务系统重要的、有要求的数据可以通过相应工作去恢复和使用异地灾备中心的备份数据，从而保证当意外发生后对重要业务和应用的影响降至最低。

7.1 异地灾备实施方案分析

数据级异地灾备方案中，基于异构存储虚拟化数据级灾备技术，是以其存储自身携带的远程卷复制（或镜像）软件实现的，而且这种方式实现的是数据块复制，需要相关的集群软件来保障数据的有效性和可用性，并且其适用面是狭窄的，只适用于一些特殊需求的应用场合；这种技术同时需要西咸信创云数据中心、11号楼信息中心、延安云计算数据中心具有相同的主机环境才能得到验证。磁盘阵列或虚拟化存储的卷复制或镜像技术要求两中心的存储同品牌，条件比较苛刻；虚拟化存储引擎，对广域网带宽要求较高。目前不同厂商产品对异构存储产品的支持也不尽相同，虚拟化存储技术正在发展阶段，各厂商技术参差不齐，比较成熟的厂商产品价格昂贵。基于数据库自身备份技术的数据级异地灾备，不同数据库厂商具有不同的技术，且具有排它性。基于灾备软件技术的数据级异地灾备，从带宽、硬件、支撑软件等各方面环境要求比较低，适合咸信创云数据中心异地灾备。

考虑到链路、带宽、投资、技术现实等各方面的因素，以及陕西省智慧教育综合服务平台（一期）结构化和非结构化数据等综合复杂情况，西咸信创云数据中心的异地灾备实施方案暂不考虑业务级远程容灾，以数据级远程灾备方案为主进行建设与实施。待各方面条件成熟后，再按需求实现业务级远程容灾。

7.2 异地容灾备份规划实施

基于灾备软件的数据级异地灾备实施方案是针对陕西省智慧教育综合服务平台（一期）数据级远程异地灾备而建的，为了保证灾备数据的可恢复性，必须在异地设有相似的验证服务器。

8.备份策略

8.1 备份策略选择

选择了存储备份软件、存储备份技术（包括存储备份硬件及存储备份介质）后，首先需要确定数据备份的策略。备份策略指确定需备份的内容、备份时间及备份方式。目前被采用最多的备份策略主要有以下四种。如下表所示：

备份策略	描述
Full Backup 完全备份	完全备份就是每次对系统进行完全的备份。当数据发生数据丢失灾难时。完全备份所需要的时间最长和消耗的磁带最多，但恢复时间最短和操作最方便。
Incremental Backup 增量备份	增量备份就是备份上一次全备份或者增量备份系统发生改变的数据。这种备份策略的优点是节省了磁带空间，缩短了备份时间。但是它的缺点在于当灾难发生时，数据的恢复比较麻烦而且可靠性比较差。其中任何一盘磁带出现问题都会影响之后的磁带恢复。
Differential Backup 差量备份	差量备份就是备份上一次全备份后到系统发生改变过的文件。它的优点是无需要每天对系统做完全备份。因此备份所需要时间短并目节省了磁带空间。还有，它的灾难恢复也很方便。系统管理员只需要全备份和增量备份的介质就可以进行系统的恢复。
Synthetic Backup 合成备份	合成备份是当备份窗口较短时进行。在进行合成备份的时候，会从完全备份、增量备份和差量备份中读取信息，然后创建一个新的完全备份。这使完全备份可以离线进行并日网络还是在继续体用，不会降低系统性能或者妨碍网络中的用户。

结合本项目情况，在实际应用中，备份策略建议采用完全备份、增量备份和差量备份三种方式组合。采用每日、每周、每月的备份方式进行组合使用，达到备份要求。

8.2 系统备份范围

- 应用系统：操作系统 GHOST 备份和应用包备份。
- 数据库：每日自动备份到备份服务器。

主机	策略设计
应用主机	1.该主机采用 LAN 方式进行数据备份； 2.每月一次基于操作系统级数据备份，备份到虚拟带库，保留 2 个月；每个月将备份数据离线保存，保存 6 个月； 3.每天一次对指定路径进行全备份，备份到虚拟带库，保留一周。
数据库主机	1.该主机采用 LAN-Free 方式进行数据备份；每月一次基于操作系统级数据备份，备份到虚拟带库，保留 2 个月；每个月将备份数据 Vault 到物理带库，保存 6 个月； 2.每天一次数据库在线全备，备份到虚拟带库，保留一周；每周一次将所有备份数据 Vault 到物理带库，保存一年。

8.3 备份容量需求

系统名称	备份容量估计	所需备份天数	备份策略
陕西省智慧教育综合服务平台（一期）_业务数据	9.39GB（每天）	每天、每周、每月	采用完全备份、增量备份和差量备份三种方式组合
陕西省智慧教育综合服务平台（一期）_教育资源数据	27.75TB（每月）	每月	以差量备份为主，对改变的数据进行备份

8.4 备份策略

结合陕西省智慧教育综合服务平台（一期）统一备份和系统要求，专门制定数据库备份策略，辅助完成平台数据备份工作。平台数据库采用物理和逻辑相结合的方式进行备份。逻辑备份采用逻辑导出的方式，每天对数据库进行备份；物理备份需要打开归档模式，使用 RMAN 对数据库进行增量备份，除了数据文件以外，还要备份控制文件、参数文件和归档日志。

逻辑备份：每天凌晨 12：00，使用 exp 命令将数据库数据导出到本地磁盘。当数据库出现故障时，可以重新搭建并导入最近的一份数据进行恢复。另外需要注意的是，使用逻辑备份只能将数据库恢复到最近备份的那一时刻，因此，逻辑备份只能是一种次要的备份方案，当物理备份不能恢复时才使用。

物理备份：物理备份使用 RMAN 对数据库进行增量备份，除了数据文件以外，还要备份控制文件、参数文件和归档日志。由于数据库存放在存储上，为了避免备份介质和数据库同时发生丢失，建议将备份介质存放在数据库服务器的本地磁盘上。另外，建议将 RMAN 备份的元数据储存在编目数据库中，使用编目数据库可以提高备份元数据的可靠性。

每天晚上逻辑备份结束后使用 RMAN 进行物理备份，具体来说采用差异增量备份，备份策略如下：周日晚上执行零级备份；周四晚上执行一级备份；周一、周二、周三、周五、周六执行二级备份。具体时间更具逻辑备份所需时间而定。采用差异增量备份可以有效减少每天的数据备份数量。每天仅备份自最近一次同级或低级备份以来所改变的数据。而做恢复时最多只要恢复本周的 1 个零级备份+最近的同级备份+本周的 1 级备份+当天的归档日志+联机日志。

恢复窗口设置为 7 天，数据库可以恢复到七天内的任何时间点，一周以前的备份集将被标记为过期备份集；

每次备份完成后检查备份集并删除过期的备份集，周日 0 级备份完成后会删除之前的所有备份集；

采用自动备份控制文件和参数文件，数据库结构变化时自动将其备份；

每次除备份数据文件外，还包括控制文件、参数文件以及归档日志，备份完毕后自动删除备份过的归档日志以及过期的备份集；

备份完毕后自动检查备份集的完整性，问题会反映在日志中。

9.容灾备份配置清单

序号	设备名称	参数说明	单位	数量	备注
1	虚拟带库	含磁盘库引擎及软件，可用备份容量 36TB，具备重复数据消除功能，2 个 8Gb FC，2 个 10 Gb iSCSI，可接入 FC SAN 网或接入以太网。	台	1	
2	物理带库	控制器、电源冗余，磁带驱动器数量≥4，非压缩速率≥120MBps；配置磁带槽位数量≥48；最大存储≥400GB，压缩后≥4TB。	台	2	
3	内网备份存储	存储双冗余控制器，24GB 高速缓存，8 个 8Gb FC 主机接口，可在线添加 FC, iSCSI, FCoE 接口；配置 40 块 1T 近线 SAS 硬盘，最大可支持 250 块硬盘；Unisphere 存储管理软件，支持中文，提供数据压缩功能，提供自动容量扩展功能；提供数据迁移功能软件；支持 FAST VP 和 FAST 缓存自动分层存储；支持快照和克隆功能，驱动器降速；支持基于文件和数据块的远程同/异步复制；支持 Windows、Linux、VMware、UNIX。	台	1	
4	测试服务器	2 盒 CPU；32GB 内存，≤320GB 内存扩展；4*8T 数据盘可支持 SSD 硬盘扩展；支持 TCG1.2 的 TCM 可信模块，配套数据保护盾软件含 2 块 4GB HBA 卡。	台	3	
5	备份服务器	2 盒 CPU；32GB 内存，≤320GB 内存扩	台	3	

		展；4*8T 数据盘，可支持 SSD 硬盘扩展；支持 TCG1.2 的 TCM 可信模块，配套数据保护盾软件含 2 块 4GB HBA 卡。			
6	容灾备份软件	备份服务器许可、应用及数据库备份客户端许可、数据库备份代理许可、重复数据删除及备份优化加速许可。	套	1	
7	陕西省智慧教育综合服务平台（一期）软件	处理器 ≥ 2* 16C；内 存 ≥ 256G；系统盘 ≥ 2*480G SSD 2.5；闪存盘 ≥ 2*3.84T SSD 2.5；数据盘 ≥ 4*8T SAS 3.5；网 卡 ≥ 2 块万兆网卡（含 2 个多模模块），双口千兆网卡，1 个 IPMI 独立管理口；Raid 卡 2G 缓存带电容保护、配置直通模式；双冗余电源；支持 TCG1.2 的 TCM 可信模块，配套数据保护盾软件含 2 块 4GB HBA 卡。	套	2	服务器虚拟化实现业务系统运行
8	数据库	国产，支持集群。	套	1	
9	数据库	Orcale 11g（64 bit 标准版(25user) RAC）支持集群。	套	1	
10	中间件	国产，64 位企业版。	套	1	
11	操作系统	Windows 2012 企业版 64 位，Linux 5 server 64bit。	套	1	

三、咨询服务需求

为保障陕西省智慧教育综合服务平台（一期）建设和管理的标准化、规范化，本项目将引入专业咨询团队，从标准规范、管理制度和技术方案等多个方面保障专业咨询服务。

1.标准规范设计

根据陕西省智慧教育综合服务平台（一期）建设需求，编制《陕西省智慧教育综合服务平台数据字典及编码规范》，规范教育基础数据的编码规则。

《陕西省智慧教育综合服务平台数据字典及编码规范》对教育基础数据的数据项、数据结构、数据流、数据储存、处理逻辑、外部实体等进行定义和描述，建立标准的编码体系，以此作为陕西省智慧教育综合服务平台基础数据进行编码的依据和准则，并确立代码与项目之间的对应关系。

2.管理制度设计

为了提高陕西省智慧教育综合服务平台的数据管理及应用水平，进一步加强数据管理，明确数据传输、数据检查、数据库管理、数据安全工作的责任，需要制定《陕西省智慧教育综合服务平台数据管理制度》。

