北京工商大学数据安全管理办法

**第一章 总 则**

 **第一条**为了维护学校安全、全体师生的公共利益，保护全体师生和各学校组织在网络空间的合法权益，保障个人信息和重要数据安全，根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》、《中华人民共和国数据安全法》等法律法规，结合我校数据资源管理办法，特制定《北京工商大学数据安全管理办法》。

**第二条**学校进行数据资源和信息系统建设中开展数据资源管理、采集登记、共享开放和开发利用及其相关管理活动，适用本办法。涉及国家秘密的数据管理，按照国家、部省和学校有关规定执行。本办法所称数据，是指学校及各单位通过各类信息系统或通过第三方产生、采集、获取的数据，包括人事、教学、科研、财务、资产等业务数据，网络、防火墙、系统日志等日志数据，视频，图片等媒体数据以及其他数据。

**第三条** 在北京工商大学校内利用网络开展数据收集、存储、传输、处理、使用等活动（以下简称数据活动），以及数据安全的保护和监督管理，适用本办法。纯粹家庭和个人事务除外。法律、行政法规另有规定的，从其规定。

 **第四条** 学校采取措施，监测、防御、处置来源于中华人民共和国境内外的数据安全风险和威胁，保护数据免受泄露、窃取、篡改、毁损、非法使用等，依法惩治危害数据安全的违法犯罪活动。

 **第五条** 数据安全管理工作由学校网络安全和信息化领导小组（以下简称“领导小组”）统一领导，北京工商大学信息网络中心（以下简称“信息网络中心”）负责全校数据安全管理工作的归口管理，负责数据安全策略的制定、执行和监督，指导、协助各部门开展数据安全防护工作的落地。

 **第六条** 信息网络中心按照有关法律、行政法规的规定，参照国家网络安全标准，履行数据安全保护义务，建立数据安全管理责任制度，制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估，制定网络安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。

**第二章 数据安全保障责任主体**

**第一条** 信息网络中心是数据安全管理制度统筹执行的责任主体，按照有关法律、行政法规的规定，参照国家网络安全标准，履行数据安全保护义务，建立数据安全管理责任制度，制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估，制定网络安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。

**第二条** 信息网络中心是服务器硬件、网络、存储相关硬件资源和信息通道的安全保障责任主体，具体实施操作系统病毒检测、网络安全检测和感知、校内网络访问权限的划分和控制等基础环境及物理层面做好数据安全防护工作。

**第三条** 信息网络中心是数据平台、服务平台、身份认证平台等校级综合信息化软件平台的数据安全工作责任主体，负责校级数据平台的数据安全等级划分、数据共享需求审核流程制定和执行、信息化系统安全策略制定等系统层面的数据安全工作。

**第四条** 各职能部门、教学院系、科研机构是生产数据和使用数据的责任主体，各部门应指定数据安全责任人，责任人应该具有足够的信息化专业素养和能力，并对本部门的数据情况具有足够的了解，能够对数据现状、数据流向、信息系统内数据安全保障措施等内容提供咨询、解释，并协助信息网络中心落实相关的数据安全管理工作。数据安全责任人参与有关数据活动的重要决策，直接信息网络中心的主要负责人报告工作。数据安全责任人履行下列职责：

* 组织开展数据安全风险评估，督促整改安全隐患；
* 按要求向有关部门和网信部门报告数据安全保护和事件处置情况；
* 受理并处理用户投诉和举报。

**第三章 数据安全细则**

 **第一条** 网络运营者通过网站、应用程序等产品收集使用个人信息数据，应当分别制定并公开收集使用规则。收集使用规则可以包含在网站、应用程序等产品的隐私政策中，也可以其他形式提供给用户。细则引用GB/T 35273-2020 《信息安全技术-个人信息安全规范》的全部内容作为保护个人隐私数据的活动依据、操作规范和行为准则。

