**中国科学院动物研究所**

**协同办公平台系统二期项目需求说明**

**中国科学院动物研究所**

**二零二二年四月**

**目 录**

[1 系统需求 2](#_Toc101883114)

[1.1 采购内容 2](#_Toc101883115)

[1.1.1 技术要求 2](#_Toc101883116)

[1.1.2 功能要求 5](#_Toc101883117)

[1.1.3 优化调整要求 6](#_Toc101883118)

[1.1.4 集成要求 6](#_Toc101883119)

[2 数据备份及灾难恢复 7](#_Toc101883120)

[2.1 文档附件数据备份及恢复 8](#_Toc101883121)

[2.2 数据库数据备份及恢复 8](#_Toc101883122)

[3 系统安全要求 9](#_Toc101883123)

[3.1 防范SQL注入 9](#_Toc101883124)

[3.2 业务安全设计 10](#_Toc101883125)

[3.3 数据安全设计 11](#_Toc101883126)

[3.4 过程安全 12](#_Toc101883127)

[3.5 设备安全 12](#_Toc101883128)

[3.6 日志分析 12](#_Toc101883129)

[4 项目管理要求 12](#_Toc101883130)

[4.1 实施要求 12](#_Toc101883131)

[4.2 培训要求 13](#_Toc101883132)

[4.3 验收 13](#_Toc101883133)

[4.4 售后服务 13](#_Toc101883134)

[5 实施计划和组织保障 14](#_Toc101883135)

[5.1 项目管理要求 14](#_Toc101883136)

[5.2 有效沟通 组织保障 15](#_Toc101883137)

[5.3 风险分析与应对策略 15](#_Toc101883138)

[6 知识产权 15](#_Toc101883139)

# 系统需求

## 采购内容

### 技术要求

|  |  |  |
| --- | --- | --- |
| **参数性质** | **技术指标名称** | **技术指标和性能参数** |
| 系统要求 | 部署环境 | 1)服务端可运行在Windows及Linux系统上；支持虚拟服务器，同时能够提供对32位和64位的部暑；  2)数据库支持Oracle、SqlServer、MySQL等数据库；  3)须部署在研究所VPN环境，支持公网移动端访问。 |
| 开发架构 | 1)系统开放性良好，能够支持跨平台的应用构建； |
| 稳定性要求 | 终端支撑 | 1)浏览器适用于市面上常用浏览器，如1E、Firefox、360、Chrome、Safari 等常见浏览器；  2)终端支持常用终端设备：PC、Android、IOS等，支持设备包括智能手机、IPAD。能自适应各种不同屏幕尺寸大小的型号手机。 |
| 稳定性能要求 | 1)具有365X24小时稳定运行能力，支持集群部署，避免意外的系统异常状态；  2)最大并发用户数：1000；  3)系统的年可用率不低于99.9%； |
| 响应速度要求 | 1)1000用户同时并发时系统响应速度不高于3秒； |
| 扩展性要求 | 个性化要求 | 1)最大限度地满足研究所的个性化管理要求，内部的个性化设置和二次开发相互独立，同时也方便管理员的管理和维护，减轻运行成本;  2)能够实现与中国科技云通行证、新一代ARP系统、邮件系统的集成。 |
| 二次开发要求 | 1)须按研究所要求，与其它应用系统进行对接，提供部分预留的其他应用系统接口或提供健全的二次开发接口，便于研究所未来进行二次开发；  2)提供二次定制及开发所需的完整应用工具、接口和文档。 |
| 表单管理 | 表单管理 | 1) 表单定制工具要求以可拖拽的图形化界面方式实现表单的定制和编辑,能够对各种表单字段类型进行处理，同时要求表单的定制与组织架构无缝结合，在表单定制操作上要求具有较强的可用性和便利性；并提供系统自带的html编辑器，维护方便；  2) 表单可视化的编辑，表单内容在数据库里面以字段形式存储，方便后期数据再利用。  3) 表单上内容和字段有权限控制，表单上可以关联人，关联流程，关联历史数据，便于应用和功能之间的协作；  4)表单内的数据不仅能来源于系统内部也能获取到其他业务系统内的数据，使得一张表单可以涵盖多套系统的数据，并可以作为审批依据，其次，表单也可以被其他异构系统调用，完成协同办公平台与业务系统之间数据的相互交互。  5)只要经过简单培训的工作人员都可以自己动手制作表单； |
| 工作流程 | 工作流程引擎 | 1)工作流系统必须采用可拖拽的图形化设计器，实现流程定制功能，同时要求流程的定制与组织架构绑定;工作流系统能够具备对复杂流程模式的支持，如并行、回退、条件分支等，  2)工作流系统还必须具有联动性，即可以将诸多关联时间与数据，可以通过流程之间的数据关联；  3)流程实现版本管理，可随时对流程进行维护，且不会影响历史数据;  4)提供丰富的消息提醒机制，提升处理效率; 如系统内消息提醒、短信提醒、邮件提醒等；  5)系统支持自定义接口，满足对异构系统的数据集成; |
| 文档管理 | 文档管理 | 1)能够对技术资料、质量体系文件、标准、规章制度资料文件进行统一的管理；  2)支持灵活的查询，支持全文检索；  3)支持对文档的审批流程； |
| 报表管理 | 报表管理 | 1)提供可视化的报表设计功能，可以方便的设计业务报表和统计报表；  2)要求支持各种常见的格式，包括表格，直方图、饼图等多种格式的图表;支持多种统计方式;  3)报表的结果可以另存为Excel或HTML格式的文件。 |
| 系统管理 | 组织机构 | 要采用图形化的工具定义组织机构图，管理者根据工作流使用者在不同工作流程中需要完成的任务，为其赋予角色。 |
| 权限管理 | 与组织机构相结合，建立权限控制和管理体系，确保系统用户对系统资源的访问受到保护和控制 |
| 日志管理 | 包括日志监控、日志审计和日志统计，系统中发生的所有对数据产生变更的操  作和系统本身的运行检测情况都要被记录在平台日志中。 |
| 故障监视和诊断 | 必须保证所选择的软件能够及时发现故障并发出告警，能够自动恢复系统,不影响任何已建立的业务连接。 |