《陕西省智慧教育综合服务平台数据管理制度》围绕数据传输（各层级对批量信息数据或规定信息数据的发送、接收过程）、数据检查（对要发送数据和已接收数据的正确性、完整性、逻辑性检查）、数据库管理、数据安全、各层级或部门对数据的录入、数据更新等工作建立明确的管理制度，理清数据管理责任，对于违反数据管理制度的，要制定明确的过错责任追究办法，通过数据管理制度和管理标准规范，确保平台及数据的绝对安全。

3.技术方案设计

围绕本期项目的执行要求，编制《教育信息系统国产化建设适配改造和迁移技术方案》、《陕西省教育厅教育数据资源体系规划报告》，进一步规范和指导平台体系和相关内容的建设。

编制《教育信息系统国产化建设适配改造和迁移技术方案》，对现有教育信息系统进行现状调研，梳理系统的功能内容、性能指标、用户数量、安全等级保护等级、安全指标、部署情况、开发语言及系统架构等，根据现状调研结果，进行系统适配分析和技术路线选型，编制适配改造和迁移方案，包括迁移改造、适配改造、适配自验证、测试认证、迁移实施、试运行和系统迁移适配保障措施等内容。

编制《陕西省教育厅教育数据资源体系规划报告》，以省教育厅实际业务为驱动，对已有业务系统和本次新建业务系统数据资源进行规划和梳理，并按照业务类型进行分类和编目，对数据进行资产管理化规划。按照“一数一源”的原则，对数据库整体结构和分类进行科学规划，对库表结构优化设计，最终规划设计实用、可靠、标准、开放的数据资源库，包括基础库、主题库、专题库、共享库等。

四、等级保护服务需求

1.系统定级

陕西省智慧教育综合服务平台部署在陕西省省级政务云，电子政务外网一侧区域，相关网络环境及云平台硬件资源的维护工作由省级政务云负责。校园安全

管理业务域部署在电信公司机房，通过互联网与陕西省智慧教育综合服务平台进行业务联动和数据共享。

（1）业务信息安全保护等级

陕西省智慧教育综合服务平台主要用于教育资源服务、教育教学管理、校园安全管控、政务事项办理等工作。业务信息主要包括教育行业组织机构信息、师生个人身份信息、教学科研信息、食品卫生安全信息、校园防疫信息、视频监控信息等。

依据 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》中业务信息受到破坏时所侵害的客体以及侵害程度，确定陕西省智慧教育综合服务平台的业务信息安全等级为第三级。

（2）系统服务安全保护等级

陕西省智慧教育综合服务平台主要为教育行政管理部门人员、师生提供课程资源共享、教育教学活动的管理及发展评估、学校食品卫生及校园安全监督管理、教育资源分布及统计分析、政务审批事项咨询办理等服务。

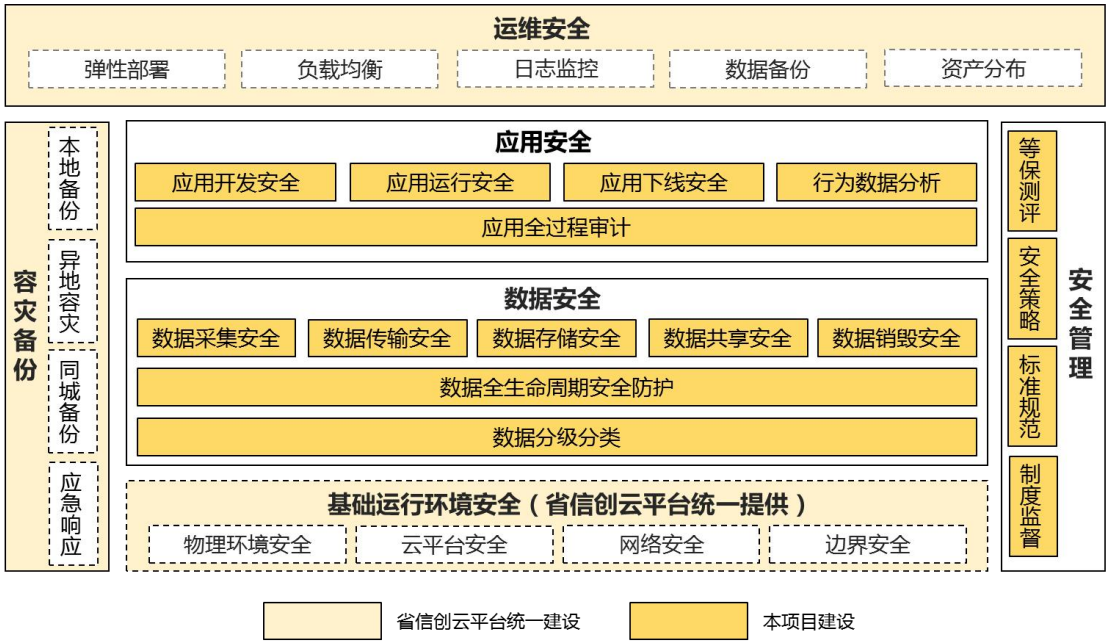
依据 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》中系统服务受到破坏时所侵害的客体以及侵害程度，确定陕西省智慧教育综合服务平台的系统服务安全等级为第三级。

（3）安全保护等级的确定

依据 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》要求，陕西省智慧教育综合服务平台的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定陕西省智慧教育综合服务平台安全保护等级为第三级。

2.安全体系架构

依照《中华人民共和国网络安全法》、《网络安全等级保护条例》等相关政策和《信息安全技术网络安全等级保护基本要求》（GB/T 25070-2019）（简称“等保 2.0”）中第三级的标准要求，以防护平台化、部署集约化设计思想为指导，构建本项目的安全架构体系，实现身份可信和行为可控。本平台安全架构如下图所示：



陕西省智慧教育综合服务平台采用集约化建设部署，充分依托陕西省信创云平台提供的安全基础设施进行安全防护。本项目基础运行环境安全、网络及边界安全、容灾备份等由省信创云平台统一提供，不再进行重复建设。

本项目安全防护体系建设内容主要包括应用安全、数据安全和安全管理三部分内容。

（1）应用安全：依托省信创云安全防护体系和统一公共支撑平台服务，围绕应用开发安全、运行安全、下线安全和行为数据分析来保障应用的安全，对设备、人、应用、服务等进行身份管理，先认证后访问，只有经过严格认证和授权的用户和终端才能访问应用和服务，建立主体到客体之间访问路径上的完整信任链，全面提升应用系统安全性。

（2）数据安全：以数据分类分级为基础，以国产密码技术为支撑，依托省信创云安全防护体系和统一公共支撑平台服务，主要围绕数据的采集、传输、存储、使用和销毁，建立数据全生命周期的安全防护体系，保证数据来源可信、访问可控、操作可查和责任可追。

（3）安全管理：主要围绕安全等保测评、标准规范、安全制度、以及安全策略组成本项目的安全管理内容，实现从安全标准到策略、从技术实现到管理措施，全方位保障项目的整体安全。

3.安全防护设计

3.1 数据安全

以“零信任”为出发点，在数据分类分级的基础上，以国产密码技术为支撑，遵循最小权限和动态授权原则，在数据资源的全生命周期，建立数据可信接入、数据加密、数据脱敏、认证授权等，保障数据中心的数据开放共享安全生态，统一数据资源流通管理，确保数据来源可信、访问可控、操作可查和责任可追。

依托省信创云安全防护体系和公共支撑平台服务，为本项目数据全生命周期提供安全保护能力。数据安全建设内容包括：数据分类分级、数据采集安全、数据传输安全、数据共享使用安全、数据存储安全、数据销毁安全等内容。

3.1.1 数据分级分类

为了让数据安全、高效的使用和共享，需要对多种来源的教育资源数据（包括陕西省教育厅数据、政府其他部门数据、行业单位数据、互联网数据等）进行数据资产梳理和数据分类分级，对不同级别的数据采取差异化安全管控措施，在确保数据合理合规流动的前提下，促进数据安全高效的开发利用和共享。

（1）数据分级

根据数据发生泄漏对国家安全、社会秩序及公共利益、公民/法人/其他组织合法权益的危害程度进行分级，数据敏感度总体上分为公开、内部、敏感。

级别	级别名称	级别描述
第一级	敏感数据	教育厅机关在教育教育管理、教学管理、公共服务等活动和内部管理中产生的，在一定时间只限于一定范围内的人员知悉，泄漏会给教育管理造成被动或损害的事项信息
第二级	内部数据	教育厅机关内部掌握，不宜公开的信息和有关部门及单位内部掌握、不宜公开的内部事项等
第三级	公开数据	教育机关依法已公开或应当公开的信息和来自于互联网的信息

（2）数据分类

按多维度多层级进行分类，例如数据来源、数据属性、数据组织和其他多维度分类，同一种维度也可按多层级分类。

3.1.2 数据接入安全

数据采集者按照数据分类分级相关规范对数据进行分类分级标识。依托信任

服务基础实施，采用接口认证、设备认证、用身份认证等多种认证方式，确保数据源可信;对接入数据进行病毒查杀和恶意代码检测,保证接入数据的内容安全。

3.1.3 数据传输安全

数据（流式数据、数据库、文件、服务接口等类型的数据）传输过程中，采取国产商用密码技术保障数据的完整性、机密性。

（1）公开数据传输安全：

进行数据完整性校验；

（2）内部数据和敏感数据传输安全：

进行数据传输加密、数据完整性校验、数据防泄漏等。

3.1.4 数据存储安全

数据存储安全主要是指数据在存储的过程中保持完整性、机密性和可用性的能力。面临的风险主要来源于数据泄露、数据丢失等问题。为解决数据存储阶段的风险问题，应对数据进行加密存储、分级保护和容灾备份。

（1）数据加密

对于敏感数据、内部数据，在存储时进行加密处理。为了满足数字资产等级化的安全要求，通过字段级别的加密方式对敏感数据、重要数据进行加密，加密后以乱码的形式存在，保证存储介质丢失和数据库文件被非法复制的情况下，敏感数据、重要数据的安全。

（2）分级保护

基于数据分类分级对内部数据和敏感数据进行分级保护,最大程度保障数据资产。

（3）数据备份

采用多副本机制对数据进行存储解决数据丢失问题。通过周期性保存在线数据的历史,以便在线数据发生损坏时,使用备份数据恢复到错误发生之前的状态,以确保数据的正常访问。同时采用严格的备份策略、流程等一系列手段确保数据应用不会对备份数据的存储数据安全产生影响。

3.1.5 数据共享使用安全

（1）认证授权

根据用户行为、情况动态进行数据授权。通过集中统一的访问控制和细粒度

的授权策略，对用户、应用等访问数据的行为进行权限管控实现集中有序的操作管理，确保用户拥有的权限是完成任务所需的最小权限，防止非法、越权访问事件发生，并对违反策略的行为进行告警、阻断等响应，根据用户行为、运行环境动态调整授权策略。

