## 一、项目概况

### 1、建设目标

随着网络信息化的不断发展，由于缺乏有效的技术措施来实施管理和检测，

因此需要采取必要的技术手段对相关设备进行的文件进行监测行为。

### 2、预期的建设效果

 发现 、监控、保护和管理，计算机、移动设备、网络存储系统上等重要信息。

## 二、项目需求描述

## （1）功能需求（详见关键技术指标中详细要求）；

## （2）性能需求（一个服务器端、1000点客户端）；

## （3）其它需求。（软件运行环境：win7\win10)

## 三、项目技术要求

### 1、总体要求

 根据哈尔滨工业大学的需求，发现 、监控、保护和管理，计算机、移动设备、网络存储系统上等重要信息。投标产品需具备安全性，实用性，易管理性，可扩展性。

**（1）安全性**

按照安全性原则，在对系统进行安全风险分析的基础上，明确系统的安全目标和安全需求，并采用一套完整的安全措施来防止这些安全风险，满足系统的安全需求，实现系统的安全目标。

**（2）实用性**

在综合考虑满足系统目前需求和今后可扩展性要求的前提下，适度控制投资规模。特别在设备选型时，在满足需求的前提下，关注性能价格比，并适度的留有余地。

**（3）可扩展性**

在系统设计时，既考虑当前的实际需要和承受能力，又考虑其长远发展的需要，要求系统具有高扩展性，当用户数目增加时，网络有灵活调整、扩充的手段和方法，服务器的处理能力也要能满足新的业务增长的要求，并能做到平滑过渡。

**（4）便捷性**

系统安装完成后，不会给涉密计算机的用户带来使用上的较大差异。在信息交互、设备、文件处理等方面，在保证涉密信息安全的基础之上，使用户的操作尽量便捷、简单。

**（5）易管理性**

方案在设计上使用分布式的部署方式。管理更加有效、简单、安全。使管理员可以轻松的对涉密计算机进行设置、管理。使系统本身的可伸缩性更好。

### 2、关键技术指标

1. 浏览器记录支持：IE、Firefox、Chrome、Opera、QQ、Sougou、UC、360、猎豹、世界之窗、桔子
2. 文件格式支持：office系列（doc、docx、xls、xlsx、ppt、pptx、pps），wps系列(wps、et、dps)，rtf、pdf、txt，网页系列(html、htm、mht)
3. 图片类型支持：jpg、jpeg、tif、tiff、bmp、dib、png、gif
4. 压缩文件类型支持：zip、rar、7z、tar、iso
5. 检查结果导出格式：html、pdf、word、excel
6. 常规检查项效率：37个常规检查项检查时间≤2分钟
7. 图片检查效率：平均单个图片检查分析时间≤2秒钟
8. 普通文档检查效率：平均每分钟扫描检查文件数量≥370个
9. 文件轻度检查耗时：平均终端文件轻度检查耗时≤90分钟
10. 深度检查磁盘效率：平均每分钟检查磁盘空间≥10GB
11. 普通文档类识别率：普通文档类识别率≥95%
12. 图片文档类识别率：图片文档类识别率可达到70%
13. 系统响应时间：用户登录管理页面≤3秒
14. 终端检查并发数量：终端检查并发检查数量≥5000
15. 服务器上线数量：最大一次性上线数量≥8000
16. 客户端空闲资源占用：CPU占用率≤10%，内存占用率≤100MB
17. 浏览器兼容支持：覆盖IE、Chrome、Firefox浏览器

### 3、对项目技术架构和技术实现途径的要求

系统的技术架构分为客户端、通信总线（服务器）、管理控制中心、数据库服务、集成服务和浏览器用户交互入口组成。

1）客户端：客户端试安装在计算机终端的代理程序，通过TCP/IP协议接收来自通信总线（服务器）下发的检查任务或命令策略，将命令交付到代理程序的控制引擎统一控制调度完成任务或命令策略执行；在有代理程序的业务模块）完成结果采集后，统一汇总到控制引擎，进行数据预处理后，经TCP/IP通信连接发送给通信总线（服务器）；

