**供应商安全责任与保密承诺函**

南昌大学：

我司(公司名称)根据与贵单位的约定，将为贵单位提供\_软件或者系统服务名称(服务时间： 年 月—— 年 月)。为落实供应链安全责任，防范网络安全重大风险，我司已组织相关人员学习本承诺函及附表所列内容，并知悉相应要求。承诺如下：

1. **通用承诺**
2. 我司不利用提供产品、服务的便利条件非法获取贵单位数据、非法控制和操纵贵单位设备，无正当理由不中断产品供应或必要的服务，不利用贵单位对产品的依赖性谋取不正当利益或迫使贵单位更新换代。
3. 我司为贵单位供应的产品、服务中未设置恶意程序和后门程序，没有任何可能导致泄密的风险装置且不存在安全漏洞。
4. 我司向贵单位供应的产品、服务不存在任何侵犯第三方及其授权许可人的知识产权情形。如含有商标、专利或者著作权等内容，我公司为合法的权利人或者授权许可人。
5. 我司保证拥有提供本合同约定服务的安全相关资质及许可，包括但不限于各类行政许可。
6. **开发安全承诺**
7. 安全检测。我司向贵单位供应软件产品或为贵单位定制开发系统时，我司将对提供的产品、系统开展安全检测、风险测评或源代码安全审计，并将向贵单位提供相关证明报告。
8. 源代码管理。我司承诺，将做好源代码的安全管控，防止源代码泄露。我司不将贵单位源代码托管至可公开访问的第三方代码平台，如需托管在不可公开访问的第三方代码平台时，我司应取得贵单位的事先书面同意并采取源代码安全管控措施，包括不限于访问控制、安全审计、安全防护策略等，防止人员违规访问源代码库。我司将加强源代码管理和技术资料泄露监测工作，及时发现违规在开放式代码管理平台、共享文档平台、网盘等上传、托管和存储情况，及时清理处置，采取措施消除影响并开展泄露溯源。合同或协议关系解除后，我司将及时删除贵单位相关源代码，不以任何方式保存或转移。
9. 漏洞管理。我司将加强产品或系统安全缺陷、漏洞的检测与监测，其中包括第三方、开源组件的相关缺陷、漏洞。对于已知缺陷、漏洞，我司将按照国家相关法规要求妥善处置，如涉及贵单位，将立即书面通知贵单位，准确传达缺陷、漏洞等风险，并协助贵单位进行整改与修复。同时对贵单位安全缺陷、漏洞等信息严格进行保密，在未经贵单位允许情况下绝不将其提供给第三方。不利用安全缺陷、漏洞信息等攻击贵单位信息系统。
10. 开发管理。我司将制定开发管理制度，明确开发过程的控制方法、管理流程、人员行为准则和代码安全规范等，并定期对相关人员开展安全开发培训。
11. 环境隔离。为贵单位提供开发服务或定制化产品时，如在我司场地实施，我司将对开发环境实施物理隔离，并对开发、测试、生产网实施有效隔离，对无线网络进行安全控制，避免开发、测试人员通过无线网络将贵单位相关源代码及敏感信息文件私自上传至互联网。
12. 知识产权。我司供应的产品或服务应用在贵单位关键信息基础设施时，承诺对产品和服务研发、制造过程中涉及的实体拥有或控制的已知技术专利等知识产权获得10年以上授权，或在产品和服务使用期内获得持续授权。
13. **交付安全承诺**
14. 我司承诺，将制定物流安全监督措施，保障交付给贵单位的产品物流安全，将采用可信或可控的产品分发、交付和仓储手段等。我司向贵单位提供产品、服务相关的技术文档时，将保证交付渠道的安全性。
15. 经贵单位认定的对关键信息基础设施、重要网络、大数据具有重大影响的核心部件，我司将提高物流安全等级，并及时将存储、交付、物流等信息报告贵单位。
16. 我司供应的产品或服务应用在贵单位关键信息基础设施时，将提供中文版运行维护、二次开发等技术资料。
17. **维护安全承诺**
18. 我司将对服务贵单位的维护人员开展安全培训、对维护人员行为进行监督与权限控制、利用合同或协议约束人员安全行为等。
19. 如在我司场地提供维护服务时，我司将采取控制手段，包括不限于记录维护的时间、人员、维护情况，对维护人员的权限审核与控制等。
20. 我司将严控人员权限管理，严禁我司人员非授权开展维护工作。
21. **数据安全承诺**