（2）数据脱敏

对敏感数据依据用户角色（外部用户、内部用户）、业务系统类型进行脱敏，不改变敏感数据原始内容和业务系统正常运行。常用脱敏算法包括固定值、模糊取整、随机化、多字符替代、高相似度替代等。

（3）数字水印

依托公共支撑平台提供数字水印标记安全服务，能对纯文本及富文本等多种数据类型进行水印嵌入、提取、检测等操作，对删除、复制、粘贴等破坏行为后的水印文件能进行提取和恢复，对水印信息进行检测和分析，从而追溯外泄源头，实现数据防泄露。

（4）安全交换

针对教育资源数据内部和外部的纵向流通和横向共享时应采用认证授权方式达到安全可控。在数据共享发布时确保数据和来源真实，涉密、涉敏等情况以数据脱敏脱密方式达到重要数据内容合规，并以审计方式达到交换实体可信、交换行为可查。

（5）数据防泄露

通过基于内容识别的关键数据发现和自然语言处理及数据分类，可以全方位的对敏感信息进行定位，如源代码，技术文档，组织机构资料，人事信息等，分析到敏感信息的存在，以此为依据来进行有效的文件访问防护和外发控制。

3.1.6 数据销毁安全

为防止数据被恶意窃取和利用，在数据使用完成后应对数据进行安全销毁操作，采用硬盘消磁机、硬盘粉碎机、硬盘折弯机等硬件设备通过物理方式彻底毁坏硬盘，确保数据介质销毁安全；采用全自动、半自动和手工擦除方式，对数据内容进行安全销毁。

3.2 应用安全

从本项目业务应用系统的开发、上线、安全运行、下线等全生命周期，完成

应用系统安全体系建设。采用“零信任”设计思想，对设备、人、应用、服务等进行身份管理，先认证后访问，只有经过严格认证和授权的用户和终端才能访问应用和服务，建立主体到客体之间访问路径上的完整信任链，全面提升应用系统安全性。

应用安全包括应用开发安全、应用运行安全、应用下线安全管控。

应用系统开发阶段，从安全需求分析、安全设计、安全开发、功能测试、上线测试等环节进行安全设计。应用业务系统上线运行后，从身份认证访问控制、应用安全、应用安全检测等环节进行安全设计；应用业务系统下线后，采取数据备份、数据清除、资源回收等措施。全过程进行审计，把日志数据和用户应用访问行为数据报送给教育厅信息化安全运营管理部门。

3.2.1 应用开发安全

根据安全开发生命周期管理的要求，制定并完善自身的应用安全开发管理规范，用以指导应用系统开发过程中各个阶段的安全工作。

（1）安全需求分析

依据应用系统等级，建立不同安全级别的应用系统安全需求标准及规范。在建设应用系统初期，就应把安全需求纳入到需求文档，形成安全需求分析说明书。应在应用系统立项阶段就对应用系统需求进行安全评审，在评审中应给与修订的意见，待其完善需求并满足应用系统安全需求规范后再启动后续流程。

（2）安全设计

软件开发人员与安全人员依据系统安全需求设计说明及相关标准规范，开展应用系统的安全架构设计。主要包括：安全框架的选择、中间件的选择、数据库组件选择、通信中间件设计、应用系统与其他系统交互的安全性设计。

（3）安全开发

依据相关标准要求，安全开发阶段主要遵从代码开发规范，依据陕西省教育厅所用的开发工具，相应制定各类开发语言安全编码规范，同时开展代码走查和代码审计活动。

（4）安全测试

依据相关标准要求，软件开发在系统测试过程中，需要开展安全性测试，同时要保证测试过程中的数据安全。在开发流程中开展代码白盒测试，对应用系统

开展代码审计，提升源代码的安全性；为安全功能设计测试用例，在系统开发过程中开展黑盒测试，做到安全功能测试的全覆盖。

3.2.2 上线测试安全

对开发的应用系统，在云平台开发测试区，开展上线发布测试，检验应用系统是否满足安全要求。

（1）应用漏洞扫描

通过专业的 WEB 漏洞扫描工具，检测发现应用系统存在的安全漏洞。主要的内容包括：常见的 OWASP 漏洞检查、配置错误检测、开源组件的安全扫描。

（2）渗透测试

渗透测试通过人工模拟黑客攻击的方式，发现应用系统中存在的安全问题。主要包括 WEB 安全、业务逻辑安全、中间件安全、服务器安全等内容。

（3）安全基线检查

通过“自动化工具配合人工检查”方式来完成基线核查，对上线应用系统基础环境配置情况进行核查，核查对象包括操作系统、Web 中间件、数据库和网络设备等，确保应用系统支撑基础环境的安全配置满足省教育厅的基线标准。

3.2.3 应用运行安全

3.2.3.1 基于身份认证的访问控制

通过建设基于“零信任”架构的身份管理系统和权限管理系统，采取严格的访问控制和安全检测方式，仅通过检测的设备、通过身份认证的用户，才能够进行业务访问。

（1）身份认证

在身份认证方面，可采用密码、口令、数字证书、人脸识别等技术手段提升应用安全能力，使用过程中不定期进行二次身份验证，及时发现异常使用人员。

在统一授权管理方面，对访问应用系统、应用功能、数据、服务接口的权限进行细粒度控制。在应用系统上线前，根据业务需求设定不同角色，通过给用户角色授权来控制所需访问的功能模块和相应安全级别的数据。

（2）应用授权

在应用访问时验证角色是否拥有对应用系统、应用功能、服务接口和数据的访问权限。

a）授权实现

应用授权采用基于角色的授权方式实现。应用系统依据其提供的功能和服务接口创建角色，并依托权限管理系统建立该角色与数据的权限关系。用户依据其身份信息被分配给具体角色，在访问应用时权限管理系统将验证该用户的角色是否拥有对应用系统、功能、服务接口和数据的访问权限，从而通过角色实现授权访问。

b）授权分类

授权模式分为静态授权与动态授权两大类，静态授权包括常规授权和敏感资源授权，动态授权包括临时授权和一事一授权。

静态授权：

针对使用公开和内部信息的应用系统，采用按岗按需的原则进行授权，依托省信创云公共支撑平台建立省教育管理用户授权管理体系，根据工作岗位的实际需求，在应用系统中创建角色，授权其可访问的数据、服务、应用的类型与级别。权限管理采用分级管理方式，由省、市二级其所辖用户进行授权管理，用户在岗位调整或者工作变化时需及时进行权限变更，由用户所在单位提出申请，由权限管理系统审核，按相应规定给予数据和服务授权。

动态授权：

针对重大突发性、临时性事件，需对用户进行数据、服务的临时授权时，由用户所在单位提出申请，并提出授权时限，可以经分管领导审批后，由权限管理系统授权，该授权到期后自动撤消。

3.2.3.2 应用安全保护

（1） 应用传输安全

为确保业务访问流量传输过程的安全性，需要使用国密算法进行加密传输。针对不同的业务，需要采用不同的访问方式，兼顾安全和易用性。本项目为 B/S 应用，采用国密安全浏览器内置的国密通信引擎进行 Web 流量的安全传输。

（2） 应用安全隔离

不同的用户使用不同的账号以实现资源与其他用户的逻辑隔离，每个用户还可根据自身安全需求申请多个账号隔离不同敏感程度业务应用集。主账号管理员还可创建不同子账号按需给应用开发者、运维、测试人员分配其角色对应的资源

访问权限，以实现应用所使用资源管理权限的隔离。

（3） Web 应用安全

依托省信创云 Web 应用防火墙，满足防御应用攻击。Web 应用防火墙具备 Web 攻击的防护、Web 非授权访的防护、Web 恶意代码防护、Web 应用合规性审计防护、网页防篡改等能力。

3.2.3.3 应用安全检测

通过应用扫描工具，对应用业务系统自身和运行环境进行安全性检查，内容包括：操作系统、空/弱口令系统账户检测、访问控制、系统漏洞、安全配置问题、系统服务；通过专业的 Web 漏洞扫描工具，检测发现应用系统存在的 SQL 注入、XSS 攻击、文件上传、远程执行等 Web 漏洞。

3.2.4 应用下线安全

为了加强系统全生命周期管控，制定应用系统下线管理制度，进一步完善应用系统全生命周期管控。

（1）系统下线要求

对于业务方明确提出下线要求的系统，应遵循应用系统下线管理制度要求，执行下线应用系统的设备回收、数据备份与清除、域名资源回收等操作。另外，对于长期处于“僵尸系统”状态的应用系统，省应急管理厅相关部门应先通知系统业务单位，请求业主判定系统是否可以下线。

（2）数据备份

对于已经明确可以下线的应用系统，应做好应用系统数据备份，数据备份包括数据库系统备份、应用系统文件备份和应用系统配置数据备份等内容。

（3）应用数据清除

为了保障应用系统数据安全性，应清除下线应用系统存储介质上的数据，保证数据不会外泄。存在多种级别应用系统时，可按照不同级别采用不同强度的数据清除手段。按照数据销毁流程，保证数据不可恢复。

（4）资源回收

应对下线应用系统的资源进行回收，包括注销应用系统证书及回收证书介质，变更撤销应用系统访问控制策略、禁用或删除安全运维账号等。对非共用资源进行释放与回收，回收的资源包括计算资源、存储资源、网络资源、安全资源等。

3.2.5 应用安全审计

实现应用流量采集和应用日志采集；对被管资源的数据操作行为、用户所有操作行为、动态授权操作行为以及运行管理信息进行采集；对采集后的流量和日志数据进行安全审计。

3.3 安全管理体系

3.3.1 安全管理制度

3.3.1.1 安全策略和制度体系

信息安全管理制度体系应结合实际业务需要，建立符合教育厅实际情况的安全制度体系，需包括信息安全方针、安全策略、安全管理制度、安全技术规范以及流程等。

（1）安全方针和策略

最高方针，纲领性的安全策略主文档，陈述本策略的目的、适用范围、信息安全的管理意图、支持目标以及指导原则，信息安全各个方面所应遵守的原则方法和指导性策略。

（2）安全管理制度和规范

各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是必须具有可操作性，而且必须得到有效推行和实施的。

（3）安全流程和操作规程

为信息安全建立相关的流程，保证安全运营可以遵照标准流程制度执行，主要的内容包括：流程制订、流程变更、流程发布等内容。

（4）安全记录单

安全记录单是落实安全流程和操作规程的具体表单，根据不同等级信息系统的要求可以通过不同方式的安全记录单落实并在日常工作中具体执行。主要包括日常操作的记录、工作记录、流转记录以及审批记录等。

3.3.1.2 制度文件管理

制度文件需要正式发布并进行定期评审修订和版本控制。信息安全管理制度应该得到单位负责人的签发和认可，只有被正式发布并真正落实的管理制度才能促使单位安全管理能力的提升和安全技术措施的有效运行。

（1）制订和发布

安全制度系列文档制定后，必须有效发布和执行。发布和执行过程中除了要得到教育厅主管部门的大力支持和推动外，还必须要有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。