### 功能要求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **业务功能** | **一级列表** | **二级列表** |
| 1 | 业务流程 | 财务管理 | 收入认领流程 |
| 所内劳务费报销线上审批流程 |
| 科研平台 | 生物医学伦理审查流程 |
| 成果转化 | 成果转移转化审批流程和成果转移转化奖励流程 |
| 2 | 科研绩效管理 | 科研成果采集 | 17类成果数据批量导入 |
| 17类成果数据添加，修改，删除、查询 |
| 17类成果数据核对 |
| 自动计算成果得分 |
| 考核结果确认 |
| 成果数据导出 |
| 科研业绩统计 | 研究组总分统计 |
| 研究组得分详情 |
| 业绩考核结果 |
| 组员得分详情 |
| 功能配置 | 研究组管理 |
| 绩效参数管理 |
| 绩效年度管理 |
| 3 | 数据资源中心平台（仅科研绩效管理数据集部分） | 对外接口 | 接口实时配置 |
| 接口实时测试 |
| 数据资源存储（仅科研绩效管理数据集） | 关系型数据库建设 |
| 非关系型数据存储建设 |
| 数据采集 | 写入接口/数据整合 |
| 写入数据的管理/清洗 |
| 4 | 数据可视化及分析 服务（仅科研绩效管理数据展示服务部分） | 所级数据展示 | 全研究所层面的，基于数据资源中心平台对外接口的数据可视化展示 |
| 特定人员/岗位的数据展示 | 特定人员/岗位层面的，基于数据资源中心平台对外接口结合科研绩效管理业务权限的数据可视化展示 |
| 5 | 与中国科技云集成 |  |  |
| 6 | 与协同办公平台一期集成 |  |  |

### 优化调整要求

根据业务需求，对一期中的流程进行调整优化，做到业务流程引擎的灵活可配置。

根据实际使用需求，对部分平台固有功能进行优化升级，包括浏览器兼容性、安全性、与办公软件对接兼容性等。

### 集成要求

* **与外网协同平台一期的集成**

协同办公平台二期建设内容需基于一期建设基础之上，进行功能完善与延伸，充分考虑必要的集成，本期功能模块需集成到协同办公平台一期平台中。

* **统一身份认证（与中国科技云通行证集成）**

中国科技云通行证是基于中国科技云的统一账号系统，协同办公平台二期需实现与中国科技云通行证的集成，实现统一身份认证，使得用户使用中国科技云通行证账号即可登录协同办公平台二期。