我司在供应产品、服务过程中，涉及接触或处理贵单位数据的，如客户个人信息、业务生产数据、重要工作文件、其他重要数据、系统源代码等，将履行下述承诺：

1. 我司具备符合贵单位要求的数据安全能力，保证采取适当的数据安全技术与制度措施充分保障贵单位数据的安全性、以及贵单位与相关信息主体的合法权益。我司保证该服务结果不会侵犯任何个人隐私、第三方商业秘密等其他合法权利。
2. 我司保证有权限处理(处理行为包括：收集、存储、使用、加工、传输、提供等)贵单位数据的我司工作人员于提供服务前接受数据安全相关专业化培训和考核，在服务期间内每年至少接受一次数据安全方面的相关培训；我司将妥善留存培训记录以供贵单位随时调取，保证我司工作人员均参加数据安全相关培训。
3. 我司将遵循法律法规、国家及行业标准以及本合同有关数据保护的相关约定，仅为本合同之目的处理贵单位数据。我司对贵单位数据的处理行为不超出贵单位的授权范围。
4. 我司将准确记录处理贵单位数据的情况，并依据贵单位需求定期或不定期向贵单位提交数据处理工作报告。我司数据处理工作报告的内容应包括但不限于我司处理贵单位数据的时间、场景、目的、行为、涉及的数据类型与字段，我司处理贵单位数据所采取的数据安全措施，我司负责处理贵单位数据的工作人员等。我司同意贵单位有权对我司进行现场或非现场检查，确保我司数据处理方式与安全要求一致。
5. 未经贵单位书面授权，我司不将贵单位授权我司开展的贵单位数据处理事项委托或提供给任何其他机构。如贵单位书面授权我司委托或授权其他第三方机构处理贵单位数据的，我司将保证其他机构具备符合贵单位要求的数据安全能力，在处理贵单位数据时采取相应的数据安全技术与制度措施保证数据安全，并就其合作机构的数据处理行为承担连带责任等。
6. 如我司或我司委托或授权的其他第三方机构发生与处理贵单位数据有关的数据安全事件，将立即以书面形式向贵单位报告，并迅速开展数据安全影响评估与安全事件调查，积极采取或配合贵单位采取止损措施，防止影响范围进一步扩大。
7. 我司保证对贵单位数据的收集、使用、存储(如适用)、销毁等处理行为均在中华人民共和国境内进行。
8. 我司保证采用加密、脱敏等安全措施传输数据，采取有效技术防护措施确保贵单位数据安全，防范贵单位数据传输过程中被第三方截获和利用。
9. 未经贵单位书面授权，我司不得存储、使用和共享其加工处理的贵单位数据或产生的服务成果(包括但不限于程序、文件、资料等)。我司为履行本合同约定而必须存储、使用和共享贵单位数据或产生的服务成果时，应获得贵单位书面授权，并向贵单位提供具备数据安全保护能力和对相应数据等采取保护措施的书面证明材料。
10. 如贵单位书面授权我司在履行本合同约定范围内存储贵单位数据的，我司将采取措施使贵单位数据与我司其他数据有效隔离，保证仅限于有权限的我司工作人员能访问贵单位数据。
11. 我司将根据“业务需要”和“最小权限”原则，对贵单位数据的访问操作进行满足业务最小数据集的访问控制，并记录访问日志和全过程监控。
12. 如我司在贵单位指定场所驻场提供服务，我司将遵守贵单位数据安全保护制度要求，未经贵单位书面授权不得以存储、传输等方式处理贵单位的任何数据。
13. 我司承诺在合同终止后立即将获取的贵单位数据及相关衍生数据进行销毁并向贵单位为提供证据证明，不得以任何方式留存贵单位数据及相关衍生数据。我司承诺具备完善的数据销毁机制，对销毁过程保留记录以供贵单位调取。同时履行以下义务：
14. 返还包含贵单位数据及衍生数据信息的文件和资料，包括不限于复制件、电子文档等；
15. 销毁无法返还的包含贵单位数据及衍生数据信息的文件和资料，包括不限于复制件、电子文档等；
16. 提供一份书面声明，确认已销毁所有包含贵单位数据及衍生数据信息的文件、资料、电子文档和相关复制件，并附销毁材料清单。
17. **人员安全承诺**
18. 我司向贵单位提供服务时，我司将建立服务贵单位的人员台账并向贵单位报备，包括人员基本信息、联系方式、工作职责、在职离职情况、系统和服务权限等，台账将动态维护。
19. 我司将向服务贵单位的我司人员告知相关保密义务，并与其签署书面保密协议，使其承担不低于合同约定的及本承诺函承诺的保密义务。
20. 对于可接触贵单位关键信息基础设施、重要网络和大数据系统的我司服务人员，我司将开展人员背景调查和保密审查，调查结果应获得公安机关确认，并将调查结果、证明材料加盖公章后反馈贵单位，证明材料包括不限于人员的缴税证明、在职证明、学历证明、项目经历证明、社保证明、无犯罪证明、保密协议等。
21. 我司将组织服务贵单位人员，定期开展教育培训活动，提升人员安全意识，包括不限于制度规范、安全培训、应急流程、内部攻防演练等。在贵单位场地提供服务时，我司将制定符合贵单位管理要求的安全保密、工作场所行为规范等管理制度，并应组织我司服务人员学习上述制度。
22. 当服务人员离职时，我司将建立离职人员账号、权限、材料等交接、清理流程，并具有完整的离职交接记录。
23. **运行安全承诺**

