**一、****项目技术需求**

**项目名称**：哈尔滨工业大学信息化专项图书馆应用交付及堡垒机系统采购项目（二次）

**项目编号**：HITZB-2020000031

**招标数量:** 应用交付系统1套，堡垒机1台

**招标控制价：**38.5万元，投标报价超过招标控制价的，按无效标处理。

招标采购内容：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **单位** | **数量** |
| 1 | 应用交付系统 | 套 | 1 |
| 2 | 堡垒机 | 台 | 1 |

（包含转换加工、相应接口软件的调试、安装、培训等）

一、项目概况

1、建设目标

1. 应用交付系统：

一键断网：响应网络安全法和教育部的相关规定，如果网站出现意外，要求3分钟内切断网络，控制影响范围，减少对学校声誉的伤害。

IPv4转IPv6：工业和信息化部、教育部等部委分别下发贯彻落实《推进互联网协议第六版（IPv6）规模部署行动计划》的通知，通知要求主要互联网、基础设施、云计算运营商等加快设施IPv6改造，政府网站和部属各单位、部属各高校及各省、自治区、直辖市通信管理局在2020年之前完成门户网站IPv6改造。而图书馆现在已上线运行的绝大部分应用系统，都是基于IPv4协议通讯，想要通过改变系统代码、结构实现IPv4转换IPv6难度极大，需要中间转换机制，将包括网站在内的各系统，由IPv4协议转换为IPv6协议。

HTTP升级HTTPS：近年有关网络信息泄露、网络钓鱼诈骗案件频发，应该更加重视互联网信息安全，原本普遍应用的HTTP协议已不能满足当前的安全需求。HTTPS是以安全为目标的HTTP通道，主要有两个作用：一是建立一个信息安全通道，来保障数据传输安全；另一种即是确认网站的真实性，这对我校图书馆犹为重要。

1. 堡垒机：

图书馆服务器、网络设备、网络安全设备越来越多，且设备管理分散，存在多对多的交叉异构管理的情况。而目前运维人员依赖于Telnet/SSH/RDP/FTP等协议对设备进行远程维护，使用KVM方式进行本地维护。还有部分厂商采用VPN远程接入进行维护。

现在的运维操作类似一个“黑盒“，我们并不知道：当前管理员/代维工程师正在进行哪些运维操作；是在哪一台设备上发生的操作；操作是谁来执行的；执行的操作是否正确。

由此，日常的技术运维操作主要存在以下操作风险：误操作导致关键应用服务异常甚至宕机；违规操作导致敏感信息泄露；恶意操作导致系统上的敏感数据信息被篡改和破坏；无法有效监控原厂商和代维厂商的维护操作；无法有效取证和举证维护过程中出现的问题和责任。

另，黑客/恶意访问也有可能获取系统权限，闯入图书馆内部网络，造成不可估量的损失。

我们必须提高系统运维管理水平，满足《网络安全法》和《国家信息安全等级保护管理规定》要求，防止黑客的入侵和恶意访问，跟踪服务器上用户行为，降低运维成本，提供控制和审计依据。

因此，需要针对单位内部网络设备和服务器进行账号和认证的统一管理，对此类资产的常用访问方式进行监控和审计。例如对字符终端、图形终端等访问方式进行监控和审计，实现对用户行为进行控制、追踪、判定，满足单位内部网络对安全性的要求。

2、预期的建设效果

1. 应用交付系统：

通过部署应用交付系统，实现“一键断网”、IPv4转IPv6、HTTP升级HTTPS。满足目前法律、法规的要求和未来技术发展的必然过程。

管理员可以自定义多种类型的访问控制策略，并按需启用，还能根据指定的要求，自动启停策略，减轻管理员的负担。一键断网功能让管理员在手机上就能控制应用的访问规则，提高安全管理工作的效率和时效性。

我单位都有大量的网站和应用系统，按照国内SSL证书的普遍价格，每年购买证书也是一笔不小的费用，然而应用交付网关能够自动申请有效的国际SSL证书，为我单位节省投资。

