信息化应用建设招标文件通用技术要求

项目验收技术复核标准

信息系统建设与运行维护技术规范

总则：

1.技术规范是规定产品、过程、服务应满足技术要求的文件。信息系统(网站)的安全贯穿软件系统的整个生命周期，学校各单位在建设与运行维护信息系统(网站)的整个过程中需遵守本技术规范。
2.信息系统(网站)的建设与运行维护应遵守“最小可用、不断更新”的总体原则。为确保信息系统(网站)安全运行，以最小可用的权限运行各种应用和数据库、以最小可用的原则定制各种配置参数和功能，禁止任何不必要的额外权限。网络安全技术日新月异，各种安全漏洞层出不穷，安全技术规范的内容必须与时俱进，满足“不断更新”的原则。

基础部署规范：

3.禁止采用失去技术升级支持，以及官方支持周期短于 3 年的操作系统，原则上禁用 Windows，禁用红帽及其所有衍生版 Linux，优先使用国产化 Linux，推荐 opencloudos/tencentos，其它开源操作系统版本选用宜具备通用性和广泛性。
4.数据库系统必须部署在 Linux，优先使用国产化数据库，其次使用开源数据库，原则上不使用国外商业数据库。
5.开发系统的编程语言、框架、依赖组件、第三方库等选用版本宜选用长期支持版，禁止使用已知存在漏洞和停止更新的技术，如 Struts2、jQuery、Flash、php、web 编辑器等。
6.上述所有软件选用版本在各个软件官网截图,自中标结果公示之日起不少于 4 年维护期(可升级，有官方技术支持)，并按季度对上述通用软件升级修补程序。
7.系统部署和运行均禁止连接互联网，涉及互联网连接的功能提交详细访问目的清单，经评估后以域名代理方式定向连接，通用升级和软件包下载通过校内镜像站完成。
8.服务器必须开启防火墙，端口开放最多不超过 2 个并严格限制访问的源 ip，web 服务只允许开放 1 个端口。
9.系统运行原则上不使用操作系统最高管理权限，并对相关服务按顺序配置开机自启动。
10.系统部署和运行遵循最小化原则，与系统运行无关以及非必要的软件、组件、工具、文档等均不得以测试、检测等理由安装或保存在服务器

开发设计规范：

10.整套系统必须在软件开发复杂度、硬件资源消耗、可扩展架构、业务逻辑优化、运维标准化等方面找到恰当的平衡点，所用服务器资源实行总量限制，禁止堆砌硬件式的水平扩展，数据库与应用一般同节点部署，初始资源分配 2vcpu、4GB 内存和 100G 磁盘，按业务实际负载优化程序代码，动态调增经评估后最大不超过 4vcpu、16GB 内存，非结构化增量文件合理存放到 nfs 卷。
11.所用技术架构不得内嵌 k8s 等相似的超越独立虚机的复杂基础架构和集群技术。
12.使用 UTF-8 字符集作为数据库默认字符集，系统数据库采用的用户名和密码满足定期修改的可变性，禁止使用数据库内置管理帐号作为系统连接帐号。数据库 temp 表空间最大不超过 2GB，保持定期清理；业务库表空间初始 100MB 起步，自增长不超过 256MB，单文件不超过 4GB，单文件达到 3.25G 才允许添加第二个文件，合理使用表分区等高级特性；无专门应用场景不启用归档特性，启用归档特性的数据库合理管控留存周期和磁盘空间。
13.提供所建应用数据库的完整数据字典设计文档，包括并不限于所有表的命名清单、每张表的字段清单，格式可参照 screw 生成的数据库文档。
14.系统数据库设计和功能设计应有效设计索引和唯一约束，超过 4 年历史数据不与当前在校数据存放同一张表，合理安排归档数据存放与查询使用，任一数据表记录原则上不超过 500 万条，根据