我司为贵单位研发并运营的系统，如涉及贵单位重要数据或客户个人敏感信息，因特殊情况暂时不能在贵单位内部署时，我司将加强网络与信息安全、数据安全管理，如涉及第三方云平台，将密

切跟踪第三方云平台内重要组件的更新管理，必要时对第三方云平台开展安全审计，我司将加强系统的安全防护和加固，并尽快组织向贵单位内迁移和部署。

**八、连续性承诺**

1. 我司将加强物理与环境安全，将提供必要的应急和灾备资源保障，强化备品备件管理，确保提供贵单位的产品、服务的持续性和可恢复性。
2. 根据贵单位认定，如我司属于重要等级产品、服务供应商，我司将针对安全类、运营类、管理类等事件进行分级分类，制定事件的监测发现、分析研判、上报、处置等措施。
3. 我司将加强与供应链上下游企业联动协同，密切关注上下游企业情况，做好风险防范与应急处置，根据贵单位需要，可向贵单位定期汇报上下游企业情况，防范供应链风险。
4. 根据贵单位认定，如我司属于重要等级产品和服务供应商，我司将制定供应链安全事件的应急响应预案，预案场景将至少包括供应链攻击、供应中断、敏感信息泄露等，预案中将明确，为贵单位提供应急响应和恢复的优先级为最高级，应急预案将定期报送贵单位。
5. 根据贵单位认定，如我司属于重要等级产品和服务供应商，我司将开展企业内部的应急演练。演练完成后，形成演练报告，评价演练效果，分析风险和不足并提出整改措施，及时整改，演练报告、问题发现及整改情况报送贵单位。同时我司将配合参加贵单位的应急演练。
6. **保密承诺**

我司与贵单位合作期间，如果我司以书面、介质或口头形式获得贵单位某些非公开的、保密的、专业的数据及相关衍生数据、服务成果等(以下统称“保密信息”),包括不限于涉及的客户个人信息、业务生产数据、重要工作文件、其他重要数据，密码本、网络拓扑图、系统源代码等信息(详见附表《保密信息范围》)。我司承诺对附表所列的贵单位保密信息承担下述保密义务：

1. 在保密期内，对保密信息保密，未经贵单位书面同意，不将保密信息用于合同以外的目的，并不将其泄漏给任何第三方，不将数据以任何形式转移、挪用或谋取合同约定以外的利益，不下载、分析和存储贵单位保密信息，不将保密信息带离贵单位/我司办公场所，而且我司应防止贵单位保密信息被销毁、丢失或改变。
2. 我司不出售、转让贵单位保密信息。不在公共场所或私人通信中谈及贵单位保密信息。不进行其他可能导致贵单位保密信息泄漏的活动。
3. 不利用合作之便获取贵单位与合作无关的保密信息。不利用贵单位保密信息从事损害贵单位利益和声誉的活动。
4. 我司人员如在为贵单位服务期间离职，不带走任何贵单位保密信息，在保密协议规定的保密期内不泄漏任何贵单位保密信息。
5. 如果法律规定或监管机构要求我司必须对保密信息或由保密信息得出的任何意见、判断等信息做出披露时，在法律允许的情况下，我司立即书面通知贵单位，以使贵单位能选择采取保护措施。且我司在披露前或披露时尽最大努力为被要求披露的保密信息获取保密措施或保密待遇，并将披露范围严格限定在有权机关或法律法规所要求必须披露的范围之内。
6. 我司承诺上述保密义务的期限为永久，保密义务不随双方合作的终止而终止。
7. 我司同意，贵单位对所透露的保密信息有权不附带任何种类的保证。
8. 我司同意，对于我司因使用贵单位提供的保密信息而使我司受到的任何损害，贵单位无需承担赔偿责任。