（2）评审和修订

省教育网络安全和信息化工作领导小组应组织相关人员对于信息安全制度体系文件进行评审，并确定其有效执行期限。同时应指定信息安全职能部门每年审视安全策略系列文档。

3.3.2 安全管理机构

3.3.2.1 信息安全组织机构及职责

陕西省教育网络安全和信息化工作领导小组是陕西省教育信息安全工作的最高领导决策机构，负责陕西省教育厅信息安全工作的宏观管理，其最高领导由陕西省教育厅主管领导担任，其主要职责是贯彻执行国家和陕西省关于信息安全工作的方针、政策，组织落实陕西省教育厅信息安全体系建设工作的目标、方针、政策。

领导小组办公室（设在省教育厅教育信息化处）是全省教育信息安全管理部门，负责落实网络安全和信息化工作领导小组各项决策，协调组织教育厅各项信息安全工作。

3.3.2.2 岗位职责及授权审批

根据教育厅实际情况，设立相关的信息安全管理岗位，但至少应包括安全主管以及“三员”（系统管理员、审计管理员和安全管理员），且“三员”工作职责需分工明确，互相监督，安全管理员需专职，不得兼任其他岗位工作。

3.3.2.3 内部沟通和外部合作

聘请专家和外部顾问成员，这些成员需要对信息安全或相关领域有丰富地知识和经验，如安全技术、电子政务、等级保护或质量管理等。专家和外部顾问负责对信息安全重要问题的决策提供咨询和建议。

同时加强与投标单位、业界专家、专业的安全公司等安全组织的合作和沟通。建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信

息。

3.3.2.4 安全审核与检查

（1）定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

（2）定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；全面安全检查可请专业的安全厂商协助完成。

（3）制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。制定安全检查评价指标，以便量化考核安全工作的执行情况。

3.3.3 安全管理人员

3.3.3.1 内部人员安全管理

针对内部人员的安全管理需从人员的录用、安全培训和教育、技能考核和调用、离岗审核等全过程进行安全管理，具体管理要求包括：

（1）录用前

应对被录用人员的身份、安全背景、专业资格或资质等进行审查， 对其所具有的技术技能进行考核；与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

（2）工作期间

对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；定期对不同岗位的人员进行技能考核。

（3）调离岗

及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；办理严格的调离手续，并承诺调离后的保密义务后方可离开。

3.3.3.2 外部人员安全管理

制定外部人员物理访问和网络接入的管理制度，并记录相关内容，具体要求如下：

（1）在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程

陪同，并登记备案；

（2）在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

（3）外部人员离场后及时清除其所有的访问权限；

（4）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

3.3.4 安全建设管理

3.3.4.1 系统定级和备案

为了进一步明确信息系统定级、备案的相关责任和流程，应明确系统定级、备案和系统测评流程，包括以下内容

（1）明确定级备案责任部门和责任人；

（2）跟公安部门沟通明确定级备案相关材料要求和格式；

（3）制定系统定级和备案工作的时间计划；

（4）定级评审相关单位和专家联系和确定；

（5）组织定级评审工作，并获得上级或相关部门的批准。

为确保系统等级保护定级备案工作的规范性和专业性，可选择专业的等级保护咨询服务完成相关工作。

3.3.4.2 系统安全方案设计

安全方案设计需根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。

安全方案应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。

安全建设项目根据实际建设阶段需设计不同的安全方案，包括总体建设规划方案、详细设计方案、建设实施方案等，安全方案需组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

3.3.4.3 安全产品采购

针对陕西省智慧教育综合服务平台一期项目的安全设备采购，需严格按照设

备采购管理流程和信创产品名录来采购相应的安全产品；并且在搭建的模拟系统中对这些安全设备和软件进行测试和试运行验证，以防止产生对系统产生不可预见的影响。

3.3.4.4 工程实施管理

在实施过程中通过招标确定项目第三方监理单位，并指定专门的项目安全工作负责人，制定项目管理制度和项目实施方案。

3.3.4.5 测试及交付管理

项目建设完成后在正式上线前进行系统测试，制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告，按照等级保护的要求，进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

在系统交付时，应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，对负责系统运行维护的技术人员进行相应的技能培训，提供建设过程文档和运行维护文档。

3.3.4.6 系统等级测评

在系统建设完成后，按照等级保护的要求选择国家认可的测评机构对信息系统进行等级测评，并在系统运行过程中定期进行测评，对于三级系统要求每年测评一次，对发现不符合相应等级保护标准要求的及时整改，并在发生重大变更或级别发生变化时进行等级测评。

3.3.4.7 服务投标单位选择

确保选择有相应资质的安全服务商、安全集成商、系统集成商和软件开发商，并与其签订协议，明确相关安全义务和责任。

3.3.5 安全运维管理

3.3.5.1 环境管理

本项目部署在省信创云机房，由信创云统一负责机房的安全管理工作。

3.3.5.2 资产管理

依托省信创云统一的数据资源管理平台，编制并定期更新与被保护对象相关的资产清单，包括各类硬件、软件、数据、介质、文档等，确定并标识资产责任部门、重要程度和所处位置等内容；根据资产的重要程度对资产进行标识管理，

针对重要信息资产制定专门的管理措施；对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

3.3.5.3 介质管理

需制定介质安全管理制度，规定介质的使用范围、介质标识、介质保存等方面的内容。对于单位介质，需将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

3.3.5.4 设备管理

对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

3.3.5.5 漏洞和风险管理

定期开展安全评估，形成评估报告，对发现的漏洞等安全问题及时通报，并限定整改时间；定期开展安全测评，形成安全测评报告，对发现的问题制定整改方案，采取措施应对发现的安全问题，相关内容形成记录。

3.3.5.6 网络和系统安全管理

（1）划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。可以指定专门的网络管理员、系统管理员、数据库管理员等，对网络设备、操作系统、数据库等进行专业化管理。

（2）指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。对重要服务器、数据库、业务应用等的管理账户应更加严格管理。

（3）建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、 日志管理 、日常操作、口令更新周期等方面作出规定；

（4）详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

（5）严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

（6）严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

3.3.5.7 变更管理

（1）明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

（2）建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

（3）建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

3.3.5.8 备份与恢复管理

（1）指定责任部门，识别需要定期备份的重要业务信息、系统数据及软件系统等；

（2）定义备份信息的备份方式、备份频度、存储介质和保存期等；

（3）根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略；

（4）建立备份和恢复流程，对备份过程进行记录，所有文件和记录应妥善保存；

3.3.5.9 安全事件处置

（1）及时向安全管理部门报告所发现的安全弱点和可疑事件；在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

（2）制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

（3）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

3.3.5.10 外包运维管理

（1）确保外包运维服务商的选择符合国家的有关规定，与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

（2）保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

（3）在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求等。

五、密码应用服务需求

1.设计目标及原则

1.1 设计目标

陕西省智慧教育综合服务平台（一期）主要用于教育资源服务、教育教学管理、校园安全管控、政务事项办理等工作。业务信息主要包括教育行业组织机构信息、师生个人身份信息、教学科研信息、视频监控信息等。一旦平台应用遭到破坏或系统数据遭到泄露和篡改，会严重侵害社会秩序和公共利益，因此需要技术和管理等方面来设计平台的密码应用体系。

根据 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》以及《政务信息系统密码应用与安全性评估工作指南》的相关要求，本项目需要符合信息系统密码应用第三级的要求，从物理和环境安全、网络和通信安全、设备和计算要求、应用和数据安全等技术层面和管理制度、人员管理、建设运行和应急处置等管理层面来规范平台的密码应用。

本项目部署在陕西省政务云平台，物理环境、网络、计算、存储等方面的密码应用基础设施由政务云平台统一提供，不再单独建设。本项目依托政务云平台环境，主要完成应用和数据的密码应用和密码安全管理体系的建设，并定期开展密码应用安全性评估，全面提升陕西省智慧教育综合服务平台的整体安全性。

1.2 设计原则与依据

1.2.1 设计原则

（1）总体性原则。密码在信息系统中的应用不是孤立的，必须与信息系统的业务相结合才能发挥作用。密码应用方案应做好顶层设计，明确应用需求和预期目标，与信息系统整体网络安全保护等级相结合，通过系统总体方案和密码支撑总体架构设计来引导密码在信息系统中的应用。

（2）科学性原则。在密码应用方案设计中，不能简单的对照《信息系统密码应用基本要求》中的每项要求堆砌密码产品，应通过成体系、分层级的设计，形成包括密码支撑总体架构、密码基础设施建设部署、密钥管理体系构建、密码产品部署及管理等内容的总体方案。

（3）完备性原则。密码应用设计方案设计应在密码技术应用（包含物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面）和密钥管理、安全管理等方面满足相关要求。

（4）可行性原则。密码应用方案设计需进行可行性论证，在保证信息系统业务正常运行的同时，综合考虑信息系统的复杂性、兼容性及其他保证措施等因素，保证方案切合实际、合理可行。

1.2.2 设计依据

（1）GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

（2）GB/T32907-2016《信息安全技术 SM4 分组密码算法》

（3）GB/T32905-2016《信息安全技术 SM3 密码杂凑算法》

（4）GB/T32915-2016《信息安全技术 二元序列随机性检测方法》

（5）GB/T33560-2017《信息安全技术 密码应用标识规范》

（6）GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》

（7）GB/T35291-2017《信息安全技术 智能密码钥匙应用接口规范》

（8）GM/T0017-2012《智能密码钥匙密码应用接口数据格式规范》

（9）GB/T36322-2018《信息安全技术 密码设备应用接口规范》

（10）GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》

（11）GM/T0019-2021《通用密码服务接口规范》

（12）GM/T0024-2014《SSL VPN 技术规范》

（13）GM/T0025-2014《SSL VPN 网关产品规范》

（14）GM/T0026-2014《安全认证网关产品规范》

（15）GM/T0027-2014《智能密码钥匙技术规范》

（16）GB/T37092-2018《信息安全技术 密码模块安全要求》

（17）GM/T0033-2014《时间戳接口规范》

（18）GB/T38635.1-2020《信息安全技术 SM9 标识密码算法 第 1 部分：

总则》

（19）GB/T38635.2-2020《信息安全技术 SM9 标识密码算法 第 2 部分：数字签名算法》

（20）GM/T0044.1-2016《SM9 标识密码算法 第 1 部分：总则》

（21）GM/T0044.2-2016《SM9 标识密码算法 第 2 部分：数字签名算法》

（22）GM/T0044.3-2016《SM9 标识密码算法 第 3 部分：密钥交换协议》

（23）GM/T0044.4-2016《SM9 标识密码算法 第 4 部分：密钥封装机制和公钥加密算法》

（24）GM/T0044.5-2016《SM9 标识密码算法 第 5 部分：参数定义》

（25）GM/T0057-2018《基于 IBC 技术的身份鉴别规范》

（26）GM/Z4001-2013《密码术语》

（27）《GB/T 15843.3-2016 信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制（ISO/IEC 9798-3：2010，IDT）》

