

网络数据安全管理办法（试行）

第一章 总则

第一条 为了规范学院的数据安全管理，进一步完善数据安全管理体系，保证学院的数据及其支撑系统的完整性、机密性和可用性，避免数据泄密，根据国家有关法律法规，特制定本办法。

第二条 本办法所称的数据是指：学院业务、数据仓库以及教学事务中各项信息系统（包括学院网站）生成的数据，适用于数据的产生、传输、使用、存储、共享、归档/销毁全链路的数据安全管理环节。

第三条 本办法内容包括：总则、数据资产范围、数据安全角色及岗位职责、数据分级分类规范、数据安全规范细则、数据输出管理细则、数据安全事件应急管理、附则。

第四条 下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

中华人民共和国国务院令（第 790 号）《网络数据安全管理办法》（2025 年 1 月 1 日起实施）

《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》

《信息安全技术 网络安全等级保护基本要求》
(GB/T22239-2019)

《信息安全及个人信息安全规范》(GB/T35273-2020)
教育部等七部门《关于加强教育系统数据安全工作的
通知》(教科信函〔2021〕20号)

第五条 本办法适用于学院及各分支机构。

第二章 数据管理范围

第六条 学院数据安全管理的范围包括：

(一) 数据资产：

所有存储在线上数据库和数据仓库中的数据，包括但不限于：

1、学院拥有的数据；包括但不限于学生个人信息、教职工信息、财务信息、教学资料等。

2、第三方委托公司存储处理的受合同约束的数据。

(二) 支撑系统：

所有的支撑设施，例如直接或间接参与确保上述数据完整性、机密性以及可用性相关的人或系统，包括但不限于：

1、场所，如：办公室、云服务器、学院机房；

2、硬件，如：服务器、网络设备、笔记本电脑、台式电脑、存储设备、移动设备；

3、软件，如：操作系统、商业软件、自行开发的软件；

4、人员，如：学院员工、外聘人员、除员工和外聘人员外的第三方人员（以下简称第三方人员）。

（三）文档和记录：

所有与管理、使用及控制上述数据资产及其支持系统相关的策略、流程及操作手册和记录。包括但不限于数据安全政策、操作流程、审计记录等。

第三章 数据安全角色设置及岗位职责

第七条 数据安全角色设置及岗位职责：

网络安全、网络综合治理和信息化领导小组（以下简称“网信小组”）。

网信小组是数据安全保护的领导机构，该部门的主要职责：

（一）主要职责是贯彻落实上级有关部门关于数据安全保护工作的开展战略、宏观规划、重大政策和工作部署。

（二）统一领导、统一谋划、统一部署学院的数据安全保护工作，统筹协调和决策学院数据安全保护工作中的重大问题等。

（三）对数据进行分级分类，制定数据安全管理体系；

（四）定期安排开展数据安全审计；

（五）推动相关方对数据安全问题进行改进；

（六）网信小组应定期召开会议，审议数据安全管理工作报告，制定数据安全培训计划，监督数据安全事件的处置等。

第四章 数据分级分类管理规范

第八条 数据分级定义：根据数据价值、敏感性、数

据风险及法律法规要求，将学院数据分为五个级别：核心、重要、敏感、内部、公开。各部门应根据本办法的要求，对本部门的数据进行分级分类，并制定相应的保护措施。保护措施应包括数据加密、访问控制、备份恢复等。

级别	定义
核心 (L5)	非授权的公开、泄露将直接对学院、学生或者员工造成严重不利影响（例如：造成重大经济损失、严重破坏学院声誉、造成监管问责，以及发生重大法律责任等）的数据。 指一旦泄露、披露或滥用可能危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等的个人信息。 涉及组织、发展或国家安全具有至关重要影响的数据。
重要 (L4)	对学院的运营、管理或决策具有重要影响的数据，如学生数据、财务资料等。 非授权的公开、泄露将直接对学院、学生或者员工造成不利影响（例如：造成经济损失、破坏学院声誉、可能发生法律责任等）的数据。 指能够单独识别自然人身份或者反映特定自然人活动情况的信息。
敏感 (L3)	指涉及个人隐私、可能对学习产生负面影响的数据。 非授权的公开、泄露将直接对学院、学生、

