**北京工商大学供应商信息安全管理办法**

1. **总则**

第一条 为加强对供应商的信息安全管理，明确管理责任和管理要求，抵御外来风险，提高供应链安全管理水平，根据《中华人民共和国网络安全法》、《网络安全审查办法》、《信息安全技术 ICT供应链安全风险管理指南》(GB/T 36637-2018)等法律法规，结合北京工商大学实际情况，特制定本办法。

第二条 采购信息化通用软硬件产品、软件定制开发、硬件定制开发以及各类信息化运行维护、咨询规划、安全服务，可能影响北京工商大学网络安全的，应当按照本管理办法进行供应商安全审查，并签订相关文件。

第三条 供应商安全管理工作坚持防范安全风险与促进北京工商大学信息化发展相结合、过程公平公正公开与知识产权保护相结合、事前审查与持续监管相结合、供应商承诺与北京工商大学审计相结合，从供应商背景、从业人员、产品、服务等可能给北京工商大学带来安全风险的方面进行审查。

第四条 本办法适用于北京工商大学所有网站及信息系统。供应商信息安全管理工作重点审查供应商产品、服务和人员的安全性、可控性，主要包括：

（一）产品和服务使用后带来的被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；

（二）产品和服务供应中断对业务连续性的危害；

（三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；

（四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；

（五）供应商派遣的相关管理人员、技术人员的人员安全风险；

（六）其他可能危害北京工商大学网络安全的风险。

第五条 采购符合本办法第二条范围内的产品、服务的北京工商大学各业务部门为供应商安全管理工作第一责任人，北京工商大学对其安全管理工作情况纳入北京工商大学各业务部门年度网络安全绩效考核。

1. **供应商选择与审查**

第六条 供应商选择。

（一）制定供应商选择策略和制度,根据产品和服务重要程度对供应商开展安全调查。

（二）应对关键产品和服务供应商实行筛选，与产品和服务供应商进行合作时，应综合考虑以下几方面因素：

1.优先选择满足下列条件的供应商：保护措施符合法律法规安全要求，组织运转过程和安全措施相对透明，对下级供应商、关键组件和服务的安全实行进一步核查，在合同中声明不使用有恶意代码产品或假冒产品,使用可信任的员工；

2.交货周期短且稳定；

3.使用可信或可控的分发、交付和仓储手段；

4.限制从特定供应商采购产品和服务。

（三）供应商选择和管理过程中包含在能提供相同产品的多个不同供应商中做选择，以防范供应商锁定风险。

第七条 供应商应当在与各业务部门开展合作前充分了解本管理办法规定，并书面承诺按照本管理办法规定配合北京工商大学的供应商管理工作：提交相关材料、接受相关审查、接受人员监督和管理、提供相关整改工作，并承诺若出现违反本管理办法规定时接受北京工商大学的处罚。

拟签订合同的供应商必须是依法设立的专门从事相关业务的公司，而且公司中境内单位或个人持有股权或股份不少于51%。供应商股东或关联公司原则上不得包含境外控股企业，如因项目需求而须与该供应商合作的，应当从严开展审核工作。

供应商为各业务部门提供的产品或服务应当符合国家相关法律法规的要求，按照强制性国家标准进行生产或服务。法律法规规定应当具备产品或服务资质的，供应商应当提供相关证明。

第八条 供应商审查。对于申报供应商安全审查的采购活动，各业务部门应通过采购文件、协议等要求产品和服务提供者配合安全审查并告知其相关责任文件内容，包括承诺不利用提供产品和服务的便利条件非法获取数据、非法控制和操纵设备，无正当理由不中断产品供应或必要的技术支持服务、遵守北京工商大学相关网络安全管理规定、签订必要网络安全责任文件等。

在供应商合同期间内，各业务部门应当切实按照本管理办法开展对供应商的审查、安全监督管理工作，并每年形成供应商安全管理工作报告，上报至网络安全与信息化领导小组，并接受小组的复审和抽查。

