附件1

**杭州师范大学**

## 网络数据安全保密协议书

甲方：杭州师范大学

乙方：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

乙方受甲方委托对\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目（以下简称“项目”）进行建设、测试、运营或运行维护。为保障甲方的网络和数据安全，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，以及杭州师范大学各项管理制度的要求，甲、乙双方本着平等、自愿、公平和诚实信用的原则签订本协议，达成如下协议：

## 一、保密范围

1.乙方为甲方提供信息化建设、运维服务所涉及的合同、协议或存在事实合作、服务关系的项目开发、维护工程活动。

2.乙方为服务甲方而了解、掌握的甲方网络、服务器等各类硬件、场地环境、信息系统、各类账号、业务数据、安全防护措施、项目建设过程资料等网络数据信息，以及直接或间接了解的学校发展规划、业务运行机制、师生身份隐私信息、文件、资料、档案等甲方核心信息。

3.甲方依照法律规定(如在缔约过程中知悉其他相对人的商业秘密)和在有关协议的约定(如技术合同)中对外承担保密义务的事项，也属本保密协议所称的专有信息秘密。

## 二、网络数据安全义务

1. 乙方应按照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，以及杭州师范大学各项管理制度的要求，履行网络和数据安全保护义务。

2. 项目涉及的乙方工作人员均需签订《杭州师范大学网络数据安全承诺书》，签订之后方可为甲方提供项目服务，且乙方应对项目涉及工作人员进行背景审查、加强安全意识培训，及时调整不合适的人员。

3.乙方工作人员离岗或不再从事本项目相关工作后，乙方应立即终止相关工作人员在本项目相关信息系统的权限，取回各类与甲方相关的软硬件设备，工作人员离岗时，乙方需办理严格的手续，承诺调离后的保密义务方可离开。

4. 乙方应当采取技术措施和其他必要措施，确保甲方的网络和数据安全，所开发维护的信息系统需满足信息安全等级保护二级及以上的要求，防止信息泄露、损毁、丢失。在发生或者可能发生信息泄露、损毁、丢失的情况时，应当立即采取补救措施，并在第一时间告知甲方。

5. 项目中所包含的建设、运营、运维的信息系统、应用、数据库等，开通相关账号权限必须经过甲方审批允许，乙方不得私开账号、擅自更改权限等，权限设定应当遵循最小授权要求，乙方的所有主机维护操作需通过甲方的堡垒机完成。

6. 乙方应合理使用操作账号，严禁乙方存在多名工作人员共用操作账号的情形，同时各类账号应采用高强度的密码，严禁使用系统默认密码或多个高校相同密码，并定期更新账号密码。

7. 未经甲方允许，乙方不得对服务器私开端口，严禁在服务器中随意安装非官方的有安全风险的软件，严禁在系统建设中私设“后门”，非法访问系统或转移、加工系统数据，不得利用学校提供的资源进行与该项目无关的工作。乙方应当告知并采取有效措施要求其参与项目服务的员工遵守本协议规定。

8. 乙方应严格按照要求采集、使用、处理、交换、共享数据资源。做好数据落地相应的数据保护工作，严格执行数据安全技术标准和安全管理措施，避免相关数据出现泄露、窃取、篡改的风险。项目相关设备从甲方运回乙方二次销售或回收前，乙方应清除其中所有相关数据。

9. 乙方应认真组织开展各项数据处理活动，查找项目数据安全隐患和漏洞，对薄弱环节和潜在威胁采取有力措施进行整改，避免和消除数据安全风险，履行数据安全保护义务。

10. 乙方应加强网络和数据安全风险监测，制定网络数据安全应急预案，完善应急机制。发现系统与数据安全缺陷、漏洞等风险时，立即采取补救措施;发生网络数据安全事件时，立即采取处置措施。确保第一时间检测发现，第一时间应急处置，第一时间向甲方报告。

11. 乙方应及时响应、处置甲方布置的安全工作，对其主管的服务器操作系统、数据库、应用服务、组件、云资源等的安全事件、隐患及时阻断、排查、处置、溯源(包括但不限于攻防演练等相关活动中发现的安全隐患或漏洞)。

12. 项目中所建设的系统、提供的基础设施服务等，乙方应无偿提供操作手册、告警流程、安全资产清单，并按照规范要求实现与甲方相关平台实现对接，提供相关解析（如日志字典等) 供甲方进行安全审计。