级别	定义
	老师、工作人员造成较小不利影响的数据。
内部 (L2)	仅供组织内部人员使用的数据，这些数据可能涉及组织的运营、管理或业务流程等内部信息。 非授权的公开、泄露将直接对学院、学生、老师、工作人员造成较小影响的数据。
公开 (L1)	允许被公共访问和对外发布的信息，并且公开信息可以自由散布而不会产生任何安全和法律问题。

数据分级示例：

级别	典型示例
核心 (L5)	学院资产、项目合同类信息 学院业务相关的核心数据 学院人事档案 学院关键业务系统的账号密码
重要 (L4)	关键项目的计划、方案等 个人身份标识数据 学院业务系统的账号密码
敏感 (L3)	学院内部全员公告、通知 学院通讯录 学院教师个人信息
内部 (L2)	学院内部管理办法 教师绩效分配表

公开 (L1)	学院官网新闻
------------	--------

数据分级授权访问要求：

级别	授权要求
核心 (L5)	经相关责任人、部门负责人、安全管理部门及学院领导批准
重要 (L4)	需得到密级确定部门主要负责人批准。
敏感 (L3)	需得到部门负责人批准。
内部 (L2)	需得到部门负责人批准。
公开 (L1)	无限制

数据分级存储要求：

级别	存储要求
核心 (L5)	电子类的应妥善保存在设有安全控制且未联网的计算机系统内。 介质由知悉部门保密执行人专人专柜保存。
重要 (L4)	电子类的应妥善保存在设有安全控制的计算机系统内。 介质由知悉部门保密执行人专人专柜保存。
敏感 (L3)	应由相关部门妥善保管。

内部 (L2)	应妥善保管。
公开 (L1)	无限制

数据分级复制要求：

级别	复制要求
核心 (L5)	禁止复制。
重要 (L4)	由定密部门保密执行人进行，复制件上应加盖复制部门公章，并在显著位置注明“复制件”字样和复制日期。
敏感 (L3)	由定密部门保密执行人进行，根据工作需求执行。
内部 (L2)	根据工作需求执行。
公开 (L1)	无限制。

数据分级网络上传要求：

级别	邮件要求
核心 (L5)	禁止通过互联网直接发送。
重要 (L4)	须经密级确定部门负责人许可，文件发送应做加密控制，不得发送到公众或私人账户，并保留发送记录。

敏感 (L3)	须经密级确定部门负责人许可,根据工作需求执行。
内部 (L2)	根据工作需求执行。
公开 (L1)	无限制。

数据分级销毁要求:

级别	销毁要求
核心 (L5)	碎纸机或集中销毁; 彻底销毁介质;
重要 (L4)	碎纸机或集中销毁; 彻底销毁介质;
敏感 (L3)	碎纸机或集中销毁; 删除数据;
内部 (L2)	碎纸机或集中销毁; 删除数据;
公开 (L1)	无限制。

第九条 数据分类定义: 数据资源按照主题域和数据服务进行分类。

(一) 主题域分类原则

1. 按照数据资源所涉及的范围, 将学院数据按照主题域进行分类, 采用大类、中类和小类三级分类法。

2. 按主题域将数据资源分为以下大类：行政管理、学生管理、教学管理、科研管理、资产管理、财务管理、人力资源管理、图书管理、安防管理、公共服务。

3. 对每一大类主题，按照关联主题信息划分中类。每一种类，按照分类属性划分小类。大类之外的其他主题可以作为扩展主题，依照主题域划分原则对所有数据资源进行全面分类。

（二）数据服务分类原则

1. 基础数据类。支撑业务系统基础数据应用，主要通过数据共享、接口调用服务等方式。

2. 公共服务类。支撑服务类平台数据应用，主要向公共服务类平台提供数据支持。

3. 决策分析类。支撑校内分析平台数据应用，主要提供各类分析、报表、决策分析支持等。

4. 报表类。向上级部门和校外其他单位报送数据服务。

第五章 数据安全规范细则

第十条 数据资产清单

每个数据资产应有其相应的责任人，数据资产责任人应理解并执行本规范中定义的职责。

部门数据安全负责人负责定义和维护上述适用范围内的数据资产清单。

第十一条 数据分类和处理

部门数据安全负责人应确保所有的数据资产都被适当的分级，并根据不同的级别，推动数据资产责任人、数据

处理人员、IT 部门等建立和实施相应的保护措施，保护措施应考虑到数据的存储、访问、传输及分发等环节。数据资产责任人负责定义和维护数据资产清单，数据处理人员负责实施数据保护措施，IT 部门负责提供技术支持和监控。

