ICS 35.020
L 70

团　　体　　标　　准

X/XXXXX XXX-XXXX

高校数据安全分类分级指南

Guide for University Data Security Classification and Grading

2022 - XX - XX 发布　　2022- XX - XX 实施

XXXXXXXXX　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由深圳大学提出。

本文件由广东省网络空间安全协会归口管理。

本文件起草单位：XXXX…。

本文件主要起草人：XXXX。

本文件为首次发布。

引　言

随着高校教育信息化智能化建设的深入开展，高校数据的规模及复杂度也进一步增加。大规模及高精度的数据给高校发展带来机遇的同时也给高校数据安全管理带来了极大的挑战。近年来，高校数据安全治理已成为推进教育信息化战略发展的重要工作之一，2020 年 9 月，国家发布《关于加强教育系统数据安全的指导意见》； 2021 年 4 月，教育部等七部门印发了《关于加强教育系统数据安全工作的通知》，明确提出“要建立教育系统数据安全责任体系和数据分类分级制度，形成教育系统数据资源目录。健全覆盖数据收集、传输存储、使用处理、开放共享等全生命周期的数据安全保障制度，有力支撑教育事业发展”等工作目标。2021 年 6 月及 8 月，全国人大常委会先后表决通过了《数据安全法》和《个人信息保护法》，这两项法案的出台表明国家层面对数据安全已有明确要求。为规范高校数据分类分级管理，提高高校数据的使用效率，更好地推动高校数据安全治理工作，依据相关法律法规及标准起草了本指南。

高校数据安全分类分级指南

1 范围

本文件规定了高校数据分类的一般要求、维度与流程，数据分级的一般要求、要素、维度、流程与变更。

本文件适用于高校范围内数据的分类分级工作。

本文件不适用于涉密高校数据的分类分级管理。

2 规范性引用文件

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

GB/T 38667-2020 信息技术 大数据 数据分类指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

高校数据 university data

高校在开展或辅助开展教育活动过程中收集、存储、使用、加工、传输、提供、公开等环节，以电子或者其他方式对信息的记录。

3.2

高校数据分类 university data classification

根据高校数据具有的共同属性或特征，将其按一定的原则和方法进行区分和归类，以便于高校的管理和使用。

3.3

高校数据分级 university data grading

根据高校数据的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用后，对国家安全、经济运行、社会稳定、公共健康和安全、高校自身造成的危害程度，对高校数据进行定级管理。

4 高校数据安全分类

4.1 一般要求

4.1.1 科学性

应按照高校数据的多维特征及其相互间存在的逻辑关联进行科学系统化的分类，分类规则应保持相

对稳定。

4.1.2 适用性

分类应结合高校实际需求，符合高校相关人员及外界人员对高校数据的普遍认知，不设无意义的类目。

4.1.3 完整性

分类维度能够覆盖全部有效的高校数据，无重要类别属性遗漏。

4.1.4 不耦合性

同一分类维度下，不同子类之间原则上不应有重复和交叉，同一级次分类维度要统一，以防造成数据分类结果冗余。

4.1.5 可扩展性

分类类目应具有可扩展性、兼容性，可适应未来高校发展变化过程中类目增减和数据类型变化等情况。

4.1.6 合规性

应保持与国家、地方、行业法律法规的相关要求相一致，原则上兼容教育系统的分类分级指南要求。

4.2 分类维度

4.2.1 部门维度

高校部门维度数据指可表征高校内部门特征或描述部门活动情况的各种数据，其子类可分为党群组织、行政部门、学部与学院、学术机构、教辅部门、产学研部门、校设研究机构、附属医院、附属学校等。不同子类可进一步划分，如党群组织又可分为党政办公室、党委组织部、党委宣传部等。

4.2.2 人员维度

高校人员维度数据指可表征高校内自然人的特征或描述高校内自然人行为活动情况的各种数据，可分为学生、教职工、其他。

4.2.3 资产维度

高校资产维度数据是指高校占有或者使用的能以货币计量的经济资源，包括各种财产、债权和其他权利。其可分为流动资产、固定资产、在建工程、无形资产和对外投资等。资产维度数据将根据其衍生属性归集至部门数据或人员数据。

4.2.4 业务维度

高校业务维度数据是指高校内部门或人员开展或辅助开展教育活动所产生的过程数据，可分为教务、行政、科研、财务、教辅、后勤、安保、资产管理等。业务维度数据将根据其衍生属性归集至部门数据或人员数据。

4.2.5 应用维度

高校应用维度数据是指高校内部门或人员为支撑或促进高校发展和改革，合理合规将高校数据应用于相关领域的数据。其可分为：智慧行政决策、智慧校园、智慧科研、智能学习等。

4.2.6 其他维度

a) 数据产生频率维度（数据更新频率进行分类，如年、季度、月、周、天、不定期等）；
b) 数据使用频率维度（数据使用频率进行分类，如年、季度、月、周、天、不定期等）；
c) 数据存储方式维度（数据存储方式进行分类，如关系型数据库存储、图数据库存储、文档数据库存储等）；
d) 高校自主决定的其他分类维度。