（28）《GB/T 15843.3-2016 信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制（ISO/IEC 9798-3：2010，IDT）》

（29）GB/T 31072-2014《统一身份认证规范 》

（30）GB/T16263.1-2006《信息技术 ASN.1 编码规则第一部分：BER、DER、CER 规范》

2.密码应用技术方案

2.1 密码应用技术框架

陕西省前期基于省政务云平台建设密码服务基础设施，已经构建陕西省省直部门电子政务外网的密码服务平台，通过提供统一、标准、规范、便利、安全、可扩展、易维护的密码服务，满足陕西省政务信息系统的密码应用需求。

本项目部署在陕西省信创云平台上，物理环境、网络、计算、存储等方面的密码应用基础设施由政务云平台统一提供，不再单独建设。依托信创云环境下PKI/CA、服务器密码机、签名/验签服务器等密码基础设施和统一密码服务平台提供的身份识别、安全隔离、信息加密、完整性保护等方面的服务，主要完成应用和数据的密码应用和密码安全管理体系的建设，实现身份认证、数据加解密、签名验签、密钥管理等密码安全应用，保障系统应用及重要数据的机密性、完整

性和操作行为的抗抵赖性，全面提升陕西省智慧教育综合服务平台的整体安全性。

2.2 物理和环境安全

2.2.1 密码保护对象

物理和环境安全保护的对象是信创云平台上的陕西省智慧教育综合服务平台所在机房区域的物理安全。

2.2.2 采用的密码措施

对应物理和环境安全性的密码应用主要有两方面：

一是采用基于国密技术的电子门禁系统和视频监控系统，对重要物理区域（如计算机集中办公区、设备机房等）出入人员的身份进行鉴别。

二是对电子门禁系统进出记录、视频监控音像记录等数据进行完整性保护。

本项目依托省信创云平台部署，省信创云平台所处的机房区域已具备进出机房的人员身份真实性、电子门禁系统进出记录数据的存储完整性、视频监控音像记录数据的存储完整性等安全性，无需重复建设。

2.2.3 密码应用配置表

指标要求	密码技术应用点	采取措施	说明
物理和环境安全	身份鉴别	由省信创云平台统一提供	由省信创云平台统一提供物理和环境安全
	电子门禁记录数据完整性	由省信创云平台统一提供	
	视频记录数据完整性		

2.3 网络和通信安全

2.3.1 密码保护对象

网络和通信安全保护的对象是信息系统与外部实体之间网络通信的安全防护，包括通信过程实体身份的真实性、通信数据机密性和完整性，以及网络边界访问控制和设备接入控制。

2.3.2 采用的密码措施

陕西省智慧教育综合服务平台 PC 端用户客户端部署符合密码相关国家、行业标准要求的安全浏览器密码模块、服务端部署符合密码相关国家、行业标准要求的国密 SSL VPN 安全网关，构建 HTTPS 国密安全传输通道，对通信方进行身份鉴别，对系统应用的重要数据在传输过程中的机密性、完整性保护，对 SSL VPN

安全网关中访问控制信息进行完整性保护。

陕西省智慧教育综合服务平台移动端 APP 中部署符合密码相关国家、行业标准要求的 SSL 密码模块(二级)、服务端部署符合密码相关国家、行业标准要求的国密 SSL VPN 安全网关，建立移动端 APP 安全的数据传输通道，对通信方进行身份鉴别服务，对通信信道中数据的机密性和完整性进行保护。

网络和通信安全层面使用密码算法、密码技术、密钥管理由符合 GM/T0025-2014《SSLVPN 网关产品规范》、GM/T0028-2014《密码模块安全技术要求》的安全接入网关（SSL VPN）、安全浏览器密码模块、SSL 密码模块（二级）实现。

2.3.3 密码应用配置表

指标要求	密码技术应用点	采取措施	说明
网络和通信安全	身份鉴别	使用信创云 SSL 认证服务实现在通信前的身份鉴别和设备接入认证，保证通信实体身份的真实性	无
	访问控制信息完整性	由信创云统一提供网络边界访问控制信息的完整性保护	无
	通信数据完整性	在 PC 端使用安全浏览器，在 APP 端部署 SSL 密码模块，与服务端 SSL VPN 安全网关之间建立 HTTPS 安全传输通道，传输过程中采用 SM3 算法对数据完整性进行保护，使用 SM4 算法对数据机密性进行保护	无
	通信数据机密性		无
	集中管理通道安全	由信创云对外部连接到内部网络的设备进行接入认证，确保接入设备真实性	无

2.4 设备和计算安全

2.4.1 密码保护对象

设备和计算安全保护的对象是通用服务器及网络安全设备，从而保障计算设备的身份鉴别、远程管理通道安全、系统资源访问控制信息完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性。

2.4.2 采用的密码措施

给运维管理人员配发智能密码钥匙，进行登录认证，防止非授权人员非法登录、访问，降低身份鉴别安全风险。在运维 PC 端安装安全接入网关客户端，先登录 SSL VPN 安全网关（位于堡垒机之前）后，再访问安全设备、服务器设备，

实现远程运维管理的身份鉴别和远程管理通道安全。

对于访问控制信息完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性，则调用统一密码服务平台的签名验签接口，执行 SM3 杂凑算法和 SM2 非对称密码算法。

（1）身份鉴别

通过在系统运维管理人员的 PC 上安装省级统一 SSL VPN 安全接入网关客户端，并向系统管理员配发 USB Key，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传输机密性保护，防止非授权人员登录、管理员远程登录身份鉴别信息被非授权窃取。

（2）远程管理通道安全

当运维人员进行远程管理设备时，通过采用省级统一 SSL VPN 安全接入网关，为用户端与服务端之间建立国密 SSL 安全传输通道，对信息传输进行机密性保护，防止非授权人员窃取或篡改运维数据。

（3）系统资源访问控制信息完整性

调用统一密码服务平台的签名验签接口，执行 SM3 杂凑算法和 SM2 非对称密码算法，对存储的系统资源访问控制信息进行完整性保护。

（4）敏感标记完整性

平台计划采用国产操作系统，不存在敏感标记。

（5）日志记录完整性

调用统一密码服务平台的签名验签接口，执行 SM3 杂凑算法和 SM2 非对称密码算法。

（6）重要可执行程序完整性、重要可执行程序来源真实性

重要可执行程序真实性完整性保护，通过调用省级密码服务平台的签名验签服务接口，基于数字签名的方式实现。本次暂不涉及此项需求。

2.4.3 密码应用配置表

指标要求	密码技术应用点	采取措施	说明
计算和设备安全	身份鉴别	向运维管理人员配发 USB Key，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传	无
	远程管理身份鉴别信息机密性		无

		输机密性保护.	
	访问控制信息完整性	调用统一密码服务平台的签名验签接口，执行 SM3 杂凑算法和 SM2 非对称密码算法。	无
	敏感标记的完整性	/	平台计划采用国产操作系统，不存在敏感标记
	日志记录完整性	调用统一密码服务平台的签名验签接口，执行 SM3 杂凑算法和 SM2 非对称密码算法。	
	重要程序或文件完整性	/	本项目不涉及重要可执行程序完整性和来源真实性

2.5 应用和数据安全

2.5.1 密码保护对象

应用和数据安全主要是实现对信息系统中应用及其数据的安全防护，应具备的密码功能包括应用的用户身份鉴别、访问控制，以及应用相关重要数据的存储安全、传输安全和相关行为的不可否认性。其中，重要数据包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信

类别	对象	描述	密码应用需求
实体身份	平台系统管理员	系统管理员	真实性
	平台用户	平台用户	真实性
访问控制信息	平台系统访问控制信息	系统访问控制策略表/文件	完整性
重要数据	鉴别数据	用户的登录口令等	传输机密性 传输完整性 存储机密性 存储完整性
	日志数据	日志类型包含人员登录、密码修改、人员导入、批量编辑。	完整性

息等。保护对象及其密码应用需求如下：

2.5.2 采用的密码措施

（1） 身份鉴别

采用经过了国家密码管理部门核准或经商用密码认证机构认证合格的密码产品，所使用的密码算法符合密码相关国家标准和行业标准，对用户实施有效的身份鉴别。为用户颁发内置数字证书的且符合 GM/T 0027-2014《智能密码钥匙技术规范》的智能密码钥匙，通过数字证书鉴别用户身份。互联网用户使用用户名、口令和短信的方式访问，应对登录的用户进行身份标识和鉴别，身份标识信息具有唯一性，身份鉴别信息具有复杂性并定期更换。

（2） 访问控制信息和敏感标记完整性

调用统一密码服务平台签名验签服务，对用户访问控制权限列表进行 SM2 数字签名，实现访问控制信息的完整性保护，保护访问控制权限列表不被篡改，防止非授权的访问。

（3） 数据传输机密性

对业务系统中重要数据在传输过程中进行正确和有效的保护，包括在网络通信安全层面搭建安全通信链路，以及业务系统应用层进行数据传输的保密性防护。数据传输机密性通过调用省级统一 SSL VPN 安全接入网关实现。

（4） 数据传输完整性

对业务系统中重要数据在传输过程中的完整性进行保护，除在网络和通信层面搭建安全通信链路以外，还应在应用层利用 MAC（消息认证码）或数字签名等技术保障重要数据在传输过程中的完整性。数据传输完整性，通过调用省级统一 SSL VPN 安全接入网关实现。

（5） 数据存储机密性

调用统一密码服务平台实现 SM4 算法，对系统重要数据进行签名，保证重要数据存储过程中的机密性、完整性保护，防止拖库、被篡改等。

（6） 数据存储完整性

调用统一密码服务平台实现 SM3 杂凑算法和 SM2 非对称密码算法，对系统重要数据进行签名，保证重要数据存储过程中的机密性、完整性保护，防止拖库、被篡改等。

（7） 日志记录完整性

调用统一密码服务平台的签名验签接口，执行 SM3 杂凑算法和 SM2 非对称密码算法。重要应用程序的加载和卸载

仅有运维人员可以对重要应用程序进行加载和卸载，运维人员的身份鉴别在“设备和计算安全”层面完成。

2.5.3 密码应用配置

指标要求	密码技术应用点	采取措施	说明
应用和数据安全	身份鉴别	为用户颁发内置数字证书的且符合 GM/T 0027-2014《智能密码钥匙技术规范》的智能密码钥匙，通过数字证书鉴别用户身份。互联网用户使用用户名、口令和短信的方式访问。	无
	访问控制信息和敏感标记完整性	调用统一密码服务平台签名验签服务，对用户访问控制权限列表进行 SM2 数字签名，实现访问控制信息的完整性保护。	无
	数据传输机密性	数据传输机密性通过调用省级统一 SSL VPN 安全接入网关实现。	无
	数据存储机密性	调用统一密码服务平台实现 SM4 算法，对系统重要数据进行签名，保证重要数据存储过程中的机密性、完整性保护，防止拖库、被篡改等。	无
	数据传输完整性	数据传输完整性，通过调用省级统一 SSL VPN 安全接入网关实现。	无
	数据存储完整性	调用统一密码服务平台实现 SM3 杂凑算法和 SM2 非对称密码算法，对系统重要数据进行签名，保证重要数据存储过程中的机密性、完整性保护，防止拖库、被篡改等。	无
	日志记录完整性	调用统一密码服务平台的签名验签接口，执行 SM3 杂凑算法和 SM2 非对称密码算法。	无