第十二条 数据安全基本准则

所有的学院教师、外包及第三方人员需遵守学院的数据安全基本准则，包括但不限于：

（一）所有对数据库及数据仓库数据的分析、加工、处理等操作，必须在学院内网服务器中进行；

（二）数据分析人员需要将上述数据传递给业务需求方时，必须先通过内部数据流程审批，审批通过之后，才能进行数据分发；

（三）禁止使用个人或学院提供的设备来接收或处理数据安全网络和数据分发平台的数据；禁止运行未经检验和来历不明的软件，禁止在各自的计算机内安装与各自业务无关的软件，禁止安装运行各种游戏娱乐软件，禁止将计算机系统口令和个人密码告诉无关人员，未经许可严禁将计算机交由外部门人员操作。

（四）严禁在没有得到适当授权的情况下，将上述范围中的数据传递给第三方。

（五）对外拷贝软盘、U 盘、移动硬盘、光盘等移动存储设备需经相关部门领导批准方可执行。

任何违反上述要求的员工，将进行通报批评、情节严重的依据学院规定进行处罚。

第十三条 数据资产访问控制

数据资产及其处理设施的访问控制应能保证数据的完整性、机密性及可用性；访问授权应遵循最小授权以及除非特别授予否则默认禁止的原则；

禁止将上述范围中的数据存储在非学院拥有的系统或信息处理设备上；

各数据支撑系统和所属管理部门应定期审查具有远程访问权限的人员，对于不再需要远程访问权限的账号应立即禁用。

第十四条 风险评估

网信小组定期对数据资产及其支撑处理设施进行风险评估，识别数据安全风险并建立和实施风险处置措施；以确保采取了适当的控制措施来保证数据的安全性。

第十五条 数据安全事件监控

网信小组应保证数据资产支撑系统建立数据异常访问监控机制，能够及时识别非授权的访问；

部门数据安全负责人和网信小组应建立数据安全风险反馈流程，以及时收集数据安全风险，并采取适当的风险处置措施。

第十六条 数据安全管理的监督

各部门负责人应定期复核所在部门具有数据资产及其支撑系统访问权限的人员清单；

网信小组将定期对学院内部各部门的数据安全管理执行情况进行审计，并推动相关部门对审计发现的问题进行

改进。

第六章 数据输出管理细则

第十七条 数据需求方必须在对外输出前取得审批及该审批的限制；

数据需求方同意将所有包含将输出数据的资料，包括线上或线下使用的，于正式对外输出前作事先的书面审批。

第十八条 超出原有数据使用目的必须再取得相关审批；

任何超出原有数据使用目的之进一步的数据披露或使用，必须重新取得学院内部审批流程后方可进行。

第七章 数据安全事件应急管理

第十九条 数据安全事件包括数据泄露（丢失、被窃取）、数据滥用、数据被篡改、数据被损毁、数据违规使用和其他数据破坏事件：

（一）数据泄漏（丢失、被窃取）事件是指因误操作、人为蓄意、软硬件缺陷或电磁泄漏等因素导致网络/系统/平台中的保密、敏感、个人隐私等重要数据暴露于未经授权者，而导致的数据安全事件。

（二）数据滥用事件是指数据使用方违规或超范围收集、使用数据而导致的数据安全事件。

（三）数据被篡改事件是指未经授权将网络/系统/平台中的数据更换为攻击者所提供的数据而导致的数据安全

事件。

（四）数据被损毁事件是指因误操作、人为蓄意或软硬件缺陷等因素导致网络/系统/平台的数据删除、乱码、数据完整性破坏、数据存储介质销毁等数据安全事件。

（五）数据违规使用事件是指在数据使用的过程中违反学院管理规定及相关国家法律规定或条例而导致的数据安全事件。

（六）其他数据安全事件是指不能被包含在以上分类之中的安全事件。

第二十条 根据国家相关政策标准和数据安全事件对国家安全、社会稳定、公众权益、单位利益和声誉的影响程度，并按照数据安全事件的影响范围及持续时间等因素，将学院数据安全事件分为四级：特别重大数据安全事件（Ⅰ级）、重大数据安全事件（Ⅱ级）、较大数据安全事件（Ⅲ级）和一般数据安全事件（Ⅳ级）。当数据安全事件同时满足多个级别的定级条件时，按最高级别确定数据安全事件等级。