供应商应向各业务部门提交以下材料：

（一）供应商安全审查申报书；

（二）拟合作供应商的背景分析报告；

（三）采购文件、协议、拟签订的合同等；

（四）供应商拟派遣的人员信息；

其他需要提供的材料。

第九条 各业务部门应对上报的材料进行审查，审查内容包括但不限于：

（一）供应商背景、股东及关联公司情况；

（二）供应商三年内违法情况；

（三）供应商三年内违反网络安全法律法规被行政处罚的情况；

（四）采购文件、协议、拟签订的合同；

（五）供应商的管理人员、工程技术人员等相关人员国籍、公民身份、资质，关键岗位人员审核是否存在过失、犯罪记录；

（六）安全保密承诺、网络安全责任书、网络产品、供应商对信息系统、组件和服务的设计、开发、实施、验证、交付、支持过程等；

（七）开发信息系统、组件或服务时接受的安全培训和积累的经验情况；

（八）供应商产品或服务资质相关证明；

（九）其他相关内容。

供应商为各业务部门提供的产品或服务应当符合国家相关法律法规的要求，按照强制性国家标准进行生产或服务。法律法规规定应当具备产品或服务资质的，供应商应当提供相关证明。

各业务部门认为有必要追加审查材料的，应当告知供应商。各业务部门自收到材料后10个工作日内确定是否开展审查工作，并书面通知申报方。各业务部门认为需要开展审查的，应当自受理之日起30个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送申报方；情况复杂的，可以延长15个工作日。

第十条 供应商应在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并在签订的协议中明确能力要求。

第十一条 建立供应商分类分级管理机制，针对不同类型的供应商建立相应的管理和风控策略，对重要供应商和一般供应商采取差异化管控措施。

第十二条 各单位与供应商及人员应签订网络安全责任书、安全保密承诺、安全保密协议（可作为合同附件）。

在与供应商签订的合同或协议中应当明确以下内容，包括但不限于：

（一）服务范围、服务内容、服务要求、工作时限及安排、责任分配、交付物要求、验收准则以及后续合作中的相关限定条件，服务质量考核评价约定。要求产品和服务供应商制定用户文档，可涵盖以下信息：

1.产品和服务的安全配置，以及安装和运行说明；

2.与管理功能有关的配置和使用方面的注意事项；

3.有助于用户更安全地使用信息系统、组件或服务的方法或说明；对用户安全责任和注意事项的说明。

（二）合规、内控及风险管理要求，对法律法规及北京工商大学内部管理制度的遵守要求。

（三）服务持续性要求，供应商的服务持续性管理目标应当满足业务连续性目标要求。

（四）对供应商进行风险评估、监测、检查和审计的权利，及供应商承诺接受北京工商大学对其所承担的外包服务的监督检查。

（五）合同变更或终止的触发条件，合同变更或终止的过渡安排。

（六）外包活动中相关信息和知识产权的归属权以及允许供应商使用的内容及范围，对供应商使用合法软、硬件产品的要求。

（七）资源保障条款。

（八）安全保密和消费者权益保护约定，包括但不限于：禁止供应商在合同允许范围外使用或者披露北京工商大学的信息，供应商不得将北京工商大学数据以任何形式转移、挪用或谋取外包合同约定以外的利益。相关工作人员应严格履行各自的安全角色和职责，主要包括依法依规保护北京工商大学重要数据和公民个人信息、不得非授权或恶意访问北京工商大学相关系统和数据，主动报告所发现的安全事件或其他风险。

（九）争端解决机制、违约及赔偿条款。

（十）报告条款，至少包括常规报告内容和报告频度、突发事件时的报告路线、报告方式及时限要求。

第十三条 应当在合同或协议中明确要求供应商不得将外包服务转包或变相转包。在涉及外包服务分包时应当要求：

（一）不得将外包服务的主要业务分包；

（二）主供应商对服务水平负总责，确保分包供应商能够严格遵守外包合同或协议；

（三）主供应商对分包供应商进行监控，并对分包供应商的变更履行通知或报告审批义务。

第十四条 供应商应提供操作系统、中间件、应用程序等安全配置的详细记录，如操作系统安全配置、操作系统加固、中间件安全配置、应用默认安全配置等。供应商需妥善保存第三方系统所有系统信息、客户信息、操作日志等，保存期限不少于6个月。

1. **准入机制**

第十五条 各业务部门应有效识别供应商服务所涉及的主管部门、业务类型、业务名称、业务环节、重要数据和客户个人信息、供应商机构、服务说明、主要风险、现有管控措施等方面，涉及重要数据和客户个人信息的应纳入业务支持实施有效的安全管控。

第十六条 第三方系统需与内部系统互联时，应提交系统架构图，经信息网络中心审核通过后进行连接。第三方系统在入网前必须通过安全评估和安全测试，确保第三方系统符合内部系统安全技术要求。