 **第二条** 个人数据收集使用规则应当明确具体、简单通俗、易于访问，采集、使用和显示个人数据时，需遵循以下安全规则：

|  |  |  |
| --- | --- | --- |
| 数据内容 | 数据内容示例 | 安全规则 |
| 个人生物识别信息 | 包括指纹，掌纹，人脸识别数据，虹膜，DNA等 | 各部门不得主动采集、存储和使用 |
| 个人身份证件信息 | 包括身份证号、护照号等 | 由管理归口部门采集和存储。信息网络中心可留存副本，并采用加密方式存储，提供单向验证查询：即部门需要查询个人在其他系统的身份信息时，可通过单向验证（输入证件号码进行查询，但不接受输入人名反查身份证件号）进行查询。应用软件界面中，除了业务需要必须呈现完整信息之外，一般情况下不显示，或采用脱敏显示。 |
| 个人家庭信息 | 包括婚姻状态、配偶信息、家庭住址、家庭成员等 | 由管理归口部门采集和存储，信息网络中心可以留存副本，可采用明文方式存储。对有合理需求的其他部门可提供共享，共享时需经信息网络中心和管理归口部门同时审核通过。共享获批后，部门可以存储该信息的副本。应用软件界面中，除了业务需要必须呈现完整信息之外，一般情况下不显示，或采用脱敏显示。 |
| 个人联系信息 | 包括手机号，邮箱地址、钉钉号、微信号、QQ号等 | 由信息网络中心统一采集，可采用明文方式存储。可对有合理需求的职能部门共享，共享时需信息网络中心审核通过。共享获批后，部门可以存储该信息的副本。应用软件界面中，除了业务需要必须呈现完整信息之外，一般情况下采用脱敏显示。可面向本人和第三方提供双向查询服务。 |
| 个人行为记录 | 包括无线连接、上网行为、门禁刷卡记录、图书借阅记录、视频监控记录、行为轨迹等 | 由管理归口部门采集存储，信息网络中心可以留存副本，可采用明文方式存储。除国家执法机构外，一般不对其他部门或个人提供共享。应用软件界面中，除了业务需要必须呈现完整信息之外，一般情况下不显示，或采用脱敏显示。 |
| 个人在校内财务信息 | 包括薪资、补助、一卡通消费记录 | 由管理归口部门采集存储，信息网络中心可以留存副本，可采用明文方式存储。可对有合理需求的职能部门共享，共享时需经信息网络中心和管理归口部门同时审核通过。共享获批后，部门可以存储该信息的副本。应用软件界面中，除了业务需要必须呈现完整信息之外，一般情况下不显示，或采用脱敏显示。 |
| 个人医疗健康信息 | 包括就诊记录、体检报告、心理评测等 | 由管理归口部门采集存储，经审批可对有合理需求的职能部门共享。信息网络中心不主动采集及留存副本。应用软件界面中，除了业务需要必须呈现相关信息之外，一般情况下不显示。 |
| 个人在教学、科研、管理活动中产生的事件记录 | 包括政治面貌、选课，成绩，个人课表，学评教，教学任务、教学成果，科研项目、科研成果，获奖信息、项目申报、资产保管、宿舍分配等 | 由管理归口部门采集和存储，信息网络中心可以留存副本，采用明文方式存储。对有合理需求的其他部门可提供共享，共享时需经信息网络中心和管理归口部门同时审核通过。共享获批后，部门可以存储该信息的副本。应用软件界面中，可明文显示。 |

 **第三条** 数据生产部门应数据安全准则：

* 数据生产部门对外共享数据时，需严格按照《北京工商大学数据资源共享管理办法》的要求执行相应的流程才能进行，不允许出现未执行流程就进行数据共享的情况。
* 不得私下将数据导出外带，不得越权查看数据，不得越权进行数据相关的操作。
* 校外单位因工作原因需要接触或使用校内数据时，必须签署安全保密协议
* 对于个人敏感数据和组织敏感信息，在存储、传输时，需采用加密或脱敏技术进行处理，因业务需要必须采用明文方式的情况除外。

**第四条** 为减少相关账号扩散引起的数据风险，信息化系统和其后台数据库建设完成后，建设单位负责回收除后续运维工作必须的相关账号和密码，并记录备案。账号密码应遵循以下安全准则：

* 信息化系统、数据库等系统的账号应专人专用，并进行记录，不得借用、转借、发送分配给单位、个人的各种系统的账号和密码；
* 对于所有信息化硬件、信息化系统、信息化服务及数据库相关账号的密码，均应满足用强密码策略的要求，即密码组成应满足以下全部条件：1）密码长度至少大于八位；2）字母与数字混合密码；3）字母须包含大小写；

**第五条** 数据管理部门数据安全准则：

* 数据集中管理部门对外开放数据时，需严格按照《北京工商大学数据资源共享管理办法》的要求执行相应的流程才能进行，不允许出现未执行流程就进行数据共享的情况。
* 不得私下将数据导出外带，不得越权查看数据，不得越权进行数据相关的操作。
* 校外单位因工作原因需要接触或使用校内数据时，必须签署安全保密协议
* 对于个人敏感数据和组织敏感信息，在存储、传输时，需采用加密或脱敏技术进行处理，因业务需要必须采用明文方式的情况除外。
* 需采取有效的措施对重要关键数据进行备份、容灾、存档等处理，保障数据内容不会意外灭失。当发生故障或误操作时，须确保在规定时间内完成数据恢复。
* 涉及校内数据传输、网站访问时，要求采用带有传输加密和身份认证的相关协议以保障通信过程的数据安全。
* 定期对数据平台的数据使用情况进行审计和分析，发现恶意调用、随意转发等违规行为及时制止，并立即停用数据使用单位的数据共享权限。
* 在处理数据平台的数据需求申请、审核过程中，应遵循相关的安全机制，以防止权限范围外的程序及个人访问未经授权的数据，安全机制包括但不限于：权限体系、申请审核过程、限次限流措施等。
* 参照国家有关标准，采用数据分类、备份、加密等措施加强对个人信息和重要数据保护。