1. 堡垒机：

通过部署统一安全运维平台（堡垒机）实现：

集中账号管理，基于唯一身份标识的全局管理，实现了单点登录，任何运维人员都无法绕过堡垒机。统一账号管理策略，实现与各服务器、网络设备等无缝连接。

集中授权管理，细粒度的命令级授权策略，针对运维人员、服务器、服务器账号、服务器应用、访问时 间等多个因素设定细粒度的授权策略，使得运维人员的权限得 到很细的划分，从而杜绝了运维人员权限不明晰的问题。

集中认证管理，提供多种认证方式，包括：本地认证、证书认证、RADIUS 认证 及生物指纹识别认证。集中认证有效地将非法用户或非授权用户拒之门外， 就像一座堡垒坚不可破。

集中操作审计，基于唯一身份标识，全程审计用户对从登录到退出的操作行为，使得事后的审计和责任的定位有了可靠有力的根据。

二、项目需求描述

主要功能需求；

应用交付系统：

一个应用交付系统完成以下几项工作：

1、提供了基于微信的访问控制工具，并为此种情况作了应用场景优化，只需点击一下，就能完全切断外界对内部应用的访问，极力缩小负面信息的传播范围。同时也能在手机上直接操作各种访问控制策略，改变任何一个应用或网站的可访问状态，3分钟内能完成访问控制任务。

2、能够快速为应用和网站接入IPv6网络，很多线上服务器因为各种原因无法直接连接IPv6网络，比如正在运行的网站系统在前期建设时未接入IPv6网络，重新接入IPv6很可能需要冒很大的风险进行停机或重新配置，工作量也很大。使用应用交付系统，无需对原有系统和服务器作任何改造，即可非常容易地令应用和网站通过IPv6访问，达到IPv6部署的工作要求。

3、应用交付系统需要内置SSL证书自动申请和更新功能，所有应用和网站，只要启用HTTPS服务，能够免费获得SSL证书，并在证书到期前自动更新，无需任何人工操作，既节省资金又能大大减轻管理员的工作负担。另，除了自动申请的免费证书，系统还需支持已有SSL证书及自建CA签发私有证书，以满足特定网络条件下的证书使用需求。

二、堡垒机：

1、集中账号管理：

包含对所有服务器、网络设备账号的集中管理。可以完成对账号整个生命周期的监控和管理，降低了管理大量用户账号的难度和工作量。同时，通过统一的管理还能够发现账号中存在的安全隐患；并且制定统一的、标准的用户账号安全策略。建立集中账号管理，单位可以实现将账号与具体的自然人相关联。通过这种关联，可以实现多级的用户管理和细粒度的用户授权。而且，还可以实现针对自然人的行为审计，以满足审计的需要。

2、集中身份认证：

[堡垒主机](mailto:Ultr@AMS)为用户提供统一的认证接口。便于对用户认证的管理，而且能够采用更加安全的认证模式，提高认证的安全性和可靠性。集中身份认证支持电子证书、双因素、动态口令和生物特征识别等多种认证方式，而且系统要具有灵活的定制接口，可以方便的与第三方LDAP认证服务器对接。

3、统一资源授权：

[堡垒主机系统](mailto:Ultr@AMS)提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过B/S、C/S对服务器主机、网络设备的访问进行审计和阻断。

4、细粒度访问控制：

最大限度保护用户资源的安全。细粒度的命令策略是命令的集合，可以是一组可执行命令，也可以是一组非可执行的命令，该命令集合用来分配给具体的用户，来限制其系统行为，管理员会根据其自身的角色为其指定相应的控制策略来限定用户。

5、运维操作审计：

操作审计管理主要审计操作人员的账号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的账号、资源进行标识后，操作审计能更好地对账号的完整使用过程进行追踪。

三、项目技术要求

1、总体要求

一、应用交付系统：

1. 系统架构：系统要求支持分布式架构，可支持策略管理服务器与应用发布服务器分离，即满足应用交付的安全，又满足管理安全。
2. 硬件：应用发布服务器1台，机架式2U，网络接口>=6\*10/100/1000 Mbps，2\*USB、1\*console。
3. 支持反向代理功能
4. 支持IPv6，支持v4站点转v6
5. SSL证书管理：支持站点SSL证书和全站SSL证书；支持Let's Encrypt免费证书自动签发；支持证书自动申请、更新；主动防御：支持广告机器人自动拦截；支持漏洞扫描器自动拦截
6. 访问控制：支持来源地址分组管理，支持站点与来源地址分组正交授权，支持多种安全等级配置，支持自定义访问控制策略，支持基于时间、浏览器特征、操作系统特征的访问控制策略，支持远程切换访问安全等级与策略，支持全局JS、CSS、HTML插入。