指标要求	密码技术应用点	采取措施	说明
	重要应用程序的加载和卸载	仅有运维人员可以对重要应用程序进行加载和卸载，运维人员的身份鉴别在“设备和计算安全”层面完成。	无

2.6 密钥管理

密钥是密钥管理系统的核心。在密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复、销毁等整个生命周期过程中，都需要通过密码技术对密钥进行保护，以确保密钥的全生命周期安全。保存在核准的密码产品中的密钥在本地存储，不进行传输；其他密钥一般采用离线方式或在线方式进行传输，并配以机密性和完整性保护措施。

本项目中平台使用国家标准中规定的国产密码算法和签名验证技术，保证管理、存储省政务云统一密码服务平台密钥信息时的真实性、完整性、不可否认性。所涉及到的国产密码算法包括对称算法 SM1、非对称算法 SM2、杂凑算法 SM3、分组加密算法 SM4 等，基础软件包括数字证书认证系统 CA、密钥管理系统 KMS 等。

2.6.1 密钥生成

密钥生成的方式，包括随机数直接生成或者通过密钥派生函数生成，其中用于产生密钥的随机数发生器应为经过国家密码管理部门核准的。密钥均应在核准的密码产品内部生成，在密钥生成时，伴随生成对应的密钥控制信息，包括但不限于密钥拥有者、密钥用途、密钥索引号、生命周期起止时间等。

2.6.2 密钥存储

密钥存储由两种安全的方式，一种是加密存储在外部介质中，另一种是保存在核准的密码产品中。对于一些信任根，如根密钥、设备密钥、主密钥等，若无法进行加密存储，则存储在核准的密码产品中，使用核准的密码产品自身提供的物理防护功能来保证存储密钥的安全。应急处理和响应措施包括停止原密钥使用、暂停业务系统服务、更新密钥等措施。

2.6.3 密钥分发

密钥分发主要用于不同密码产品间的密钥共享。对于根密钥的分发，采用离

线分发。由于本项目涉及人的参与，离线分发过程需要对相关实体进行身份鉴别，在线分发则可借助数字信封、对称加密等方式实现密钥的安全分发。

2.6.4 密钥导入与导出

对密钥的导入与导出，应严格按照密码产品管理要求由专门的密码管理人员操作，采用加密、知识拆分等方法保证密钥导入、导出的安全性。密钥的导入和导出主要是指密钥从密码产品中进出，既可以在同一个密码产品中进行密钥的导入和导出，也可以将密钥从一个密码产品中导出后导入到另一个密码产品中。为了保证密钥的安全性，密钥一般不能明文导出到密码产品外部。此外，在密钥导入和导出过程中，应当确保系统的密码服务不间断，即不影响密码服务的正常运转。

2.6.5 密钥使用

对于用于公钥解密的私钥和签名的私钥要明确区分，并按照当初设定的用途规范使用这些密钥。不同类型的密钥不能混用，一个密钥不能用于不同用途。例如，用于保密性保护的对称密钥一般不能再用于完整性保护，用于加密和签名用途的公私钥对要进行明显区分。第一次使用公钥前，应当对证书的有效性进行验证。对于密码产品操作手册中有明确更换周期的密钥，要按照操作手册中的要求进行更换。

2.6.6 密钥备份与恢复

信息系统应当根据自身的安全需求制定密钥备份的策略，特定情况下还可采用密码产品自身提供的密钥导出和导入功能进行密钥的备份和恢复，但必须确保备份和恢复机制的安全性。密钥备份和恢复的操作应在密码产品内留存由日志记录信息。

2.6.7 密钥归档

密钥归档是对不再使用的密钥分类记录并安全保存的管理过程。通过制定密钥归档操作规程，保证归档密钥的安全性和正确性。密钥归档的操作应当被安全管理员记录，并在密钥设备中生成日志记录。归档后的密钥应当进行备份以防止存储设备故障或丢失，并应当采用必要的访问控制措施保证归档密钥的安全性。

2.6.8 密钥销毁

一般情况下，密钥在到达设计的使用时限时，将自动进行销毁。在紧急情况

下，有两种密钥销毁方式：一种是由密码产品自身进行自动销毁，例如，在符合GM/T0028-2014要求的三级及以上密码模块中均具有拆卸响应功能，即当模块检测到外界入侵后将自动销毁密码模块内的密钥和其他敏感安全参数；另一种是需要人工执行销毁操作，操作员发现密码产品被入侵后可手动执行密钥销毁操作。信息系统应当根据自身的安全需求，指定密钥的销毁策略和操作规程，尤其是针对那些没有拆卸响应功能的密码产品所保存的密钥。

2.7 密码应用部署

依托陕西省政务云平台，采用密码机建立统一的密码硬件支撑平台，建立统一CA数字证书系统、密钥管理系统、电子签章、签名验签服务器、统一认证等实现云上业务应用的身份认证、数据加密、完整性保护等。

2.8 安全与合规性分析

指标要求	**密码技术应用点**	**采取措施**	**标准符合性**（符合/不适用）	**说明**（针对不适用项说明原因及替代性措施）
物理和环境安全	身份鉴别	由省信创云平台统一提供物理和环境安全。	/	
	电子门禁记录数据完整性		/	
	视频记录数据完整性		/	
	密码模块实现		/	
网络和通信安全	身份鉴别	使用信创云SSL认证服务实现在通信前的身份鉴别和设备接入认证，保证通信实体身份的真实性。	符合	
	访问控制信息完整性	由信创云统一提供网络边界访问控制信息的完整性保护。	符合	

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
	通信数据完整性	传输过程中采用 HMAC-SM3 算法对数据完整性进行保护。	符合	
	通信数据机密性	使用 SM4 算法对数据机密性进行保护。	符合	
	集中管理通道安全	由信创云对外部连接到内部网络的设备进行接入认证，确保接入设备真实性。	符合	
	密码模块实现	利用信创云 SSL VPN 网关实现。	符合	
设备和计算安全	身份鉴别	向运维管理人员配发 USB Key，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传输机密性保护。	符合	
	远程管理身份鉴别信息机密性	向运维管理人员配发 USB Key，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传输机密性保护。	符合	
	访问控制信息完整性	调用统一密码服务平台的签名验签接口，执行 HMAC 或 Hash、数字签名的密码计算。	符合	
	敏感标记的完整性	/	不适用	平台计划采用国产操作系统，不存在敏感标记
	日志记录完整性	调用统一密码服务平台的签名验签接口，执行 HMAC 或 Hash、数字签名的密码计算。	符合	

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
	重要程序或文件完整性	/	不适用	本项目不涉及重要可执行程序完整性和来源真实性
	密码模块实现	依托省政务云平台的密码模块、服务器密码机。	符合	
应用和数据安全	身份鉴别	为用户颁发内置数字证书的且符合 GM/T 0027-2014《智能密码钥匙技术规范》的智能密码钥匙，通过数字证书鉴别用户身份。互联网用户使用用户名、口令和短信的方式访问。	符合	
	访问控制信息和敏感标记完整性	调用统一密码服务平台签名验签服务，对用户访问控制权限列表进行 SM2 数字签名，实现访问控制信息的完整性保护。	符合	
	数据传输机密性	数据传输机密性通过调用省级统一 SSL VPN 安全接入网关实现。	符合	
	数据存储机密性	调用统一密码服务平台实现 SM3 杂凑算法和 SM2 非对称密码算法，对系统重要数据进行签名，保证重要数据存储过程中的机密性、完整性保护，防止拖库、被篡改等。	符合	
	数据传输完整性	数据传输机密性通过调用省级统一 SSL VPN 安全接入网关实现	符合	

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
	数据存储完整性	调用统一密码服务平台实现SM3杂凑算法和SM2非对称密码算法，对系统重要数据进行签名，保证重要数据存储过程中的机密性、完整性保护，防止拖库、被篡改等。	符合	
	日志记录完整性	调用统一密码服务平台的签名验签接口，执行HMAC或Hash、数字签名的密码计算。	符合	
	重要应用程序的加载和卸载	仅有运维人员可以对重要应用程序进行加载和卸载，运维人员的身份鉴别在“设备和计算安全”层面完成。	符合	
	密码模块实现	依托安全浏览器、信创云的SSL VPN安全网关、电子印章系统、服务器密码机、时间戳服务器和CA系统实现。	符合	

3.密码安全管理方案

密码安全管理体系从管理制度、人员管理、建设运行以及应急处置四个方面制定安全管理方案。

3.1管理制度

管理制度的制定是密码安全管理的重要手段，为了提高系统及相关设施的安全及平稳运行，制定包含密码人员管理、密钥管理、建设运行、应急处置以及介质管理的管理制度，经各级部门审批后下发。对于密钥的管理，制定包含密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等保障密钥全生命周期安全性的管理制度。同时明确各级管理人员及操作人员的操作规程，指导日常工作的开展。

制度编制完成后应结合省厅制度管理相关办法，对制度的修订、发布、版本控制、记录管理等内容进行管理。

3.2 人员管理

首先，梳理相关岗位人员业务及职责，结合业务内容制定相应的密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限，新编制的制度在试运行一段时间后，可以合并到原有岗位职责中，将密码安全责任固化到各个岗位中。

其次，建立培训及评价管理制度。制度中明确培训的要求、内容、时间及培训效果评价等相关内容，实施定期专业学习培训与计划性按需培训，培训结束后通过现场提问、考试等形式进行效果评价。

在信息化考核管理制度中新增密码应用安全考评相关指标项点。同时与关键人员签订保密协议。

3.3 建设运行

投入运行前，依照密码相关标准梳理密码应用需求，制定密码应用方案，经过评审以后制定密码应用实施方案。邀请外部测评机构从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度五个方面对密码应用进行安全性评估并出具密评报告，经过测评的系统方能正式上线运行。

依据密码应用管理制度实施运行控制，定期开展安全性评估工作，不断整改完善，保证信息系统的安全及平稳运行。

3.4 应急处置

制定密码应用应急处置方案，明确应急处理组织体系，明确应急事件的等级及应急处置流程，制定相关应急预案。成立由应急决策小组、应急指挥小组、应急执行小组及应急保障小组共同组成的应急管理组织体系，各小组由应急决策小组统一管理和调度。应急预案应包括组织人员、信息传递流程及方式、时间处置程序、内外部沟通机制及联系方式等内容。同时对于应急预案应进行日常演练，检验应急预案的完整性、可操作性和有效性，提高应急事件发生后的综合处置能力。应急事件的分级一般根据事件的影响大小分为特别重大事件（一级）、重大事件（二级）、较大事件（三级）、一般事件（四级）。