第十七条 供应商在北京工商大学以往的服务项目中出现过重大的信息安全违规事件，不得再引入该合作公司。

1. **风险管理**

第十八条 源代码安全管控

（一）源代码包括开发人员自行编写实现功能的程序代码，相应的开发设计文档及相关资料，全部须纳入源代码管理体系，基于身份和口令授权访问，不得未经学校授权进行修改、删除、上传外网等操作。

（二）对于因合作需要，向外复制、传播源代码的情形，需与对方签订保密协议，明确对方应当承担对源码保密的责任和义务。

（三）在应用系统上线前，对开发单位提供软件源代码中可能存在的恶意代码通过第三方的检查工具或人工进行审查，并保留相关检查报告。

第十九条 产品开发生命周期管理流程

（一）规范产品由规划设计到终结使用的全生命周期的安全管理要求，在构建、部署、操作和使用时考虑产品的安全性，并在开发周期内不断检测产品可能存在的安全缺陷。

（二）在设计之初，做好产品的架构、风险分析和评估，确认其符合规格说明书、系统架构图和设计方面的安全条例，确保产品的可靠性规范、保险性规范和安全性规范。

（三）产品上线进行安全性测试，从物理环境、网络传输、数据库系统和管理人员等方面进行安全测试、应急演练、综合评估，保证各个层面均落实安全措施。

（四）产品的设计、研发、交付、使用、废弃等各阶段，以及制造设备、工艺等的风险进行及时更新，并根据风险调整相应制度、策略和措施。重点项目、服务、产品应当预留有充足的备件，可在关键组件断货后维持到新的关键组件到货。

（五）要求供应商对其交付的网络安全产品实行安全配置，并在安全组件、安全服务重启或重装后进行安全默认配置。

第二十条 应建立并持续完善风险管理制度和流程，充分识别并评估信息系统外包可能产生的风险，包括但不限于：

（一）业务中断。支持业务运营的外包服务无法持续提供导致业务中断。

（二）数据泄露、丢失和篡改。因供应商的不当行为或其服务的信息系统遭受网络攻击，导致北京工商大学重要数据或用户个人信息泄露、丢失和篡改。

（三）服务水平下降。由于外包服务质量问题或内外部协作效率低下，使得信息系统服务水平下降。

可能导致的战略、声誉、合规等其他风险。

第二十一条 针对可能给业务连续性管理造成重大影响的重要外包服务，应当事先建立风险控制、缓释或转移措施，包括但不限于：

（一）事先制定退出策略和供应链安全保障方案，并在外包服务实施过程中持续收集供应商相关信息，尽早发现可能导致服务中断或服务质量下降的情况；

（二）明确措施和方法，在供应商质量不能满足合同要求的情况下，保障获取其外包服务资源的优先权；

（三）要求供应商提供必要的应急和灾备资源保障，制定应急处理预案并在预案中明确为北京工商大学提供应急响应和恢复的优先级，原则上应为最高级；

（四）组织供应商参与应急计划编制和应急演练，至少每年在综合性演练或专项演练中纳入一个或多个供应商开展一次相关演练；

（五）考虑预先在北京工商大学内部配置相应的人力资源，掌握必要的技能，以在外包服务中断期间自行维持最低限度的服务能力。

第二十二条 应当制定和落实网络和信息安全管理措施，包括但不限于：

（一）对供应商和外包人员进行网络和信息安全教育或培训，增强网络和信息安全意识，供应商应与北京工商大学签订安全保密协议，外包人员应签署安全保密承诺书；

（二）明确外包活动需要访问或使用的信息资产，按“必需知道”和“最小授权”原则进行访问授权，严格管控远程维护行为；

（三）对信息系统开发交付物（含拥有知识产权的源代码）在上线前进行安全扫描和检查（包括源代码审计、漏洞扫描、专业的第三方安全测试等）；

（四）对客户信息、源代码和文档等敏感信息采取严格管控措施，对敏感信息泄露风险进行持续监测；

（五）对供应商所提供的模型、算法及相关信息系统加强管理，确保模型和算法遵循可解释、可验证、透明、公平的原则；

定期对外包活动进行网络和信息安全评估。

第二十三条 应识别具有集中度风险的外包服务及其提供商，积极采用分散外包活动、注重外包项目知识产权保护、提高自身研发运维能力、储备潜在替代供应商等手段，减少对个别外包供应商的依赖，降低集中度风险。

第二十四条 应当对符合重要外包标准的非驻场外包服务进行实地检查，原则上每三年覆盖所有重要的非驻场外包服务。对具有行业集中度性质的供应商，可采取联合检查、委托检查等形式，减少重复性工作，减轻供应商的检查负担。