二、堡垒机：

1. 硬件指标：系统以软硬件一体方式提供，标准机架，千兆电口≥2个，硬盘≥1T，1U机架式
2. 性能要求：并发会话数：字符并发会话数≥500 个，图像并发会话≥200个
3. 管理设备数量：标配100个管理设备授权
4. 智能终端：支持基于Android、IOS系统的智能终端接入运维服务，并提供相关证明资料截图
5. 身份认证：除基本口令认证外，系统内置生物指纹认证模块，并在同一页面显示，通过用户名+口令+指纹录入（可组合方式）进行认证并运维使用，达到统一身份认证的安全要求，并提供相关证明资料截图
6. 动态口令：系统登录需要内置动态口令双因素认证，双因素系统需要内置在系统中，不需要使用其它的服务器（或虚拟机）进行安装，用户建立、令牌配置、令牌绑定等操作，必须在同一个管理界面中完成，客户端为手机APP方式查看令牌秘钥，并提供相关证明资料截图

2、关键技术指标

一、应用交付系统：

★**项参数要求必须满足，且能够提供产品功能截图或官方网站、产品宣传册截图或者厂商出具明确应答并盖章，否则按无效标处理。**

1. 系统架构：系统要求支持分布式架构，可支持策略管理服务器与应用发布服务器分离，即满足应用交付的安全，又满足管理安全。
2. 硬件：应用发布服务器1台，机架式2U，网络接口>=6\*10/100/1000 Mbps，2\*USB、1\*console。
3. 支持多机分布式部署。
4. 性能要求：支持管理端与服务端前后端分离
5. 支持多服务端负载均衡
6. 支持多管理端高可用配置
7. 可管理网站主机数量>=100
8. ★反向代理：支持反向代理功能
9. 支持多域名，支持正则表达式配置域名
10. 支持HTTP1.1 HTTP2
11. ★支持IPv6，支持v4站点转v6
12. 支持静态文件缓存
13. 负载均衡：支持后端多主机负载均衡
14. 支持业务健康检测，自动移除故障节点
15. 支持多种负载均衡策略
16. ★SSL证书管理：支持站点SSL证书和全站SSL证书
17. ★支持Let's Encrypt免费证书自动签发
18. ★支持证书自动申请、更新
19. ★访问控制：支持来源地址分组管理，支持站点与来源地址分组正交授权，支持多种安全等级配置，支持自定义访问控制策略，支持基于时间、浏览器特征、操作系统特征的访问控制策略，支持远程切换访问安全等级与策略，支持全局JS、CSS、HTML插入。
20. 用户认证：支持LDAP、Radius、Oauth2用户认证
21. 支持CAS中央认证服务的SSO
22. 可以与WebVPN联动，支持基于用户、组身份授权访问应用
23. ★主动防御：支持广告机器人自动拦截
24. ★支持漏洞扫描器自动拦截
25. 支持恶意地址自动拦截
26. 支持服务器信息隐藏
27. 支持错误页面封装
28. 运维安全：支持业务健康检测
29. 支持业务故障告警
30. 支持安全事件告警
31. 支持事件全日志查询
32. 支持管理员登录IP限制
33. 支持管理员二次登录认证
34. 支持手机远程一键断网
35. 远程操作功能使用反向连接，不开放外网管理端口
36. 统计分析：支持全局和站点访问流量分析
37. 支持全局和站点访问来源分析
38. 支持全局和站点点击量分析
39. 支持全局和站点用户地区来源分析
40. 支持用户来源、IP、主机访问日志查询，支持时间段查询
41. 支持top站点统计和top页面统计
42. 支持站点错误分析
43. 支持日志统计
44. 可用性证明此产品的同类用户证明文件
45. 售后服务3年原厂商设备保修和售后服务
46. ★系统测试因要接入核心网络系统关键业务，为保证接入现有网络系统的兼容，不影响现有网络系统业务的正常运行，部署前需提供产品给甲方测试，测试期为5个工作日，测试结果与投标书中的应答一致时，且能够满足用户的实际需求，方为测试通过，签署合同并进行部署；**测试报告与投标书中的应答不一致时，测试未通过，按无效标处理。**

