河南工业大学信息与数据安全管理规定

第一章 总则

第一条 为进一步加强我校信息与数据的管理，实现安全、统一、共享的数据服务，有效发挥数据在教学、科研和管理工作中的重要作用，根据《中华人民共和国计算机信息系统安全保护条例》、《河南工业大学校园网管理办法》和《河南工业大学信息化建设项目管理办法 》，特制定本规定。

第二条 信息和数据的安全是指建立健全学校网络基础设施、网站、信息系统及数据内容等的安全保障体系，提高安全防护能力，保障网络、信息及内容的安全性、完整性、可用性和可控性。

第三条 数据安全管理原则

（一）统一标准原则。数据的格式及管理应符合国家、河南省、学校等制定的相关标准和规范。

（二）全程管控原则。建立从数据采集到数据消亡的全过程管控体系，确保数据真实、准确、完整、及时。

（三）安全共享原则。在保证数据安全的前提下，实现数据的共享、使用以及衍生服务。

第四条 数据管理目标

（一）保障数据完整准确：建立数据质量监督核查机制和管理规定，保障数据在各个环节的规范性、完整性和准确性。

（二）保证数据安全可靠：建立数据的分级管理与备份、容

灾机制；明确数据的所有权和管理权限，保证数据更改的可追溯性；根据相关文件要求，做好数据保密工作。

（三）提升数据服务质量：制定完善的数据服务管理规定，保证数据容易获取和使用，充分发挥数据作为学校无形资产的价值。

第二章　信息与数据建设与管理

第五条　学校网络安全与信息化领导小组对信息与数据建设进行指导和决策。信息化管理中心代表学校执行信息与数据管理工作。

第六条　信息和数据按照学校数据中心、数据生产单位、数据使用单位等组织架构进行建设与管理。信息化管理中心是学校数据中心的建设和管理单位，各单位、各部门既是信息与数据的生产单位，又是信息与数据的使用单位；其中教学、科研、财务、学工、人事、后勤等部门及相应业务信息系统是学校核心数据源。

第七条　数据中心职责

（一）定期对全校的网站及信息系统开展安全检查，针对不合格的网站或信息系统，采取及时补丁、期限整改、暂停运行访问、复查等措施，确保安全。

（二）负责对全校数据资源进行统一规划和分类。确定各类数据对应的生产单位和使用单位，保障数据来源的唯一性。

（三）建立统一的数据标准、编码标准以及相关技术规范，确保数据的一致性和标准性。

（四）负责校级信息中心库、大数据平台、信息门户等公共基础设施与平台的建设、运维和管理工作。负责信息与数据安全防护策略和数据备份、恢复及容灾方案的制定与执行，确保数据安全可用。

第八条 数据生产单位职责

（一）数据生产单位负责人，为本单位数据生产管理的第一责任人，必须确保通过信息系统完成数据全生命周期的管理工作。

（二）数据生产单位在系统建设和数据处理过程中必须遵循国家和学校发布的相关文件和数据编码标准，并严格按信息系统使用管理规定规范数据管理的相关工作。

（三）数据生产遵循“谁主管，谁提供，谁负责”原则。数据生产单位负责数据的采集、录入、审核、维护、发布、备份和归档。数据生产单位须真实、准确、完整、及时地更新数据。

（四）各类信息系统须按要求与学校统一数据平台对接，以便系统打通和数据的共享。数据生产单位不得向数据使用单位或个人直接提供数据，应由统一数据平台提供访问接口和数据服务。

（五）数据生产单位在数据交换接口完成后，需变更用于交换的数据结构时，须经过信息化管理中心申请批准后方可实施。

第三章 信息与数据使用与共享

第九条 数据的产生部门是数据维护的唯一部门。如数据发生错误、损毁，数据生产部门有责任提供最终备份数据，并以此为标准数据供数据使用部门开展后续工作。

第十条 数据的使用部门使用数据之前，需要向学校数据中心和数据产生部门提出申请，在获得批准备案授权后，方可使用。

第十一条 数据的使用部门在调用来自数据产生部门的数据时，不可以对源数据做任何改动，不可以做其他可能影响到数据源准确性的任何操作。

第十二条 数据的产生部门如需关闭数据接口，停止数据提供，需提前书面通知数据中心和数据使用部门，并由数据中心做记录备案。

第四章 信息与数据安全与保密

第十三条 遵守国家有关法律、法规，严格执行《中华人民共和国计算机信息网络安全保密规定》。

第十四条 信息中心、各厂商、校内各部门之间，需进行批量数据及有关信息交换和共享使用的，数据信息提供方和需求方必须签署数据信息使用及保密协议，明确各自使用和保密职责。

第十五条 参与信息化建设及系统维护的相关公司，学校各级信息化从业人员，未经批准与授权，不得进入非公开的信息与数据保护区域，不得接触或其他用户的相关信息数据。不得以任何形式泄漏数据中心的信息、数据、文件及账号、密码等等相关保密信息。不得使用其他用户的账号和 IP 地址等系统资源。