2）通信总线（服务器）：通信总线（服务器）是数据处理和转发中心，通过JDBC数据库连接协议，监视发现数据库服务中任务和策略命令，根据分发范围和配置要求，转发到相应的客户端；通过TCP/IP协议接收客户端的上报的执行结果数据，进行统一的数据存储处理。通信总线（服务器）可以根据业务规模需要进行动态扩容增加负载，以保障客户端通信的承载能力。

3）管理控制中心：管理控制中心是管理员进行任务管理、策略下发、配置管理和数据结果查看的管理入口。管理控制中心采用经典的MVC设计模式，严格区分展示层、业务模型层以及数据库持久层，保持松耦合可扩展的技术架构。管理控制中心通过标准JDBC数据库连接协议，将任务、策略、配置、命令等数据存储到数据库中。

4）数据库服务：数据库服务是通信总线（服务器）和管理控制中心的信息桥梁。管理控制中心通过数据库服务完成任务、命令等策略的创建，而通信总线（服务器）通过监视数据库变化，完成任务命令的接收和下发；数据库服务由统一的proxy代理完成对外的JDBC连接能力，实际数据库节点可以根据应用规模动态的增加负载节点，避免数据库单点故障和大规模数据入库或查询压力。

5）集成服务：集成服务是与其他应用系统对接集成的服务接口集合，通过提供标准WEBSERVICE接口完成数据的集成共享，也可以通过标准的SYSLOG协议、SNMP等协议完成信息或通知发送，以保障系统信息集成能力。

6）浏览器：浏览器是管理员进行管理和数据查看的软件入口。本系统通过对IE内核、GOOGLE内核及Firefox内核类型浏览器的HTML5渲染兼容调优，支持普遍的浏览器兼容技术要求。

7）**全面兼容：**全面支持Microsoft Windows 2000/XP/2003/Win 7（32位、64位）/Win 8（32位、64位）/WIN10(32位、64位)操作系统。

8）**日志管理：**详细记录系统的运维日志及管理员操作日志，对日志进行分类管理，包括用户登录日志、账户管理日志、检查任务日志、系统管理日志、业务操作日志、日志管理记录等，支持对日志进行查询及日志导出。

9）检查系统客户端以服务形式运行在终端主机上。采用多模匹配进行敏感文档识别、通过OCR技术进行图片识别、通过MFT深度磁盘扇区级检索进行深度扫描。检查结果结果通过SOCKET加密通信以xml的形式报送给服务器。服务器对收到的xml数据进行解析，并进行数据库存储。

**1.客户端静默运行：**客户端采用c++语言开发，以服务的形式运行在终端计算机上，不影响用户的正常办公，设置开机自启动，开机后自动连接服务器，自动上线无需做任务设置。同时客户端使用进程守护机制，防止客户端程序被非授权停止或非正常卸载，保证客户端完整性。

**2.数据通信加密：**客户端从服务器接受检查任务以及向服务器上传检查结果均通过网络传输，为保证检查任务数据和检查结果数据不被非法或恶意窃取，客户端和服务器通信数据加密后传输，客户端发送前首先进行编码加密，服务器收到数据后进行解密解码，再进行数据库存储。

**3.数据库安装轻量化：**为了降低实施和维护难度，数据库采用MYSQL，开源、跨平台、高性能。MySQL数据库是开放源码的免费数据库，无版权隐患，可以针对不同的应用进行相应的修改；同时支持AIX、FreeBSD、Linux、Mac OS、NovellNetware、OpenBSD、OS/2 Wrap、Windows等多种跨平台操作系统； MySql是一个快速、多线程、多用户的SQL数据库服务器，用多线程能很容易充分利用CPU，提高性能，可以方便地支持上千万条记录的数据库； MySql通过主从复制技术实现高效读写，通过在主服务器（master）和从服务器（slave）之间切分处理客户端查询的负荷，可以得到更快的数据读取速度。

**4.多引擎并发检查：**在进行文件敏感信息检查时采用多模式匹配算法，能够同时进行多个关键字的搜索和匹配，搜索多个关键字增加所用的时间与搜索单个关键字的时间基本相同，避免搜索时间线性增长，大大提高了效率。同时，针对文件检查采用多引擎并发提速，使用多个进程同时进行检查，进一步提高检查速度；引擎的个数根据当前计算机资源的利用情况动态分配，当CPU内存占用高时，少开一些进程；当CPU内存资源占用低时，多开辟一些进程，在不影响用户正常办公的情况下达到资源的最佳利用，提高检查效率。