二、堡垒机：

技术要求（带★项为必须满足项）

1. 产品资质：获得公安部颁发的 《计算机信息系统安全专用产品销售许可证》 ，并出具加盖厂商公章的复印件
2. 厂商资产：设备生产厂商必须具备《ISO9001质量管理体系认证证书》，并提供相关证明资料
3. ★投标人必须具有原厂商该项目的支持授权和服务承诺函
4. ★设备生产厂商应具有漏洞发现能力，具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位资质》，至少曾经获得中国信息安全测评中心颁发《中国国家漏洞库-信息安全漏洞提交证明》，不低于15份，并出具加盖厂商公章的复印件
5. ★设备生产厂商应为CNVD技术组成员单位，出具CNVD官网截图证明及证书号并加盖厂商公章的复印件
6. ★设备生产厂商具备中国信息安全测评中心颁发的《国家信息安全测评 信息安全服务资质证书》（安全工程类一级）资质，能力范围包括：安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和维护等，并出具加盖厂商公章的复印件
7. ★设备生产厂商至少具有一名由国家计算机网络应急处理协调中心省级分中心或国家中心聘请的公共互联网络安全专家，并出具加盖厂商公章的复印件
8. 不少于三年7×24免费原厂售后服务
9. 部署方式：旁路模式，系统内置SSL VPN系统支持远程用户安全接入, SSL VPN用户名与密码策略与堡垒机完全一致，并提供相关证明资料截图
10. 管理结构：B/S架构，采用HTTPS方式远程安全管理。
11. ★集中管理：支持分布式集中管理部署，在网络中只需输入同一个IP，集中管控平台会根据登录身份自动跳转到分布式部署的堡垒机上进行管理。并提供相关证明资料截图
12. 使用方式：支持WebPortal登录方式，支持使用任意运维客户端工具直接登录业务系统，基本上不改变当前运维人员操作习惯。
13. 硬件指标：系统以软硬件一体方式提供，标准机架，千兆电口≥2个，硬盘≥1T，1U机架式
14. 性能要求：并发会话数：字符并发会话数≥500 个，图像并发会话≥200个
15. 管理设备数量：标配100个管理设备授权
16. 运维管理：运维管理：支持B/S、C/S两种不同方式的运维接入，适应运维人员的运维习惯，两种运维方式实现无差别保存运维记录，提供相同的操作方式和审计入口
17. 浏览器支持：至少支持除Windows系统下的 IE/Chrome/火狐浏览器运维管理外，还需支持基于Mac OS X系统的Safari浏览器调用本地客户端运维和管理
18. ★智能终端：支持基于Android、IOS系统的智能终端接入运维服务，并提供相关证明资料截图
19. 用户角色：系统具有用户多角色划分功能，如系统管理员、设备管理员、普通用户、分组管理员、审计管理员等，对各类角色需要进行细粒度的权限管理。
20. ★身份认证：除基本口令认证外，系统内置生物指纹认证模块，并在同一页面显示，通过用户名+口令+指纹录入（可组合方式）进行认证并运维使用，达到统一身份认证的安全要求，并提供相关证明资料截图
21. 登录认证日志可以统一审计
22. 系统自身内置指纹身份认证并支持二代居民身份证指纹
23. ★动态口令：系统登录需要内置动态口令双因素认证，双因素系统需要内置在系统中，不需要使用其它的服务器（或虚拟机）进行安装，用户建立、令牌配置、令牌绑定等操作，必须在同一个管理界面中完成，客户端为手机APP方式查看令牌秘钥，并提供相关证明资料截图
24. ★认证日志：认证过程需要有详细的过程，为了故障排除，在前台界面至少需要显示出成功登录和认证错误，认证错误至少可以分为：密码错误、Licenses错误、用户名格式错误、来源地址禁止、有效时间禁止等明细的选项。
25. 认证模式：各分支机构设备到集中管理中心进行认证，所有的帐号、资源、权限都在集中管理中心进行管控，集中管理中心可以为各分支机构建立组管理帐号，分支机构的组管理帐号只能管理分支机构的设备、用户等资源
26. 主帐号关联：支持以主账号为基准，支持直接查询并编辑与该主账号相关的策略
27. 支持以设备为基准，支持直接查询该主账号有权限运维的所有设备
28. 支持以设备为基准，支持直接查询该主账号的所有审计信息
29. 支持以设备为基准，支持直接查询并编辑与该设备相关的策略
30. 设备关联：支持以设备为基准，支持直接查询有权限运维该设备的所有普通用户
31. 支持以设备为基准，支持直接查询该设备的所有审计信息