* **与新一代ARP系统集成**

外网协同平台二期实现从中国科学院ARP系统同步信息。根据新一代ARP发布的最新接口进行调整。

**组织架构维护**

根据ARP接口规范，与ARP系统进行组织机构及人员信息的同步。

根据实际管理机构，建立协同办公平台二期中的组织机构与ARP系统中的组织机构对应关系。

因ARP系统中无岗位信息，须在协同办公平台二期中完善岗位信息，并维护人员信息与相应的岗位信息的对应关系。

**人员信息同步**

当ARP系统中新增人员或者变更人员信息时，协同办公平台二期进行同步。其中包括ARP提供的人员基本信息与人员详细信息。

# 数据备份及灾难恢复

在协同办公平台二期中所涉及到数据主要是分为两部分：

一是在系统中的文档，所涉及到的文档附件如pdf附件、ppt附件等等，以及所涉及到的图片资料，这方面的数据存放于应用服务器中的目录文件中；

二是在系统中的关系型数据，如文档目录的架构、流程的信息等等，这方面数据是统一存放于数据库中；

所以针对协同办公平台二期数据的备份与恢复也就需要分别对这两方面的数据进行预案设计。

## 文档附件数据备份及恢复

这部分数据是存放于应用服务器中。

* **文档备份**

系统中文档备份，可以通过系统直接完成。

* **文档的恢复**

文档数据恢复，直接把文件备份目录下的数据全部拷贝至文件存放目录下。

* **数据网络备份**

手动备份可以直接通过操作系统中的备份工具进行操作；

自动备份可以利用的操作系统的“任务计划”的功能来实现或者利用外界的备份工具。

## 数据库数据备份及恢复

这部分数据是存放于数据库服务器中, 由数据库提供的维护工具进行维护。

* **完全备份**

选择作为维护计划的一部分来备份数据库，备份的时间为每日进行。

进行数据文件的完全备份，并将备份文件放到不同于数据文件的磁盘上，可使系统崩溃造成的损失减小到一天以下。

* **事务日志备份**

将事务日志作为维护计划的一部分进行备份。

事务日志备份对将数据库恢复到故障点是必需的。并使数据库日志文件空间得到重用。

* **将报表写入目录中的文本文件**

将每日数据库维护的日志报表存入文件，报表包含维护计划执行步骤的细节，包括任何错误信息。使数据库管理员能够掌握数据库维护操作的执行情况。

* **数据的恢复**

直接将数据库备份数据恢复到系统中或者通过软件工具方式来实现。

和使用安全。并配合研究所完成系统的定级及等保测评工作。

# 系统安全要求

系统的安全来源于对系统的有效控制与管理，主要体现在整个系统运营的过程安全、权限管理、日志分析、业务复核、数据的安全以及多维度安全措施使用。

协同办公平台一期已经过等保备案并进行测评，二期建设的过程和部署过程应遵守研究所相关管理规定及安全规范，保证在建设期间和建设结束后，该系统的等保安全情况不低于建设前。

## 防范SQL注入

为了避免 SQL 注入的出现，在项目实施过程中需要正确地使用 PreparedStatement 方法或者存储过程，尽量避免在 SQL 语句中出现字符串拼接的操作，减少对数据的机密性、完整性和可用性产生的影响。

## 业务安全设计

对于系统的业务安全来说，系统在以下几个方面对安全性方面进行了相应的设计：

对关键数据的加密存放，如用户、操作员的密码等；

（1）在访问控制方面，对信息资源进行分级管理的基础上，配置安全策略，控制对敏感和重要信息资源的操作，在应用程序的开发过程中，对权限控制、登录规则、密码规则、URL权限、SQL注入、XSS攻击等做相应的处理，实现对应用系统的访问控制。

（2）对关键数据的流水日志记录，系统严格的留痕设计，对于重要的操作均采用独立的流水记录，保证相关业务的发生均有相应的流水记录，保存处理时的关键信息；而对于一般性的操作，则通过日志记录的方式，确保重要的信息能得以保存，供后续的查证使用；

（3）对业务操作的严格权限检查，任何业务的操作，在应用服务器处理层，均需进行相应的功能权限检查，防止一切非法的调用，确保系统的业务处理的安全性；

（4）对业务操作的严格控制性检查，可设置用户、操作员的限制，设置客户与操作员可操作的对象限制等；

（5）对业务可自定义复核设计，可通过对业务操作的参数化定义，来设置对业务处理的不同等级的复核要求，防范意外事件的发生；

（6）对系统的运行监控设计，可监控系统的网络状况、业务处理情况以及数据交换的情况等，从而可有效地及时发现异常事件的发生。

## 数据安全设计

在数据安全方面：系统在设计上充分考虑到业务稽核的需要，在数据库后台表的设计中，通过对关键数据表增加校验字段来保证数据的客观公正；通过对关键数据根据系统提供的加密方式加密后存放，可保证即使是数据库管理人员也无法从表中直接查询到关键数据；通过对各业务表之间的逻辑关联，确保非法的数据修改可通过数据间的关联关系得以查找。 数据安全还表现在数据的一致性和可稽核性方面：首先系统所有操作均有留痕，这是可稽核的首要条件，另外，系统的数据记录是连续的、互相关联的，并且充分平衡的。