**5.深度检查：**文件被清楚后，无法被操作系统访问，但其文件名及文件内容仍残留在磁盘分区中。根据NTFS、FAT等文件系统数据访问的基本原理，可检索出的关键字所在扇区号及占用簇号，遍历磁盘分区目录树，与各节点占用簇块空间进行交叉比对，返查得到关键字所在文件全路径。实现对文件的深度检查。返查后文件分为两类文件：可恢复文件(包括正常文件、被删除但文件信息仍然完整的文件)和不可恢复文件（文件碎片或目录）。可恢复文件均可根据关键字对其进行定位，进而恢复整个文件；而对于不可恢复文件，也可以恢复文件所在扇区的残留信息。

 对磁盘深度信息检索，改进多项深度信息（如深度关键字检索、U盘深度记录、深度上网记录、深度文件操作记录等）检索算法；对同一扇区块中深度信息进行同时挖掘，避免对磁盘的多次遍历造成的检查效率瓶颈；实现深度多信息检索的横向合并，提升深度信息检索的总体效率。

对虚拟机文件及镜像文件,也采用深度检查的方式，在不打开虚拟机及镜像的情况下对虚拟机及镜像文件进行二进制检查，检查虚拟机及镜像文件中的上网信息、敏感文件信息及USB使用记录信息，提高检查效率。

### 4、项目验收及质保期

合同签订后60个工作日内交付所有功能并接受验收。

项目验收须达到如下要求：

产品测试完成，正常运行，符合项目要求。

项目免费质保周期为 3年。

### 5、付款方法和条件

签订正式合同后，按照如下验收节点，支付中标额的 %，具体要求为：

（1）在签定合同后，支付中标额的30 %。

（2）项目终验完成后3 个工作日内，支付中标额的 60 %；

（3）项目运行 1 年后，支付合同剩余10% 款项。

### 6、售后维护要求

（1）对项目使用培训的要求

投标方需根据用户需求不断改进系统功能和性能，应针对本项目的最终用户和系统运行维护用户提供分层次培训。需提供灵活多样的培训方式，对运行维护人员的技术培训等。

应制定详细的人员培训方案，培训方案应包括培训目的、培训时间安排、人员层次、人数、次数、培训课程（包括课程介绍）主要内容（列出培训基本内容）培训组织方式等。

对于提供的所有培训，必须保证师资力量。

培训的内容及方案应由双方协商制定。供应商前来进行技术培训的人员的费用包括在合同总价中。

（2）对项目售后服务的要求

在项目实施地点要有售后服务机构。

提供移动检查硬件设备，在服务期内，应始终通过现场服务、电话服务、远程服务等方式提供快速、高效的维护服务。

服务期内须提供所供软件系统的系统BUG修复、系统性能优化等服务。

协助提供系统数据备份服务，并定期检验数据备份的有效性。

投标人在投标时须提出软件系统及运行环境的定期维护计划，对采购人要求的不定期维护提出响应措施。

技术支持方面，提供7×24小时的技术咨询服务，每年提供至少2次对系统运行状况的评估服务，提供每月1次巡视服务，检测软件系统及运行环境的运行情况。

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1小时；中断时间不能超过3小时。

质保期三年

## 四、项目与学校信息化总体框架兼容的要求

注意：

此部分要求是学校所有信息化项目必须执行的基本技术要求，原则上不允许删减，如有特殊要求需要删减，须报学校网络安全和信息化办公室审批，项目申请单位可根据项目具体情况增加或细化要求。

以下相关要求须最终列入正式合同条款。

所有投标人须按照以下各小节的技术要求分项应答，明确具体的技术实施方案。如不予应答或未给出具体实施方案，则视为不满足招标要求。

### 1、系统对接要求

本软件是专用安全软件不需要和相关系统对接

（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。

本项目为成品安全防护软件，不完全按照此类要求

### 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。

本项目为成品软件，不完全按照此类要求

## 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。