学校数据共享和接口规范提供相应功能接口和数据接口。
15.遵循《中南民族大学信息标准》，实现数据集成与交换，与校内任何系统之间的数据交换必须经过数据中心共享库，交换到数据中心共享库的数据须在源头转换为公共数据平台数据标准。
16.禁止使用加密狗等外接授权方式，授权文件应避免机器码、mac 等发生变化而失效。
17.本地验证功能必须不少于 9 位不少于 3 种符号类型的密码强度，登录错误超出自定义次数封停自定义时长，可组合自选源 ip 和帐号设置封停规则，达到自定义时长后自动解锁。
18.最高管理员权限帐号需具备双因素认证、指定源 IP 等验证方式。对满足自定义时长的未登录帐号批量进行自动停用。
19.具备与 12306 技术难度相当的图形验证码，验证码模块生成的随机数不能在客户端的静态页面中的网页源代码里出现，验证码内容不能与客户端提交的任何信息相关联，验证码可每次出现，也可以输错密码 1 次后出现，用户名、密码和验证码必须在同一个请求中提交给服务器，必须先判断验证码是否正确，进行验证码校验后，立即将会话中的验证码信息清空，而不是等到生成新的验证码时再去覆盖旧的验证码。
20.基于 B/S 建立的系统，必须设置有效过滤，防止 SQL 注入、防止 XSS 跨站脚本，防止 csrf 跨站请求伪造等,禁止动态构建 XPath 语句,禁止使用除 get/post 之外的 http 方法,禁止通过 POST/GET 方式传递 SQL 语句，不得使用拼接方式组合 SQL 语句。禁止使用 websocket 实现功能。
21.上传功能具备防止命令执行、防止上传脚本文件的能力,禁止使用 ftp 服务作为文件传输功能。对于上传文件类型进行严格控制,禁止仅使用 js 进行控制，必须在服务器端采用白名单方式对上传或下载的文件类型、大小进行严格的限制。上传目录不能有执行权限，原则上不允许有未经登陆验证的上传点，禁止以用户提交的数据作为读/写/上传/下载文件的路径或文件名。
22.所有文件和目录结构命名应避免使用中文,禁止将系统运行无关的文件、文档存放在发布路径，禁止暴露敏感文件在发布目录，如配置信息(如数据库连接信息)/源码备份文件，.git 或.svn 仓库，日志文件，数据库文件等，页面的相互调用采用相对路径，禁止使用“../”方式访问文件和目录。所用静态资源、前端样式引用全部本地化调用。
23.禁止使用国外代码托管平台存放、调试本系统使用的所有代码和程序，如 github 等。
24.因 IPS、WAF 等安全防护导致的拦截，一律优先修改程序，存在拦截的 URL 不做白名单放行。
25.优先支持适配国产浏览器，在质保期内完全适配当年主要流行浏览器不少于 5 种(360 除外)，移动端浏览器不少于 1 种,原则上不依靠浏览器插件实现打印、报表、文档编辑、文档预览等功能。
26.报错页面不暴露任何有关服务器和运行环境的信息，友情提示信息给予系统归属部门的联系人和联系电话，禁止显示网络中断、联系网管等相关字样。

集成规范：

27.面向校内师生的登录原则上集成使用学校统一身份认证，优先使用 CAS 集成，特殊情况经评估后可用 LDAP，仅面向最高管理权限和其他人员可提供独立本地验证。
28.集成学校统一消息接口实现卡片消息，消息提醒，短信等通知、待办推送。
29.涉及网上支付的功能，基于中南民族大学统一支付平台进行集成对接。
30.发布应用可灵活配置独立的小门户和碎片化应用，集成到学校信息门户和企业微信，应用内的组织架构及人员状态应与数据集成保持一致，并基于集成数据实现同人多身份角色、在校状态等的灵活权限配置。
31.应用发布不独占域名，各功能和模块配置在既有域名的虚拟目录下，格式为 domain.scuec.edu.cn/application-name
32.移动端基于 Html5 构建集成到企业微信、钉钉，不使用独立 APP，注意页面布局和功能适配。
33.依据功能需求描述包含在项目内，且未列举在招标文件中的潜在的对接集成，应充分理解项目建设目标并合理做出技术集成规划和测算，不再单独提供集成费用。
34.实施及质保服务期间，提供并随时更新详细的互联示意图，包括且不限于系统内置服务，系统与其它服务、接口之间的连接方向、连接端口等。
35.涉及与互联网集成的接口明确传出与传入的信息细节，对于传出的数据由归属单位依据《数据安全法》、《个人信息保护法》严格审查后完成相应保密手续再进行对接集成

升级平替旧系统规范：

36.旧系统结构化数据和非结构化数据全部迁移至平替新系统，并在新系统中提供旧系统数据的查询、复核功能。
37.迁移至平替新系统前做好充分的技术验证和业务准备，两套系统并行时间越短越好，最长不超出 10 个工作日，旧系统关机下线。