（一）特别重大事件（Ⅰ级）

特别重大事件是指能够导致特别严重影响或破坏的数据安全事件，包括以下情况：

（1）500 条以上师生个人信息数据丢失或被窃取、被损坏、被非法使用，造成特别重大经济损失的，或者特别重大损害公众利益，对学院师生产生极大负面影响；

（2）有条件共享数据和不予共享数据丢失或被窃取、

篡改、假冒，产生特别重大的社会影响；

（3）其他造成或可能造成特别重大危害或影响的数据安全事件。

（二）重大事件（Ⅱ级）

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：

（1）大于 300 条小于 500 条师生个人信息数据丢失或被窃取、被损坏、被非法使用，造成重大经济损失的，或者重大损害公共利益，对学院师生产生重大负面影响；

（2）有条件共享数据和不予共享数据丢失或被窃取、篡改、假冒，产生重大的社会影响；

（3）其他造成或可能造成重大危害或影响的数据安全事件。

（三）较大事件（Ⅲ级）

较大事件是指能够导致较严重影响或破坏的信息安全事件，包括以下情况：

（1）大于 100 条少于 300 条师生个人信息数据丢失或被窃取、被损坏、被非法使用，造成严重经济损失的，或者严重损害公共利益，对学院师生产生严重负面影响；

（2）有条件共享数据和不予共享数据丢失或被窃取、篡改、假冒，产生严重的社会影响；

（3）其他造成或可能造成较大危害或影响的数据安全事件。

4. 一般事件（Ⅳ级）

(1) 100 条以内师生个人信息数据丢失或被窃取、被损坏、被非法使用造成一般经济损失的，或者一般损害公众利益，对学院师生产生一定负面影响；

(2) 有条件共享数据和不予共享数据丢失或被窃取、篡改、假冒，产生一般的社会影响；

(3) 其他造成或可能造成一般危害或影响的数据安全事件。

第二十一条 学院开展数据安全监测预警与信息通报，发现问题及时上报与处置。

第二十二条 各信息系统主管单位根据业务特点制定数据安全事件应急预案，建立数据安全应急处置流程，包括应急响应流程、应急处置措施、应急资源调配等，同时，定期开展数据安全事件应急演练。

第二十三条 应在安全事件报告和响应处理过程中，分析和判断事件产生的原因，收集证据，记录处理过程，总结经验教训，制定补救及预防措施，且过程中形成的所有文件和记录均应妥善保存。

第二十四条 定期组织开展数据安全教育和培训，提升全员数据安全意识，确保数据安全策略的有效防护。

第八章 附则

第二十五条 本办法由网信小组办公室负责解释和修订。本办法在执行过程中，广大教职工和学生应积极提出意见和建议。对于合理的意见和建议，网信小组办公室应及时采纳并进行修订。

第二十六条 本办法自正式发布之日起执行。

附件 1

贵州交通技师学院（贵州省交通运输学校）
数据输出申请审批文件

申请人		[申请人姓名]				
申请部门		[申请部门/单位全称]				
申请理由		[详细阐述申请输出数据的具体原因和目的,包括数据的用途、重要性等]				
申请使用范围						
申请 输出 数据 具体 内容	数据名称	数据描述	数据格式	数据量 (MB)	数据来源	级别
	[数据名称 1]	[详细描述数据内容、范围、时间等]	[如 CSV、Excel、各系统数据库导出]		[数据来源说明]	(L1~L4)
部门领导审批		年 月 日				
分管领导审批		年 月 日				

注：请申请人认真填写此表格，确保信息真实、准确、完整。审批人员需根据实际情况，在“审批意见”填写“同意”或“不同意”，并签署姓名和日期，相关部门领导同意后，需要加盖部门章。如申请被批准，申请人需按照审批意见和相关规定进行数据输出和使用。