32. 命令限制：系统需要支持黑名单、白名单功能，黑名单为用户不能执行的命令，用户绑定黑名单后，则不允许执行黑名单的命令，但可以执行除黑名单之外的所有命令，白名单为用户只能执行的命令，用户绑定白名单后，则仅允许执行白名单中的命令
33. 用户黑白名单绑定，需要详细到哪个主帐号，使用哪个从帐号登录到哪个设备
34. 帐号锁定：细颗粒的帐号锁定功能，可以指定哪个主帐号与哪个从帐号的绑定进行了锁定，如果一个绑定关系进行了锁定，则只有当绑定关系解锁时才能正常登录
35. 授权模式：各分支机构设备到集中管理中心进行授权，所有的帐号、资源、权限都在集中管理中心进行管控，集中管理中心可以为各分支机构建立组管理帐号，分支机构的组管理帐号只能管理分支机构的设备、用户等资源
36. 操作审计：支持的协议：登录协议：RDP、Telnet、SSH V1、SSH V2、VNC
37. 文件传输协议：FTP、SFTP，FTP,SFTP要求可以记录上传下载文件，同时为了防止存贮占用过大，可以根据上传下载文件大小进行定制选择记录，比如只记录3M以下的文件
38. 支持Oracle、MS SQL Server、IBM DB2、Sybase、MySQL等数据库审计
39. 支持HTTP、HTTPS操作审计
40. 可通过应用发布的方式进行协议扩展，无需定制即可支持其他通用及专有的运维客户端程序。
41. ★应用发布：支持C/S、B/S应用发布，支持堡垒机内置应用发布服务器，登录应用发布时无缝连接（Remoteapp建立连接桌面过程予以屏蔽），应用发布支持授权、SSO自动登录、录相审计。应用发布系统需要支持http、https、PLSQL等通用软件的自动密码填写。
42. ★应用发布支持文件中转功能，打开发布后的应用在上传及下载文件时，先将文件上传及下载到中转站（临时网盘功能），再根据权限进行上传下载文件。保证文件的上传下载文件的权限可控。
43. 支持的浏览器：系统无需用户在终端安装java运行环境，即可支持IE/chrome/火狐等浏览器登录操作及运维使用
44. 支持的设备访问方式：登录菜单访问：客户端访问审计系统即可显示用户能访问的资源菜单，用户通过字符菜单或图形菜单选择方式直接访问设备。
45. ★Web方式登录：用户可以在Web界面中直接调用至少支持Mstsc、WinSCP、FlashFXP、SecureCRT、Putty、Xshell等客户端，登录到目标系统；直接登录：用户不需要菜单选择、不需要通过WEB界面点击，直接通过客户端登录方式认证要求使用主帐号和密码。并提供相关证明资料截图。
46. 操作行为记录：审计人员可以审计所有的人操作，分支管理员只能审计各分支机构设备及人员的操作，各运维人员只可以审计自身的操作
47. Telnet、SSH审计内容：包括访问起始和终止时间、用户名、来源IP地址、目标设备IP、设备名称、设备用户、协议类型、占用空间、事件类别、详细文件审计以及操作内容回放。
48. RDP、VNC、HTTP、HTTPS等协议审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、设备用户、协议/应用类型、事件等级、详细文件审计以及操作内容等；支持操作内容录像回放。
49. 数据库运维操作审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、应用类型、操作内容等；支持操作内容录像回放。
50. 审计回放时，支持完全通过WEB方式调用操作审计录像回放，支持正常、快进、慢进、鼠标拖拽播放。
51. 支持通过基于时间、IP、用户、设备、设备账号、命令、等组合访问控制策略，授权用户可访问的目标设备。
52. 审计模式：集中中心审计员可以审计所有分支机构的操作，各分支机构审计员只可以审计本身支机构的操作，各运维人员只能审计自已的操作。
53. 访问控制及异常告警：告警方式至少支持Mail和Syslog
54. 系统需要有用户登录统计功能，可以统计哪些用户被哪些来源IP进行密码登录尝试，统计至少包括以下项目：来源地址、被登录IP、登录协议、尝试用户、尝试次数，可以直接导出为Xls/Html/Pdf/word格式便于查看
55. 系统具有细颗粒的告警功能，可以定义哪个主帐号，登录到哪个设备的从帐号时发送告警；
56. 报表输出：报表输出：系统支持各种报表输出，包括运维报表、权限报表、登录报表、操作报表、定期报表等
57. 报表模式：集中管理管理员可以打印所有设备的报表，分支机构管理员只能打印本分支机构的设备报表