第二十五条 每年应当至少开展一次全面的信息系统外包风险管理评估，并向学校网络安全与信息化领导小组提交评估报告。

第二十六条 应当开展信息系统外包及其风险管理的审计工作，定期对信息系统外包活动进行审计，至少每三年覆盖所有重要外包。发生重大外包风险事件后应当及时开展专项审计。应承担内部审计职能和责任，内部审计项目可委托上级主管单位或聘请独立第三方实施。

第二十七条 应考虑重要外包终止的可能性，并制定退出策略。退出策略应至少明确：

（一）可能造成外包终止的情形；

（二）外包终止的业务影响分析；

（三）终止交接安排。

1. **安全机制**

二十八条 供应商在交付产品或服务时，应当使用可信或可控的分发、交付和仓储手段，并且在运输或仓储时使用防篡改包装或手段。各业务部门或供应商发现使用（或所提供）的网络产品、服务存在安全缺陷、漏洞等风险时，及时采取措施消除风险隐患，并向网络安全与信息化领导小组报告。

第二十九条 各业务部门应建立明确的信息系统及网站外包服务目录、服务水平协议以及服务水平监控评价机制，确保相关监控信息和评价结果的真实性和完整性，且数据至少保存到服务结束后三年。

第三十条 各业务部门应当对外包服务过程进行持续监控，及时发现和纠正服务过程中存在的各类异常情况。常见指标包括：

（一）信息系统和设备及基础设施的可用率；

（二）故障次数、故障解决率、故障的响应时间、故障的解决时间；

（三）服务的次数、客户满意度；

（四）业务需求的及时完成率、程序的缺陷数、需求变更率；

（五）外包人员工作饱和率、外包人员的考核合格率；

（六）网络和信息安全指标、业务连续性指标。

当监控到信息系统外包服务出现异常情况时，应当及时督促供应商采取纠正措施；情节严重或未及时纠正的，应当及时约谈供应商高管人员并限期整改。对于逾期未整改的供应商，应当暂停或取消其服务资格。对于关联外包，应当将外包服务质量纳入对供应商的业绩评价范围，建立外包服务重大事件问责机制。

第三十一条 各业务部门应当定期检查供应商的服务涉及的网络链路、安全设备、网络设备和服务器等的运行状况，审查供应商的服务涉及的安全策略、审计数据、恶意代码、补丁升级等安全相关事项的工作情况。

第三十二条 各业务部门应当根据不同重点时期，依据网络安全关注重点对供应商服务进行专项的信息安全检查和审查，确保供应商的服务的可用性和数据的可靠性。

第三十三条 应当对供应商的财务、内控及安全管理进行持续监控，关注其因破产、兼并、关键人员流失、投入不足和管理不善等因素引发的财务状况恶化及内部管理混乱等情况，防范外包服务意外终止或服务质量的急剧下降。

第三十四条 当供应商安全管理办公室监控到信息系统外包服务出现异常情况时，应当及时督促服务提供商采取纠正措施；情节严重或未及时纠正的，应当及时约谈供应商高管人员并限期整改。对于逾期未整改的供应商，应当暂停或取消其服务资格。

第三十五条 对于关联外包，应当将外包服务质量纳入对供应商的业绩评价范围，建立外包服务重大事件问责机制。

第三十六条 应在信息系统外包服务到期前，就是否继续外包进行评估决策。外包服务结束时，应对供应商进行评价，评价结果作为供应商后续准入的重要参考依据。对具有持续性特点的外包服务，终止外包或更换供应商前，应制定周密的退出和交接计划。

1. **违规处置**

第三十三条 供应商不配合北京工商大学开展的供应商安全管理活动的，如未签订合同，则不予其开展后续合同签订工作；如已签订合同，供应商应当按照本管理办法规定开展整改工作，如供应商拒不整改或整改不合格的，则取消合作，依法要求供应商赔偿北京工商大学损失。

第三十四条 对在采购、审查、管理过程中出现违规的供应商，视情节轻重由供应商安全管理办公室商讨并决定是否列入供应商黑名单。被列入黑名单的供应商三年内不得直接或间接参与北京工商大学采购活动。

第三十五条 参与供应商安全管理工作的相关机构和人员应严格保护企业商业秘密和知识产权，对供应商提交的未公开材料，以及审查工作中获悉的其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或用于安全管理以外的目的。

1. **附则**

第三十六条 本制度的解释权归北京工商大学信息网络中心。

第三十七条 本制度自发布之日起生效。