13. 未经甲方书面批准，乙方不得以直接或间接方式向第三方透露甲方相关保密信息，包括本项目的相关文件、技术方案、实施计划、经费预算等相关信息，以及学生、教职工信息、统计数据等各类信息。乙方不得将上述信息进行买卖，牟取不正当利益。

14. 乙方应采取一切合理必要措施，防止甲方的信息泄露、损失或被盗用。如发生信息泄露、损失或被盗用，乙方应立即通知甲方并采取补救措施。

15. 对于甲方向乙方提供的计算机信息系统登录用户名和密码（包括但不限于服务器、VPN账号、邮箱账号、上网账号等），乙方仅用于维护使用，不得擅自做其他用途或泄露给第三方。

16. 乙方应在项目建设过程中，严格遵守国家法律法规和行业标准，确保甲方数据的安全。乙方承诺不利用甲方提供的信息化设备制作、复制、发布、转摘、传播含有下列内容的信息：

（1）反对宪法基本原则的；损害国家荣誉和利益的；

（2）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（3）煽动民族仇恨，民族歧视，破坏民族团结的；

（4）破坏国家宗教政策，宣扬邪教和封建迷信活动的；

（5）散布谣言，扰乱社会秩序，破坏社会稳定的；

（6）散布淫秽、色情、赌博、 暴力、凶杀、恐怖或者教唆犯罪的；

（7）侮辱或者诽谤他人，侵害他人权益的；

（8）含有法律法规禁止的其他内容的；

17. 乙方不得利用甲方提供的网络侵犯国家的、社会的、集体的或甲方的利益和公民的合法权益。

18. 乙方不得利用甲方提供的计算机和网络系统发送垃圾邮件、攻击其他网络和计算机系统，传播计算机病毒，以及进行其他危害互联网信息安全的行为。

19. 乙方应提高保密意识，不得与业务无关的任何人在公开场合、社交软件、电子公告系统、网络新闻上谈论、发布和传播甲方项目相关信息或甲方敏感信息。

20. 乙方应制定数据的备份策略和恢复策略，定期对甲方的数据进行备份，并进行数据备份恢复演练，确保数据的完整性和可恢复性。在项目完成后，乙方应将甲方数据完整、无损地交还给甲方，不得在乙方留存甲方项目相关的数据副本。

21.乙方不将涉密计算机联入非涉密网络；不在涉密计算机上连接和使用非涉密移动存储设备；不在非涉密计算机上连接和使用涉密移动存储设备。

22. 乙方应定期对甲方项目相关的信息系统进行安全检查和维护，定期安装系统的最新补丁程序，及时发现并修复安全隐患。

23.乙方在项目建设及服务过程中，应确保项目文档由专人负责保管，确保项目文档的使用受到控制，甲方提供给乙方的保密信息，乙方应指定专人接收、登记、返还。

24. 甲乙双方因故不能实施本项目，甲方有权收回所有项目相关资料，乙方不得私自保管、转移、复制。

## 三、知识产权保护

1. 乙方在项目开发过程中产生的所有知识产权，除另有约定的，均归甲方所有。

2. 未经甲方书面批准，乙方不得将甲方的知识产权转让、许可或以其他方式处置给任何第三方。

## 四、违约责任

1. 乙方任何人员有任何违反本协议条款行为的即构成乙方违约，乙方应向甲方支付项目合同价款的30%作为违约金。给甲方造成损失的，甲方有权追究其法律责任并要求赔偿相应损失。构成犯罪的，将移交司法机关并追究其刑事责任。

2. 如因乙方原因导致甲方网络安全事件或数据泄露、损失或被盗用，乙方应承担全部法律责任，并赔偿甲方因此造成的损失。

## 五、争议解决

1. 本协议的签订、履行、解释及争议解决均适用中华人民共和国法律。

2. 双方在履行本协议过程中发生的争议，应首先通过友好协商解决；协商不成的，任何一方均有权向有管辖权的人民法院提起诉讼。

## 六、其它条款

1. 本协议一式两份，甲乙双方各执一份。协议自乙方签字盖章之日起生效。

2. 本协议未尽事宜，可由双方另行签订补充协议。补充协议与本协议具有同等法律效力。

甲方（公章）：杭州师范大学 乙方（公章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

负责人（签字）：\_\_\_\_\_\_\_\_\_\_\_

日期： 年 月 日 日期： 年 月 日