 **第六条** 数据使用者应该采取充分的措施保障应用和数据的安全，防止因病毒、木马等因素导致数据失窃，数据使用应遵循以下数据安全准则：

* 需要共享其他部门数据时，需严格按照《北京工商大学数据资源共享管理办法》的要求执行相应的流程才能获取数据访问权，不允许未执行流程而通过其他非正常途径获取数据访问权。在调用申请时需填写调用数据目的、需求和使用方式，由该数据归口管理部门和信息网络中心管理员按照数据安全等级进行审核。
* 数据使用者获取数据访问权后，必须严格按照申请流程所指定的应用内容、使用范围访问数据，不得将所获得的数据用于其他用途，不得超申请范围访问数据，不得将获取的数据访问权转交、泄露给任何第三方，不得将数据从流程所申请的应用中导出、复制、外传、外带。
* 对于个人敏感数据和组织敏感信息，在存储、应用、显示时，需采用必要的加密或脱敏技术进行处理，因业务需要必须采用明文方式的情况除外。
* 原则上数据需求方需通过校级数据共享平台获取校内其他单位的数据，有特殊大数据量、实时性要求的，向信息网络中心报备，由信息网络中心统一协调数据，并备案记录。

**第七条** 各部门不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人数据。个人信息主体同意收集保证网络产品核心业务功能运行的个人数据后，网络运营者应当向个人信息主体提供核心业务功能服务，不得因个人信息主体拒绝或者撤销同意收集上述数据以外的其他信息，而拒绝提供核心业务功能服务。

**第八条** 各部门在数据采集、共享、使用全过程中，应做好数据安全保障工作，做好数据资源共享风险评估和安全审查。加强数据资源安全防护和安全监测技术措施，建立数据定级及人员访问控制、信息审计追踪、安全应急处理和灾难恢复机制，对数据资源及副本建立应用日志审计，确保信息汇聚、共享、查询、比对、下载、分析研判、访问和更新维护情况等所有操作可追溯，日志记录保留时间不少于六个月，确保数据安全。

**第九条** 为防止数据因人为因素、技术故障发生的信息丢失，各信息化建设主体单位应按照如下要求开展数据备份工作，备份原则如下：

* 采用备份文件与生产库数据文件物理隔离的备份策略，防止因存储故障造成的数据丢失；
* 对最近一周内的数据每天备份：周一至周日对数据进行增量备份；
* 对最近一个月的数据，每周至少保留一个全量备份；
* 对最近一年内的数据，每月保留一个全量备份；
* 每年至少保留一个全量备份；
* 建议采用主备模式或集群模式进行数据库的部署，减少因架构问题导致的数据损失；
* 如具备条件建议开启数据库归档模式，以便快速回退数据至误操作节点；

 **第十条** 若数据需求方从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务。以经营为目的收集重要数据或个人敏感信息的，应向学校网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

 **第十一条** 针对采取自动化手段访问收集学校网站数据的情况，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

**第四章 数据处理使用**

 **第一条 数据管理部门**保存个人信息不应超出收集使用规则中的保存期限，用户注销账号后应当及时删除其个人信息，经过处理无法关联到特定个人且不能复原（以下称匿名化处理）的除外。

 **第二条** **数据管理部门**收到有关个人信息查询、更正、删除以及用户注销账号请求时，应当在合理时间和代价范围内予以查询、更正、删除或注销账号。

 **第三条** **相关部门**利用用户数据和算法推送新闻信息、商业广告等（以下简称“定向推送”），应当以明显方式标明“定推”字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。开展定向推送活动应遵守法律、行政法规，尊重社会公德、商业道德、公序良俗，诚实守信，严禁歧视、欺诈等行为。

 **第四条** 数据管理员向他人提供个人数据前，应当评估可能带来的安全风险，并征得个人信息主体同意。下列情况除外：

* 从合法公开渠道收集且不明显违背个人信息主体意愿；
* 个人信息主体主动公开；
* 经过匿名化处理；
* 执法机关依法履行职责所必需；
* 维护国家安全、社会公共利益、个人信息主体生命安全所必需。

 **第五条** 数据管理员发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报信息化建设领导小组同意；信息化建设领导小组不明确的，应经上级相关部门批准。

 **第六条** 信息系统管理员对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。第三方应用发生数据安全事件对用户造成损失的，相关管理员应当承担部分或全部责任。

 **第七条** 若数据管理职责因为职务或其它因素出现变化的，数据承接方应承接数据安全责任和义务。没有数据承接方的，应当对数据作删除处理。法律、行政法规另有规定的，从其规定。

 **第八条** 数据使用人员分析利用所掌握的数据资源，发布预测、统计信息、个人和部门等信息，不得影响国家安全、经济运行、社会稳定，不得损害他人合法权益。

**第四章 数据安全监督管理**

 **第一条** 信息网络中心在履行职责中，发现相关管理人员数据安全管理责任落实不到位，应按照规定的权限和程序约谈相关负责人，督促整改。

 **第二条** 发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，相关管理人员应当立即采取补救措施，及时以电话、短信、邮件或信函等方式告知个人信息主体，并按要求向行业主管监管部门和信息化建设领导小组报告。

 **第三条** 违反本办法规定的，由有关部门依照相关法律、行政法规的规定，根据情节给予公开曝光、没收违法所得、暂停相关业务等处罚；构成犯罪的，依法追究刑事责任。