六、项目管理服务

项目建设涉及到的环节较多，在前期设计、项目实施与试运行过程中需要多方参与，对项目的管理提出了较高的要求，所以健全项目管理机制，制定项目管理制度、管理办法以及质量要求制度，可有效的促进项目最佳实践，实现项目效益最大化，支撑未来数年甚至更长时间的业务发展需要。

项目建设过程中应遵循的管理制度和质量要求(不限于)如下：

a 项目建设单位应当确定项目责任人，建立健全各种所需项目管理规范，加强对项目全过程的统筹协调，强化信息共享和业务协同，并严格执行招标投标、政府采购、合同管理等制度。招标采购涉密信息系统的，还应当执行保密有关法律法规规定；

b 项目建设单位应当按照《中华人民共和国网络安全法》等法律法规、党政机关及教育部门网络安全管理等有关规定，建立网络安全管理制度，采取技术措施，加强信息系统与信息资源的安全保密管理，定期开展网络安全检测与风险评估，保障信息系统安全稳定运行；

c 项目采用安全可靠的软硬件产品。在具体实施过程报批阶段，要对产品的安全可靠情况进行说明。项目软硬件产品的安全可靠情况，网络安全审查情况是项目验收的重要内容；

d 项目建设单位充分依托陕西省政务云资源开展集约化建设；

e 符合要求的大型信息化项目实行工程监理制。

六.项目管理

1.项目进度管理

1.1 进度管理的主要任务

项目进度管理对项目进度进行跟踪控制，以保证项目按照预先设定的计划轨道行驶，使项目不要偏离预定的发展进程。对项目的跟踪控制是项目实施机构的反馈过程，要在项目实施的全过程对项目进行跟踪控制。

（1）制定完整周密的项目工作计划

制定完整周密的项目工作计划，明确各任务的依赖关系，合理规划和安排任务的时间进度、编排方式。

（2）严格执行项目时间进度计划

严格执行项目工作计划，明确关键里程碑，保证工程和项目严格按照时间进度计划进行。

①对项目进行跟踪控制。

②明确项目完成应达到的目标，建立项目监控和报告体系，确定为控制项目所必需的数据。

1.2 项目进度表

为本项目制定严谨的项目建设与实施进度表，作为控制整个项目进程的指导性文件，将作为度量和报告项目进度执行情况的重要手段。

1.3 项目进度计划管理

进度计划管理对进度的改变应加以控制和管理。在项目实施过程中，可能会出现各种影响项目进度的因素。根据这些实际情况的需要，根据进度控制的工具和方法，制订出针对这些改变的进度管理计划，作为整个项目计划的一部分。

1.4 项目进度更新

根据本项目实际进度与计划进度比较分析结果，以保持项目工期不变、保证项目质量和所耗费用最少为目标，做出有效对策，进行项目进度更新，这是进行进度控制和进度管理的宗旨。项目进度更新主要包括两方面工作，即分析进度偏差的影响和进行项目进度计划的调整。

1.5 阶段性评估

项目运行包括各个阶段，在不同阶段，需要各个部门配合完成不同的工作。任何一个环节出现问题，都会影响到后续工作的进行。所以，明确各个阶段的任务和双方职责，促进项目的顺利执行。

对项目实施进行阶段性评估，小结项目的实施是否按计划进行并达到所期望的阶段性成果，如果出现偏差，研究是否需要更新计划及资源，同时落实所需的更新措施。

项目的进度是否能够按照设计规划的进行是影响项目效果的关键因素，所以评估项目的成功与否，首先必须评估项目的进度是否按照预期的进度进行，如果每一步或者每一阶段，都能够严格的按照进度进行，项目一定会成功，否则就是项目设计出现了问题。

1.6 比较与分析

将项目的实际进度与计划进度进行比较分析，以评判其对项目工期的影响，查找实际进度与计划不相符合的原因，进而找出对策，这是进度控制的重要环节之一。

1.7 项目需求变更控制

进度变更的形式有多种：口头或书面、直接或间接、由外部或内部因素导致的、强制性的或有多种选择的。这些具体的改变要求的结果可能是加快进度，也可能导致进度拖延。

变更控制不能仅在过程中靠流程控制，有效的方法是在事前明确定义。事前控制的一种策略是在项目开始前明确定义，否则“变化”也无从谈起。另一种策略是评审，特别是对需求进行评审，这往往是项目成败的关键。需求评审的目的不仅是“确认”，更重要的是找出不正确的地方并进行修改，使其尽量接近“真实”需求。另外，需求通过正式评审后应作为重要基线，从此之后即开始对需求变更进行控制。

要在项目开始就对项目组和客户进行宣传和培训，让所有成员都理解变更控制的重要意义；在项目过程中要对变更控制的执行情况进行审计，发现违反规定的事件要严肃处理，否则过程很快就会失效。

变更控制的目的是管理变化。变更控制对项目成败有重要影响，其核心策略是事前要明确定义、事中要严格执行。实施变更之前有四个重要控制点：授权、审核、评估和确认。在实施过程要进行跟踪和验证，确保变更被正确执行。

在本项目的实施过程中，对于合理的变更、扩展、替换或修改要求，将采取一定的项目变更控制方法进行处理，以保证项目的进度和质量。为了如期完成既定的项目开发、部署、实施等任务，需对项目变更进行管理和控制，确保项目变更不影响相关任务的执行。

2.项目质量管理

2.1 质量保证体系标准

本项目将借鉴先进的质量管理模式和科学的质量管理体系与流程，根据项目周期和管理特点选用合适的质量控制规程。目前，主要采用 ISO9001 质量标准和系统集成软件成熟度模型（CMMI）两种控制规程。本项目需采用 ISO9001：2000

质量体系标准，同时遵循 CMMI 的相关标准进行系统集成质量控制，项目实施过程将严格执行这些质量标准。

2.2 质量管理措施

质量管理主要包括两个过程：质量计划制定和质量控制。

（1）质量计划：是质量管理的第一过程域，它主要指依据相关的质量方针、产品描述以及质量标准和规则等制定出来实施方略，其内容全面反应用户的要求，为质量小组成员有效工作提供了指南，为项目小组成员以及项目相关人员了解在项目进行中如何实施质量保证和控制提供依据，为确保项目质量得到保障提供坚实的基础。

（2）质量控制：是贯穿整个项目全生命周期的有计划和有系统的活动，经常性地针对整个项目质量计划的执行情况进行评估、检查与改进等工作，向管理者、顾客或其他方提供信任，确保项目质量与计划保持一致。是对阶段性的成果进行测试、验证，为质量保证提供参考依据。

2.3 质量管理规范

本项目将采用 ISO9001 质量体系认证和软件能力成熟度 CMMI 质量管理体系规范，对项目的过程实现全面的跟踪与监督管理。

2.4 项目级质量控制措施

项目质量的控制贯穿于整体项目，从项目的策划，到项目的评审、设计、实施，至始至终融入质量保证要求。在本项目的建设中，实行如下质量控制措施。

（1）项目策划质量控制措施

①对每一项项目任务制定设计计划，划分设计阶段，规定每一阶段的设计任务，开展的质量活动及控制措施和验证方法等；

②编制的设计计划可确保前一阶段的活动未达到要求，不能转入下一阶段；

③设计人员应按相应的设计，实验规范开展设计、实验工作，并依此作为控制和评价设计工作的准则；

④设计人员应运用优化设计和可靠性、可维护性技术，开展设计工作；

⑤执行设计文档和技术文件的审查制度，保证设计质量满足规定要求。

（2）设计评审质量控制措施

①在设计的适当阶段，有计划地对设计结果进行正式评审，评审结果应形成文件并予以保存；

②根据项目的功能级别和管理级别，实施分级、分阶段设计评审合同要求时，应邀请用户方或其他代表参加评审；

③每次评审的参加者包括与被评审的设计阶段有关的所有职能部门的代表，需要时也包括其他专家。

（3）项目实施质量控制措施

项目实施中的质量管理工作是非常复杂的，存在很多不可以控制的因素，因此，在项目实施阶段根据 ISO9001、CMMI 等质量保证体系标准，需要设计多种质量管理措施。

（4）项目验收质量控制措施

①验收预检

验收预检是单位工程在正式验收前一次全面检查，对存在的问题没有全部解决前，不得报请验收。预检条件如下：

a 各系统分项工程基本完成。

b 各系统设备安装、调试完毕，达到试运行。

c 竣工技术档案资料基本齐全。

②项目验收

项目验收是在修复验收预检存在的问题基础上，由项目经理部并报请甲方进行交付使用前的正式验收。项目验收所具备的条件如下：

a 验收预检时提出的问题全部解决。

b 各分系统试运行达到设计要求并具备甲方使用条件。

c 各系统工程技术资料齐全，全部分类整理装订线册，可移交给甲方。

2.5 过程级质量控制措施

对软件产品的质量控制贯穿于开发的全过程，针对本项目主要采取以下措施和方法进行控制和管理：

（1）制定质量保证计划

质量保证计划就是为了实现质量目标的计划，而质量目标则是由商业目标决定的，开发软件产品的最终目的是为了赚钱，所以人们为提高软件质量所付出的

代价是有上限的，项目负责人当然希望在保证软件质量的基础上，成本越低越好，质量保证计划是全面质量管理的行动纲领，QA 人员在裁剪原则指导下，对组织的标准过程进行裁剪，形成项目标准过程。

（2）组织正式技术评审

技术评审的目的是尽早地发现工作成果中的缺陷，并帮助开发人员及时消除，从而有效提高产品质量。在软件开发的每一个阶段结束时，都要组织正式的技术评审。国家标准要求单位必须采用审查、文档评审、设计评审、审计和测试等具体手段来保证质量。

（3）加强软件测试

软件测试是质量保证的重要手段，因为测试可发现软件中大多数潜在错误。

（4）进行过程检查

CMMI 和 ISO9001 所述的质量保证，实质就是过程检查，即检查软件项目的工作过程和工程成果是否符合既定的规范。符合规范的工作成果不见得就是高质量的，但是明显不符合规范的工作成果十有八九是质量不合格的。过程检查的要点是：找出明显不符合规范的工作过程和工作成果，及时指导开发人员纠正问题，切勿吹毛求疵或者在无关疼痒的地方查来查去。

（5）采用技术手段和工具

质量保证活动要贯彻开发过程始终，必须采用技术手段和工具，尤其是使用软件开发环境来进行软件开发。

（6）推行软件工程规范（标准）

用户可以自己制定软件工程规范（标准），但标准一旦确认就应贯彻执行。

（7）对软件的变更进行控制

软件的修改和变更常会引起潜伏的错误，因此必须严格控制软件的修改和变更。

（8）对软件质量进行度量

对软件质量进行跟踪，及时记录和报告软件质量情况。

（9）对质量保证活动相关的所有记录文档进行保存

需保存的文档有：QA 检查单、不符合项表、质量保证报告、质量保证审计报告、各项评审记录等。质量保证小组在项目组专用的服务器上建立目录进行保

存，并分配相关权限给各项目干系人，由公司指定 QA 人员及时对保存的文档进行更新和维护。项目各阶段产生的文档，在每个阶段结束后由相应责任人提交给项目管理专责归入公司过程资产库存档。