第十六条 各业务系统数据库管理员负责本系统数据库的规划、新建、空间分配、用户分配、操作日志的监控、数据库的

负载监控以及对数据库各项操作记录及相关资料的存档备案工作。

第十七条 业务数据必须定期、完整、真实、准确地转储到不可更改的介质上，备份数据资料保管地点应有防火、防热、防潮、防尘、防磁、防盗等设施。

第十八条 各类用户须配合信息化管理人员进行必要的安全检查。对信息系统中发生的有关安全事件，有关使用单位应在12小时内向信息化领导小组通报。

第五章 用户及密码管理

第十九条 业务系统管理员要根据工作的需要，认真制定用户权限的分配方案，方案在部门负责人签字同意并在信息化管理中心备案后执行，对于不再使用的账号需及时清理。

第二十条 管理员用户密码必须由管理机构内部人员掌握，严禁其他单位或部门人员以任何方式获取密码及相关权限。普通用户遗忘密码修改，需提供真实身份证明材料，经该系统管理员进行修改。

第二十一条 数据库密码必须通过复杂性检验。特殊情况需要他人以自己的密码进入系统时，应征得部门负责人书面同意，并在工作完成后及时修改密码。

第六章 应急方案及处置措施

第二十二条 紧急事件。

（一）学校主页、新闻网站、移动门户以及重要业务系统等

受到攻击并可能发生内容篡改或替换的事件，如:

1.影响学校系统正常运转的攻击事件，如与服务门户、教务财务系统等相关的攻击事件。

2.可能造成师生隐私信息被窃取、丢失、损坏的入侵与漏洞。

3.其他可能对学校或社会公共安全造成危害或不良影响的事件或漏洞。

应立即切断攻击来源的网络连接，并向分管领导报告，征得同意后，停止或部分停止系统运行。同时系统管理员应检查有关日志等资料，查找攻击来源并及时汇报；情况影响极为严重的，应立即向公安部门报告。

4.信息系统或数据库崩溃

应立即向部门主管领导汇报实际情况，征得同意后，业务系统管理员应及时对崩溃系统或数据库进行恢复；如无备份，应立即上报学校信息化管理部门，获取技术支持。

第二十三条 普通事件

对校内开放系统或网站的页面发生攻击或有隐藏漏洞；影响不大的攻击事件或可能造成中低隐患的漏洞；其他不构成公共危害或社会不良影响的安全事件或漏洞。

相关信息化应用管理部门应及时向信息化管理中心汇报，在信息化管理中心技术指导下，进行事件的处理。

第七章 附 则

第二十四条 本办法由信息化管理中心负责解释，自发布之

日起施行。

附件：河南工业大学数据授权与保密协议

信息化管理中心

2020-10-1

附件：

河南工业大学数据授权与保密协议

系统名称：

本着数据谁使用谁负责的原则，校内数据提供单位、校内使用单位、使用方技术支持单位三方签定数据授权与保密协议。

校内数据提供单位简称提供单位，校内使用单位简称使用单位，使用方技术支持单位简称技术支持单位，下同。

提供单位、使用单位、技术支持单位三方经平等协商同意，自愿签订本协议，共同遵守本协议所列条款。

一、提供单位授权使用单位对提供单位掌握的相关数据进行读取、复制、存储、备份、分析、挖掘。

二、使用单位应当妥善保管提供单位授权的数据，采用技术手段保证数据的保密和安全，严格要求技术支持单位做好数据保密工作。

1.保密的内容和范围

（1）涉及提供单位为使用单位提供的所有的信息化数据，包括提供单位服务器和终端计算机上的数据。

（2）凡以直接、间接、口头或书面等形式提供涉及保密内容的行为均属泄密。

2. 三方的权利与义务、责任

（1）使用单位、技术支持单位应自觉维护提供单位的利益，严格遵守本委托方的保密规定。

（2）使用单位、技术支持单位同意并承诺，未经提供单位书面许

可，使用单位不得将相关保密信息，通过存储介质、网络等途径，传播至任何其他人员或机构以及不可控制范围。

（3）使用单位、技术支持单位不得利用所掌握的数据开展商业活动及牟取私利；

（4）使用单位、技术支持单位了解并承认，提供单位将具有商业价值的保密信息保存在由使用单位维护的服务器上或终端计算机上，并且由于系统维护服务、数据备份服务等原因，使用单位、技术支持单位有可能在某些情况下访问这些服务器和终端计算机。如果这些数据未经提供单位许可，披露给他人，所造成对提供单位的直接损失，一经证实，提供单位有权通过法律途径向使用单位、技术支持单位索赔。

3. 本《协议》项下的保密义务不适用于如下信息：

（1）非由于使用单位、技术支持单位的原因已经为公众所知的；

（2）由于法律的适用、法院或其他国家有权机关的要求而披露的信息。此协议至签字之日起生效。

校内使用单位负责人（签名盖章）：

年　月　日

使用方技术支持单位负责人（签名盖章）：

年　月　日

校内数据提供单位负责人（签名盖章）：

年　月　日