* 身份认证方面

口令采用不可逆加密算法及种子加密保存，口令无法还原成明文。通过配置系统安全策略（复杂程度要求等），实现登录失败处理功能。

* 业务安全

在核心业务的流转中使用图片验证码，防止核心业务被非法用户采用工具恶意攻击。

* 信息安全

在框架级解决方案中防止SQL注入，框架采用多层架构避免数据库的提示信息直接反映到页面；SQL书写采用中对输入变量采用转义处理，以防SQL注入，避免暴露数据库信息。Cookie信息采用签名、加密处理，防止非法用户截获cookie信息后进行破解。

## 过程安全

系统的设计考虑了对数据流的过程安全控制、客户身份的认证、操作人员的身份认证以及操作权限的严格控制等各个方面。通过对这些方面严格的数据检查，可防止非法的数据入侵、账号盗用、非法操作等。

## 设备安全

保障了结构安全、业务安全、数据安全、过程安全后就必须考虑设备稳定性，硬盘，网卡损坏，断电等安全问题，系统运维监控系统自动对设备的运行情况进行监控。

## 日志分析

日志分析包括系统分析及业务分析。 业务分析指所有用户对数据的操作（添加，更改，删除）都要需要审计，内容应包括操作人，时间，操作类型，更改内容，操作结果。任何应用、任何权限的操作人都不能对操作日志进行更改。同样，针对某些业务，也可有针对性进行必要的日志分析，分析其相应用户的行为。

# 项目管理要求

## 实施要求

本项目要求合同签订后90天内完成实施，正式上线前试运行一个月。为保证项目按时按质顺利进行，应建立专门的项目开发组和管理组，由专人负责。提供详细的项目实施时间表和各阶段各方人员安排及相关的工作内容;提出完整、合理、可行的项目管理计划，其中包括关于项目进度控制、质量控制、风险控制、文档管理以及与本项目相关的协调工作等的详细描述。

项目实施中必须根据研究所需求进行开发设计、实施，以满足研究所部门间信息共享的需求。

## 培训要求

本项目中要对研究所人员提供技术培训，包括操作人员培训和管理维护人员培训。投标人应在投标文件中提出培训计划，计划包括培训类别、培训项目、人数、时间、地点及培训方式等详细内容，达到使相关人员熟练使用系统的目的。

## 验收

在整体项目正式上线运行一个月无故障后即可申请项目验收。中标人要提供详尽的项目验收方案，包括验收组织、验收内容、验收标准、验收报告等。

## 售后服务

项目通过验收之日起，必须提供至少一年的原厂免费维护、升级服务，若有升级版本须及时通知用户，是否升级由用户决定;免费服务期结束后，投标人应提出升级、维护服务方案，并对服务内容、费用、方式、范围等方面进行承诺，另行签订服务合同。

保证有专门的客户服务机构和人员，能够提供7\*24小时电话服务响应;对于必须派人现场解决的问题，保证在收到现场服务通知后，6小时内到达现场。

在服务期内，根据研究所的业务需求变化进行二次开发和本地化服务，在需要与其他系统实现对接或者数据交互时，配合第三方做好技术衔接工作。

为本项目提供定期健康检查服务，在服务期内每两月进行一次产品巡检和用户回访，并组织用户、厂商，进行技术交流，提高整体维护水平，减少故障隐患。

# 实施计划和组织保障

## 项目管理要求

供应商须为本项目组建稳定的、专业的、独立的项目团队，专门负责本项目服务实施工作，并进行相关的项目管控和随时调整项目实施方向。投标人须针对本项目成立专门的项目组，确保人力、物力的投入，项目组成员必须稳定，项目实施团队成员在项目终验前如果人员退出或更换，需要征得招标人同意。

项目经理须具备丰富的协同办公系统建设经验，具有快速解决问题的能力，有较高判断故障和管理协调的能力，具有项目管理相关认证资质证书，至少具有3年以上协同办公平台的项目经验，能够深刻理解协同办公平台工作内容。

## 有效沟通 组织保障

项目启动后实行每周项目进展书面报告，每月现场汇报沟通制度，以确保项目进度的有序正常推进。若遇重大问题可根据需要随时召开项目沟通会议进行决策。

## 风险分析与应对策略

充分认识和预见到风险的存在，并及时有效地制定措施以避免风险、缓解风险、管理风险，保障项目成功。人员组织方面项目承担方要确保开发支持团队的人员稳定。技术架构方面要采用业界成熟稳定的技术平台。部署实施和上线切换阶段要确保提前做好相关预案，有效规避实施过程风险，做好风险防控工作。

# 知识产权

协助甲方申请《绩效管理系统》软件著作权一个。