2.6 产品级质量控制措施

本项目将采用以下三种方式来确保软件产品的质量：

（1）质量保证：质量保证人员通过有计划地检查“工作过程和工作成果”是否符合既定的规范，来监控和改进“过程质量”与“产品质量”。

（2）技术评审：由同行专家、技术人员对工作成果进行评审，尽早发现工作成果的缺陷。

（3）产品测试：通过测试方案和运行测试用例，找出软件缺陷。例如：应用软件的单元测试、集成测试、系统测试、验收测试等。

3.项目资金管理

对投资进行合理配置和管理，保证投资得到最大限度的回报。

3.1 在系统设计上尽量实用，不让项目建设单位对于过于虚无或者不实用的功能或技术进行不必要的投资。

3.2 在项目管理中，保证项目的工期的按时完成，不耽误项目建设单位的计划时间和使用。避免在工期上拖延整个项目的实施，从而保证投资在规定的时间内实现。

4.项目绩效管理

开展事前绩效评估、绩效运行监控和项目绩效评价，评价发现项目存在建设方案部分内容不合理、项目缺乏详实实施计划等问题，积极探索推进项目绩效管理。

4.1 事前绩效评估：本项目具备专业性强、技术更新快、非独立性、系统涉及面广、安全性要求高、个性化显著等特点，事前绩效评估重点关注项目方案是否符合陕西省教育信息化管理整体布局以及数据存储要求实际、项目建设中技术应用是否细化应用场景、明确节点分配和存证内容等。通过成本效益分析、风险评估、专家论证等，为政府决策和预算安排提供科学依据。

4.2 绩效运行监控：通过对预算执行、项目建设进度等核心指标的跟踪及偏差度分析，及时发现政务信息化项目在建设过程中的管理漏洞和目标偏差，及时纠偏，优化项目绩效目标实现路径，强化项目执行过程管控。

4.3 项目绩效评价：针对项目专业技术性强、政府采购覆盖面达、受益对象广等特点，重点关注建设方案是否科学合理、业务办理效率和服务对象满意度是否提升等内容，采取定性和定量相结合等方式，既对项目建设完成、交付使用前进行构建质量、标准评价，又对项目投入运行使用效果评价，提出后续优化项目管理的可行性建议，提高项目管理精细化水平，提升资金使用效益。

5.相关管理制度

建立健全的管理工作制度是完成工程的重要保证，根据工程的特点和要求，制定以下管理制度。

5.1 系统实施方案、实施计划审查制度

项目建设单位在收到项目实施单位提供的《工程实施方案报审表》、《工程项目进度计划审核表》，在工程实施前，会同监理单位、项目实施单位复查设计方案及项目计划，广泛听取意见，避免设计中的差错和遗漏。

5.2 开工报审制度

当项目实施单位的准备工作已完成时，向监理单位和项目建设单位提出《工程开工报审表》，经监理单位和项目建设单位现场落实后，由总监理工程师签发《开工令》。

5.3 变更设计制度

如因错漏，或发现实际情况与设计不符时，由项目实施单位提出《工程变更单》，经项目建设单位、监理单位、项目实施单位会商同意后进行变更审查和确认，由三方代表在《工程变更》上签字。

5.4 工程质量管理制度

项目建设单位对项目实施单位的施工质量有监督管理责任。项目建设单位在检查工作中发现的工程质量缺陷，应责成监理方及时记录，指明质量部位、问题及整改意见，限期纠正复验。对较严重的质量问题或已形成隐患的问题，通知项目实施单位，同时要求项目实施单位应按要求及时做出整改，克服缺陷后通知项

目建设单位复验签认。如所发现工程质量问题已构成工程严重质量问题，应按合同规定条款办理。

5.5 工程质量检验制度

业主对项目实施单位的施工质量有监督管理的权利与责任。

（1）监理单位在检查工程中发现一般的质量问题，应随时通知项目实施单位及时改正，并做好记录。测试不合格时可发出《业主通知单》或《工程暂停令》，限期改正。

（2）如项目实施单位不及时改正，情节较严重的，监理单位可在报请项目建设单位批准后，发出《工程暂停令》，指令部分工程、单项工程或全部工程暂停施工。待项目实施单位改正后，报项目监理单位进行复验，合格后发出《复工令》。

（3）分部分项工程、单项工程或分段全部工程完工后，项目实施单位经自验合格，可填写《******（阶段）报验申请表》或《工程预验收/终验申请单》，经项目建设单位和监理单位现场查验后，发给《分项、分部工程检验认可书》或《竣工证书》。

（4）要求监理单位每周填写《监理周报》。

（5）项目建设单位需要承建单位执行的事项，除口头通知外，可使用《业主通知单》，催促项目实施单位执行。

5.6 工程质量事故处理制度

（1）凡在项目建设过程中，由于设计或安装原因，造成工程质量不符合规范或设计要求，或者超出验收标准规定的偏差范围，需做返工处理的统称“工程质量事故”。

（2）工程质量事故发生后，项目实施单位必须用电话或书面形式逐级上报。对重大的质量事故，监理单位应立即上报。

（3）凡对工程质量事故隐瞒不报，或拖延处理，或处理不当，或处理结果未经项目建设单位同意的，对事故部分及受事故影响的部分工程应视为不合格，不予验收，待合格后，再补办验收手续。

（4）项目实施单位应及时上报《质量问题报告单》，并应抄报项目建设单位和监理单位各一份；对于一般工程质量事故，由项目实施单位处理，填写事故

报告一份报本监理单位；对大质量事故，由项目实施单位填写《质量问题报告单》一式两份，由监理单位组织有关单位研究处理；对重大质量事故，由项目实施单位填写《质量问题报告单》一式三份，报项目建设单位和监理单位，由项目建设单位组织有关单位研究处理方案，报批准后，项目实施单位方能进行质量事故处理。待质量事故处理后，经监理方复查，确认无误，方可继续进行安装或开发。

5.7 工程进度监督及报告制度

（1）项目建设单位监督项目实施单位严格按照合同规定的计划进度组织实施，项目实施单位每周以工作周报的形式，向项目组报告各项工程实际进度及计划的对比和形象进度情况。

（2）项目建设单位审查项目实施单位编制的实施性组织设计，要突出重点，并使各单项、各工序进度密切衔接。

5.8 资金使用监督制度

（1）项目建设单位通过要求项目实施单位对工程实施方案及工程设计方案的优化，确保投资控制在预算之内。

（2）对项目出现重大设计变更或因新技术而增减较大投资的工程，项目实施单位应及时掌握并报项目建设单位，以便控制投资。

5.9 工程报告制度

项目实施单位按周编写《工作周报》，并于项目验收提出本项目的《工作总结报告》，报项目建设单位项目组。《工作阶段总结报告》或《工作周报》内容应具体说明施工进度、施工质量、资金使用，以及重大安全、质量事故、有价值的经验等。

5.10 工程竣工验收制度

（1）项目验收的依据是批准的设计文件，包括变更设计（系统集成项目为设计方案、设备采购清单及验收标准）、有关规范、工程质量验收标准以及合同及协议文件等。

（2）项目实施单位按规定编写和提出验收交接文件是申请验收的必要条件，验收文件不齐全、不正确、不清晰、不能验收交接。

（3）项目实施单位应在验收前将全部验收文件及技术文档，提供项目建设单位和监理单位各一份，审查确认完整后，报项目组，其余分发有关使用单位保管。

5.11 管理日记和会议制度

（1）项目建设单位要求项目实施单位应逐日将所从事的业务写入《工作日记》，特别是涉及设计、项目实施单位需要返工或改正的事项，应详细做好记录。

（2）在项目实施过程中，监理单位负责协调工程各方进行工程实施，并负责组织有关工程协调会议，建立项目实施单位、项目建设单位和监理单位的三方协调制度。

5.12 引入 ISO9001 质量保证体系

在工程的建设中引入 ISO9001 质量保证体系。质量体系将从建设单位的领导和管理职责开始，明确建设单位的质量方针和质量目标，规定与质量有关的各类人员职责，以及对各个开发环节建立起一套切实可行的管理规程。从建设单位的最高领导到第一线程序员都要无一例外地严格遵守执行，不仅如此，还要按规定做出相关的记录，随时准备接受审查和评审。

引入 ISO9001 质量保证体系，在项目建设中全面贯彻 ISO9001 质量体系，确定工程的总体质量目标和各阶段的质量目标，依据 ISO9001 质量体系的要求制订详细的质量保证计划，由专业项目管理人员进行有效的监控管理，保证系统顺利建设，达到预期目标。

5.13 落实项目档案管理制度

严格按照《国家电子政务工程建设项目档案管理暂行办法》（档发〔2008〕3 号）的管理规定，对项目建设过程中形成的、具有保存价值的各种形式和载体做好登记记录。项目建设单位在项目执行期间，落实相关档案管理人员，明确职责，制定档案工作计划，确保项目档案完整、系统、有效。

（1）概述本项目建设管理体制、方法、原则；

（2）提出项目建设的实施策略，例如项目会议制度、信息沟通制度、重大事项的决策制度等；

（3）分类介绍本项目各实施策略的具体内容。

6.技术力量和人员配置

为保证本项目的建设顺利进行，依项目实际需要配备强大的技术力量和专业技术人员队伍，要坚持少量、精干和满足需求的原则，并根据有关规定确定管理的方式和方法。专业技术人员队伍由项目管理办公室负责整体领导和建设，下设各个角色如下：

项目经理：由实施单位该项目负责人担任，全面负责项目监督、协调、组织等实施工作。

质量控制：由用户质量负责人和项目实施单位质量保障部门员工共同组成。负责检查监督施工组织设计的质量保证措施的实施，组织建立各级质量监督体系。

培训：联合相关的教育部门、开发单位及应用单位人才组建培训组，选拔培训人员，课程设计、培训材料准备、师资准备，按照项目培训计划和实际需求安排并执行培训相关工作。

验收：负责单体和系统的阶段验收、整体验收，负责完成不同层次的验收工作。

实施：由项目实施技术人员担任，在项目经理授权下全面负责项目执行安装、调试，系统部署等工作，并对实施过程文档进行核对、整理、收集，保证其完整性、准确性和可追溯性。

七、项目服务完成时限要求

根据本服务项目相关工作，咨询服务工作中相关规范、制度、方案设计于签订合同后 90 个日历日内完成；等级保护服务于 2023 年 6 月 30 日前完成；密码应用服务于 2023 年 6 月 30 日前完成；备份系统与备份服务于合同签订后 90 个日历日内建成备份系统，并开展备份工作；项目管理于本项目合同签订后立即开展相关工作，根据省教育厅安排限时完成。