物联终端及自助终端规范：

38.物联终端操作系统优先使用国产 Linux 系统，必须开启主机防护按源 IP 开放业务端口和管理端口，每年不少于 4 次升级系统补丁。
39.物联终端应具备 5G 专网或以太网接口，通过 L2TP 和 L2TP over IPsec 协议连入业务专网。
40.物联终端远程管理仅限 ssh 和 rdp 协议，并指定固定源 ip 进行远程维护。

敏感数据保护：

敏感数据包括但不限于：口令、密钥、证书、会话标识、License、隐私数据（如短消息的内容）、授权凭据、个人数据（如姓名、住址、电话等）等，在程序文件、配置文件、日志文件、备份文件及数据库中都有可能包含敏感数据。
1.禁止在代码中存储敏感数据。
2.禁止密钥或帐号的口令以明文形式存储在数据库或者文件中；密码必须进行带 salt 的哈希之后保存数据库。
3.禁止在 cookie 中以明文形式存储敏感数据。
4.禁止在隐藏域中存放明文形式的敏感数据。
5.禁止用自己开发的加密算法，必须使用公开、安全的标准加密算法。
6.禁止在日志中记录明文的敏感数据。
7.禁止带有敏感数据的 Web 页面缓存。
8.带有敏感数据的表单必须使用 HTTP-POST 方法提交。
9.在客户端和服务器间传递明文的敏感数据时，必须使用带服务器端证书的 SSL。
10.禁止在 URL 中携带会话标识（如 jsessionid）。
11.禁止将对用户保密的信息传送到客户端。

质保服务要求：

1.按功能模块进行验收，每个功能模块自验收之日起质保期不少于 5 年。
2.与质保服务人员签订保密责任协议，严肃管理参与人员对有关数据、文件、资料、消息的流转、传播、保存、销毁的责任与义务。
3.系统部署实施期间，指定 1 名接口人完成所有工作事务的对接，不少于 2 名固定驻场人员跟随学校工作时间进行现场服务。自系统验收之日起，根据学校工作时间至少固定 1 人驻场服务承担所有技术运维服务及厂家事务对接，非驻场人员根据工作事项安排动态增补，无故不得随意更换固定驻场人员，验收后驻场服务期不少于 2 年，质保金根据驻场服务考核结果在第 2，5 年退还。驻场服务期结束后，30 分钟电话响应，2 小时内现场响应。
4.质保期内，包括操作系统、数据库、技术框架等在内的所有新发布的漏洞情报，2 小时内响应，4 小时内出具解决方案，12 小时内消除漏洞。
5.质保期及续保期内，注意安全设备规则库定期升级，因 IPS、WAF 等安全防护拦截导致的问题，一律优化修改程序进行解决。
6.实施及质保服务人员应保持固定，服务期间最多变更 1 次固定驻场人员，涉及数据操作的人员应在开工前与系统归属单位签署保密协议，严格管理实施过程中涉及的数据、资料、文件、帐号、密码等传播范围、使用范围和存储位置。
7.上线后开展的升级、调优等工作，应提前测试验证，提交归属单位处置方案，明确预案、备份、

回退等详细措施和时间工序，经审核认可后方可开展工作。服务方禁止安装、使用任何第三方远程管理工具(如 teamviewer、向日葵等)，因安全整改而下线的系统，经复测合格后方可恢复上线，其它原因下线的服务器原则上不再提供临时开启短暂运行。
8.严禁将所提供运行环境作为开发、测试环境使用，未达到生产规范标准的环境待整改完毕后方可重新恢复上线。

评分标准要求：

1.信息安全要求：设置评分项，信息系统安全服务资质证书；
2.运维要求：信息技术运维服务能力证书，驻场服务期限和服务标准；
3.上线要求：提供检测报告说明渗透测试结果和代码安全审计结论。

辅助建设内容：

1.网络安全等保测评:所建应用应根据测评定级完成该系统的等保测评和定级备案,作为验收条件。
2.自助服务：所建应用具备自助打印或其它自助服务终端 API 开放和集成特性，应在投标中包含与智慧校园的 AI 识别、校园卡集成、数据集成等方面的技术规格和成本，对自助终端的远程管理、稳定性、安全性符合中南民族大学自助终端管理规定的要求。
3.授权管理：根据业务管理要求，建立适用于该系统的授权管理、授权申请及审批制度。各岗位权限应合理控制并相互制约，严禁设置全功能的超级用户，严格控制系统维护的临时用户。所有操作人员应在权限范围内进行操作，并对本人的账号、密码严格保密。