3、项目验收及质保期

合同签订后 30个工作日内交付所有功能并接受验收。

项目备品备件要求：若无法及时解决故障，免费提供备品备件服务。

安装调试服务：原厂安装调试。

**项目验收须达到如下要求：**

(1).验收依据：招标文件、投标文件、厂家货物技术标准说明及国家有关的质量标准规定，均为验收依据。

(2).货物运输与验收：货物需由信誉高的大型物流公司运输，包装须规范，保证设备完好，设备运抵采购人处，设备落地到采购方指定位置，运费及人工费，包装材料清理费均由供货商负责，由双方对照采购清单及技术要求进行验收。

(3).系统验收：成交供应商根据采购要求进行设备安装、调试、测试、培训后，由采购人进行使用性能方面的验收。验收合格的标准包括但不局限于：

成交供应商根据采购人要求进行设备安装、调试、测试、培训并正式运行后，性能稳定。

如验收未通过，成交供应商需对缺陷进行整改，然后重新提出验收申请。

**质量保证期**

自验收合格之日起3年（产品质保期有具体要求的，按相应产品的质保期要求执行），质量保证期内乙方应负责免费维修。

4、付款方式和条件

签订正式合同后，按照如下验收节点验收合格后，支付中标额的费用，具体要求为：

（1）在签订正式合同后，支付中标额的30%；

（2）在第一个验收节点验收合格后（设备到场签收 系统调试完成），支付中标额的65%；

（3）尾款5%，在项目整体验收合格运行1个月后支付。

5、售后维护要求

提供3年原厂硬件质保、3年原厂软件及规则库升级服务，在保修服务期内，对提供的产品进行免费维修、损坏件更换。对系统软件的改进，增加的功能在服务期内及时免费提供。

提供最新的技术支持服务，以及后期的版本升级，保证升级后的系统能够稳定运行。

故障响应方面，提供7×24小时的故障服务受理；对重大故障提供7×24小时的现场支援，一般故障提供5×8小时支援；故障服务的响应时间小于2小时；中断时间不能超过3小时。

四、项目与学校信息化总体框架兼容的要求

1、系统对接要求

（1）统一身份认证接入要求

统一身份认证服务通过统一管理用户的认证过程和认证信息，使登录后的用户在应用之间可以不需再次登录，为用户带来 “单点登录，多点漫游”的便利。校园用户提供与校园其他系统数据/功能对接的唯一标识，因此在系统登录与用户身份需与校园统一身份认证服务进行对接。

（2）共享数据中心数据对接要求

按学校相关的数据标准，以只读视图的方式授权和开放系统数据，这些数据将会被同步至共享数据中心，供其他业务系统使用。

面向其他应用系统需提供数据访问接⼝的服务，根据数据访问的要求对元数据进行封装，以 Web Service 接口的形式对外发布。

（3）统一通信平台对接要求

基于校园各类应用系统信息统一收发要求，除系统内通知消息外，所有业务系统通过短信、微信、邮件等通道发送的消息均须对接校园统一通信平台，由统一通信平台负责发送，包括回执消息的接收。