4.3 分类流程

分类流程包括：分类规划、分类准备、分类实施、结果评估、维护改进，具体可参考 GB/T 38667-2020 第 5 章及第 8 章的相关方法及流程。

5 高校数据安全分级

5.1 一般要求

5.1.1 科学性

应按照数据资源的多维特征及其之间的逻辑关系进行标准化分级，确保高校数据分级的准确性、客观性、稳定性。

5.1.2 适用性

应充分参考高校各类数据应用场景，保证高校数据分级的可行性、实用性。

5.1.3 就高从严

数据集的定级应根据下属数据项目的最高级别定级，依从就高从严原则。

5.2 分级要素

5.2.1 重要性

重要性是指数据对国家安全、公共利益、组织权益、个人权益等潜在对象的重要程度。

5.2.2 精度

精度是指数据所描述的数据对象与事务实体的精确与准确程度。

5.2.3 规模

规模是指数据规模及数据描述的对象范围或能力的大小，以此评估发生数据安全事故时潜在的可能影响范围。

5.2.4 业务

业务是指高校内部门或人员的职责分工及工作中产生的数据。

5.2.5 安全风险

数据安全风险是指高校数据遭篡改、破坏、泄露或非法利用的可能性、后果及对应程度。

5.2.6 其他要素

高校自行定义的其他分级要素。

5.3 数据影响分析

5.3.1 影响对象

影响对象是指高校数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响的对象，通常包括国家安全、公共利益、组织权益、个人权益。具体影响对象定义如表 1 所示。

表1 影响对象定义

影响对象	定义
国家安全	国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。
公共利益	能够满足一定范围内所有人需要的对象，即具有公共效用的对象，或者说，能够满足一定范围内所有人生存、享受和发展的、具有公共效用的资源和条件。
组织权益	法律规定的组织及对应法人所具有的生产运营、声誉形象、公信力、知识产权等权益。
个人权益	自然人的政治权、人身权、财产权以及其他合法权益。

5.3.2 影响程度

影响程度是指数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能造成的影响程度。影响程度从高到低可分为特别严重、严重、一般、轻微。对不同影响对象进行影响程度判断时，采取的基准不同。如果影响对象是组织或个人权益，则以本单位或本人的总体利益作为判断影响程度的基准。如果影响对象是国家安全、经济运行、社会稳定或公共利益，则以国家、社会或行业领域的整体利益作为判断影响程度的基准。具体影响程度定义如表 2 所示。

表2 影响程度定义

影响程度	定义
特别严重	对影响对象造成特别严重损害，且结果不可逆，损失无法补救。
严重	对影响对象造成严重损害，且结果不可逆，但可以采取措施降低损失。
一般	对影响对象造成一般损害，且结果可以补救。
轻微	对影响对象造成轻微损害，且结果不需补救。

5.4 分级维度

5.4.1 概述

高校根据相关分级要素对影响对象和影响程度进行综合评估，将数据分为三类：核心数据、重要数据、一般数据。

5.4.2 核心

核心数据是指在高校内具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能对国家安全产生特别严重或严重危害，如直接影响政治安全、国家经济命脉、重要民生等。满足以下条件之一，应纳入核心数据建议范围：

a) 高精度、未公开的高校全部数据；

b） 10 万及以上个人信息或 1 万以上个人敏感信息；

c） 经评估的其他数据。

5.4.3 重要

重要数据是指在高校内达到一定精度和规模的数据，一旦被泄露、篡改或破坏，可能对国家安全造成一般危害、公共利益造成特别严重或严重危害。满足以下条件之一，应纳入重要数据的范围：

a） 高校全部数据；

b） 1 万及以上个人信息或 1000 以上个人敏感数据，个人敏感信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等；

c） 全国性的业务数据；

d） 卫生健康、科技等其他领域确定的重要数据；

e） 经评估的其他数据。

5.4.4 一般

一般数据是指除核心数据和重要数据之外的其他高校数据。根据高校数据一旦被泄露、篡改、破坏，可能对组织及个人权益影响程度，可对一般数据再分为三个等级：

a) 一级：内部敏感级。内部敏感级数据是指此类高校数据一旦被泄露、篡改或破坏，可能对高校组织及高校人员权益造成特别严重危害，非特殊情况不公开或共享。满足以下条件之一，应纳入内部敏感级数据的范围：

——高校特殊业务的全部数据，如财务、学生成绩等；

——经评估的其他数据。

b) 二级：有条件对外共享级。有条件对外共享级数据是指此类高校数据一旦被泄露、篡改或破坏，可能对高校组织及高校人员权益造成严重危害，可部分公开、小范围共享或经上级相关要求及高校同意可全部公开或共享。满足以下条件之一，应纳入有条件对外共享级数据的范围：

——试题数据；

——经评估的其他数据。

c) 三级：除一级和二级外的其他一般高校数据。

5.5 分级流程

5.5.1 分级准备

第一步：对高校数据进行盘点、梳理与分类，形成统一的数据资源目录，识别数据安全定级关键要素。

5.5.2 分级判定

第二步：参照高校数据定级维度，结合国家及行业有关法律法规、部门规章、分级要素对数据安全等级进行初步判定，确定拟定为核心数据和重要数据的范围。

5.5.3 分级审批

第三步：各单位将数据资源目录和拟确定的核心数据和重要数据范围，由校网信办审核完后，统一报送至教育主管部门评审。

5.5.4 分级实施

第四步：拟定具体的分级实施流程，可使用自动化开发工具或脚本，利用其分级算法对高校数据进

行分级。同时记录分级实施过程中的各个步骤及其分级结果。分级实施过程中，对于重要数据目录共享应报校网信办审核同意，核心数据目录共享应报教育主管部门审核同意。

5.5.5 结果核查

第五步：核查验证分级结果及实施过程是否合规，包括但不限于分级判定及分级过程记录的核查。必要时重复第二步。

5.6 分级变更

数据安全定级完成后，出现下列情形之一时，高校应对相关数据的安全级别进行变更。

a) 数据内容发生变化，导致原有数据的安全级别不适用变化后的数据。

b) 数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化。导致原定的数据安全级别不再适用。

c) 因数据汇聚融合，导致原有数据安全级别不再适用汇聚融合后的数据。

d) 需要对数据安全级别进行变更的其他情形。

变更重要数据范围的，应报校网信办审核同意；变更核心数据范围的，应由校网信办审核后，报教育主管部门同意。