**十、风险管理承诺**

1. 我司将根据贵单位要求，配合提供供应链产品及服务的相关信息，包括不限于版本、型号、生产厂商、开发类型、涉及的操作系统、是否有信息回传厂商、回传信息主要内容、联系人等基本要素。对于我司提供的产品、服务中包含的第三方或开源产品，我司将提供使用的第三方或开源产品信息。
2. 我司将积极配合贵单位的风险评估、监测、检查和审计等工作以及国家有关部门和监管机构的检查，并根据贵单位或国家有关部门或监管机构的整改要求及时纠正，整改结果将定期向贵单位汇报。
3. 我司承诺将做好网络安全保护工作，落实供应链安全责任，防范网络安全重大风险，保证不因我司及我司人员原因，导致外界获取贵单位保密信息或导致贵单位发生网络安全事件。
4. 供应链产品供应和服务过程中发生以下重大风险事件时，我司将立即向贵单位书面报告：
5. 贵单位重要数据或客户个人信息泄露；
6. 贵单位数据损毁或者重要业务运营中断；
7. 由于不可抗力或我司重大经营、财务问题，导致或可能导致多家银行保险机构产品或服务中断：
8. 产品或服务非正常中断、终止或我司非正常退出；
9. 因我司不当行为或信息系统遭受网络攻击或其他原因，造成贵单位客户重大资金损失；
10. 发现重大的我司违法违规事件；
11. 国家及监管机构发现的其他重大事件。
12. 我司原因造成贵单位保密信息的泄露或发生贵单位网络安全事件时，我司将立即开展处置，最大限度降低影响，保障贵单位及客户权益，同时我司将承担相应责任。
13. 如我司或我司人员违反本承诺函的承诺，则贵单位有权采取以下措施中的一项或几项：
14. 要求我司立即停止侵害。
15. 暂停、中止或终止与我司的合作或我司所提供的服务，并要求我司退还已支付款项及同期存款利息。
16. 要求我司采取有效措施防止泄密范围及贵单位损失的扩大。
17. 要求我司赔偿给贵单位造成的直接和间接的损失和费用(包括但不限于律师费用、仲裁费用和执行费用等)。
18. 其他进一步追究我司法律责任的权利。
19. 如违反上述承诺，我司愿意承担相应的法律责任。

**附表：保密信息范围**

公司 名称

\_\_\_年\_\_\_月\_\_\_日

(多页请加盖骑缝章，如为联合体投标或代理商，原则上应由原厂商盖章)

**附表：保密信息范围**

A、除贵单位书面表明为非保密信息外，我司从贵单位获取的所有息及材料，不论是书面、口头、磁记录、光学记录、电子记录还是其它记录形式都属于保密信息，包括但不仅限于:

1. 所有与贵单位的业务、经营、计划、交易、市场、财务、目前或将来拟采用的经营方式、财务、交易、信托资产等有关的不被公众领域所知的文件资料和信息。
2. 所有贵单位计算机应用系统的IT规划、软件设计方案、数据结构、设计方案、实施方案、技术细节、实现方式、设备参数配置、操作监控手段、数据加密算法、源代码、系统日志、密码本等相关信息和技术文档。
3. 所有贵单位计算机设备、网络设备、存储设备、安全设备、监控设备的参数配置、IP 地址、口令、操作监控手段等相关信息;计算机主机系统和网络设备运行记录、运行报告及应急方案等。
4. 所有贵单位的生产数据、业务数据、生产经营信息及贵单位客户信息等相关信息。
5. 所有贵单位网络规划、网络架构、网络、IP 地址信息及运行维护方案等相关信息。
6. 所有贵单位信息安全规划、策略、设计、实施方案等信息安全方面的相关信息。
7. 所有贵单位的工程实施文档、项目文档、管理文档等。
8. 所有贵单位及上下级单位的采购需求、采购计划及与第三方厂商签订的合作协议等信息。
9. 我司在工作过程中发现的贵单位系统、管理流程中存在的洞、缺陷
10. 我司在对贵单位进行服务时提交的工作成果。

B、贵单位的保密信息不包括:

1. 已成为公共知识或可通过其他正当公开渠道获得的信息。
2. 我司从有权披露该信息的第三方合法获得的且我司对之不负有保密义务为信息。
3. 我司独立于本承诺确定的保密信息而自主开发出来的文件、资料和信息。