信息发送须严格遵守各通信运营商对信息安全管理和企业用户授权的相关要求，包括但不限于信息审计、黑白名单设置和信息模板管理等要求。

（4）校园门户集成要求

包括四个方面的集成内容：

1）资讯对接：为系统的资讯类内容提供RSS或API订阅接口，以供第三方系统的统一调用。

2）待办/已办接口对接：包括系统产生的流程类状态信息等。此类数据需由系统提供相应的webservice接⼝，供门户系统待办/已办功能调用。

3）服务对接：校园门户内提供校园办事服务功能，涉及到师生服务的申请、办事类应用需与办事服务进行对接。

4）应用对接：校园门户提供开发者服务功能，支持门户内应用的开发与集成，对于能够为师生提供的简单应用，应在门户平台中遵循相应的接口与界面规范建立对应的应用（第（5）条要求的移动应用集成同理）。

5）应用或服务与门户的对接可能涉及到直接跳转、数据集成、界面集成等多种方式，每个应用或服务具体的对接策略待之后双方视具体情况共同商议决定。

（5）校园移动应用集成要求

包括移动数字校园APP与校园微信公众服务号/企业号，内置的应用商店。功能支持HTML格式的、移动端页面优化的应用服务直接入驻，技术上涉及到认证、身份的对接等。对于第三方系统已形成的移动端服务，可直接进行测试迁移。对于一些数据查询类型的服务，可通过数据与校园共享数据中心的同步后进行独立设计。其他移动端功能性应用可根据需要逐步实施。具体的技术方案可由双方技术人员进行详细对接。

（6）校园统一支付缴费平台的集成要求

如果项目中存在支付缴费类业务，应具备与学校统一支付缴费平台集成的能力：

1）能根据统一支付缴费平台提供的标准化开发接口实现支付缴费业务的定制与开发。

2）能提供标准开放式接口，用于统一支付缴费平台获取相关数据。

具体的技术实施方案可由本项目施工单位和统一支付缴费平台施工单位协商确定。

（7）校园一卡通系统集成要求

如果项目中存在与一卡通系统相关业务，应具备与校园一卡通系统对接集成的能力：

1）能根据一卡通系统提供的标准化开发接口实现与一卡通系统的集成开发。

2）能提供标准化开放式接口，用于一卡通系统获取相关数据。

具体的技术实施方案可由本项目施工单位和一卡通系统施工单位协商确定。

2、对系统扩展性的要求

具备良好的应用集成能力，提供标准的数据接口，支持二次开发。

扩展能力是由系统的技术架构和技术的先进性所决定的。系统的扩展性是系统的生命力之所在，良好的扩展性和二次开发能力，能确保系统具有适应性，降低系统的实施和开发成本。

系统须具备良好的扩展性，具有较长的生命周期，在后期的应用过程中能够基于平台进行业务扩展。

3、对系统安全性的要求

**（1）总体要求**

1）系统提供商对于因为程序代码、框架技术以及使用的中间件而产生的应用系统漏洞或***bug***等程序错误终身负责维护升级；

2）系统上线前须经学校的安全准入检测，不合格的系统不能上线并验收；

3）系统运行过程中定期或不定期接受相关部门的安全评测，接到系统安全评测或渗透报告后须提供详实可行的整改报告，经复测验证合格后方可再次上线运行。

**（2）系统配置要求**

1）系统必须保证为正常上线系统，须更新为最新。禁止采用失去技术升级的系统（如：***windows 2003***等）；禁止采用含有已知漏洞的组件、应用程序、框架（如：***Struts 2.5 - Struts 2.5.10***）、应用程序服务器、***web***服务器、数据库服务器和平台定义，以上系统必须执行安全配置，禁止默认安装。所有的软件应该保持及时更新，采用***struts2***的系统原则上不允许对校外提供服务；

2）保证系统服务正常并与上线系统保持一致，无调试和报错信息（如：断点、***printf***等调试信息），无注释信息，删除系统默认安装的各种例程、文档及管理程序；

3）系统中禁止暴露配置信息（如数据库连接信息）、源码备份文件、.git,.svn仓库等，严禁在***github***等平台公布代码。

**（3）服务要求**

1）从本机关闭不需要的端口（如：关闭***windows netbios***等服务），设置本机防火墙（如***iptable***）对访问的源地址进行限制，相关服务设置类似***host.allow***和***host.deny***等策略；

2）须按照标准端口配置服务，严禁自行设置非标服务端口。

**（4）数据库配置要求**

1）数据库和应用系统如在同一台服务器，须采用本机回路进行访问，如前端及数据库分为不同服务器，须设置本机防火墙访问规则，禁止非前端服务器访问数据库网络端口；

2）使用最低权限的数据库用户作为***web***应用所需，禁止具有不必要的额外权限。

**（5）开发要求**

1）对用户输入进行严格有效过滤，防止***sql***注入、***xss***跨站脚本、命令执行，***crsf***跨站请求伪造等，建议采用白名单过滤策略；

2）禁止在***HTTP***请求中以明文或可逆编码（如***base64、url***编码等）的形式传递***SQL***语句到后端程序代入执行，禁止由***Web***前端直接生成和传递***SQL***语句到数据库进行执行，数据库查询必须采用预编译和参数结构化查询。如果程序确实需要将***SQL***语句作为内容（非可执行代码的形式，如学生毕业设计、代码样例等）到后台，请在项目上线交付前书面说明相应的功能代码及位置；

3）控制上传点，对于上传文件类型进行严格控制（禁止用***js***进行控制），上传目录不能有执行权限，原则上不允许有未经登录验证的上传点；

4）设置有效的身份认证、会话管理及访问控制机制，防止越权、平行权限及提权等（禁止利用***js***进行控制及验证）。

**（6）密码复杂度要求**

系统必须有密码复杂度检查模块，设置有效的验证码或者滑动等手段防止暴力破解，密码长度须大于8位，含字母（大小写）、数字及符号组合，重要系统须采用二次认证。禁止在数据库中明文存放用户密码，需进行带***salt***的哈希之后入库。对于多次错误登录进行封堵。如果长期不登录默认账号应停用处理。

**（7）数据保护要求**

对于身份信息、单位职务、财务信息、健康信息、通讯信息等敏感信息禁止在数据库中明文存放。

**（8）系统安全评测和等保评测要求**

为配合系统安全评测及等级保护定级和评测的相关要求，须提供如下系统信息：

1）操作系统版本、补丁情况；

2）开放的网络端口及用途；

3）所有第三方中间件、开发包、数据库、服务版本及管理地址。如：***tomcat*** 8.0、***apache*** 2.4.2 、***jquery*** 3.1.0、***mysql*** 5.0等；

4）系统的用户登录路径、登录用户名和密码（必须为复杂密码，评测后更改），系统密码的设置策略（是否满足（6）关于密码复杂度的要求）；

5）系统访问路径和系统管理端路径。

4、对系统部署方式的要求

系统部署应充分考虑到哈尔滨工业大学现有信息化总体框架以及对未来发展的适应性，要求系统支持单机部署、双机部署、集群部署以及云平台部署的相关要求，并支持负载均衡。

对提出的系统资源配置需求，需提供相应的申请内容，包括但不限于业务平台拓扑、计算资源需求、网络资源需求、存储资源需求（要求提供针对我校实际需求的计算依据，如最大并发、用户增长、网络带宽、CPU、内存、存储需求量测算及具体对外提供服务端口等）。

5、对相关文档和交付物的要求

乙方在项目验收通过后向甲方提供该项目形成的成果和相关文档。乙方向甲方提供的成果和文档资料不得人为设置技术障碍影响甲方的维护和二次开发。

本项目交付成果（参见项目建设内容）。

提供的文档资料包括：

（1）《项目实施计划》

（2）《项目实施计划变更协议》（如果有变更）

（3）《需求说明书》

（4）《需求变更协议》（如果有变更）

（5）《上线试运行确认单》

（6）《系统技术文档》

（7）《系统管理员手册》

（8）《用户手册》

乙方按哈尔滨工业大学档案馆归档要求，完成项目归档工作。

五、技术情报和资料的保密要求

采购甲乙双方均对对方提供的技术情报和资料承担保密义务，如需公开或向第三方提供，需经对方同意。乙方在工作中获取的甲方提供的信息、资料、数字均应予以严格保密，乙方负责本项目的人员不得向任何单位和个人泄密。如因泄密造成后果的，乙方应承担全部法律的责任。乙方对甲方提供的信息资料等在完成合作后返还甲方。

不论本合同是否变更、解除、终止，本条款长期有效。