基于DSMM的数据分类分级探索与实践

云桂桂，杜彬，刘淑梅
（北京化工大学信息化办公室（信息中心），北京 100029）

摘　要：数据资产已成为极其重要的新型资产之一，并成为高校数字化转型最有效的助推器，其安全问题也日益突出，数据分类分级是实现数据安全管理的首要条件。首先，分析了数据分类分级存在的两大难题；然后，依据DSMM，从制度流程和技术工具2个维度开展研究，并依托学校数据平台实践，构建了学校的数据分类分级保护体系，为学校数据安全管理与共享提供了坚实保障。

关键词：数据治理；分类分级；数据安全；数据安全能力成熟度模型
中图分类号：TN
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024246

Exploration and practice of data classification and grading based on DSMM

YUN Guigui, DU Bin, LIU Shumei
Center of Information Technology, Beiing University of Chemical Technology, Beijing 100029, China

Abstract: Data assets have become one of the most important new assets and the most effective booster for digital transformation in universities. Its security issues are becoming increasingly prominent, and data classification and grading are the primary conditions for achieving data security management. Firstly, the two major challenges in data classification and grading were analyzed. Then, research conducted from the perspectives of institutional processes and technical tools based on the DSMM. With the practice of school data platforms, a data classification and grading protection system for schools was constructed, providing a solid guarantee for school data security management and sharing.

Keywords: data governance, classification and grading, data security, DSMM

0　引言

经过多年的信息化建设，高校已经积累了大量教学、科研、管理等重要的业务数据，并将其汇聚到学校数据中台进行统一管理。近年来，随着数据的价值凸显，数据资产已成为学校重要的新型资产之一，是高校数字化转型最有效的助推器。但其中涉及师生的个人敏感信息，伴随而来的数据安全问题日益突出[1]。

2021年《教育部等七部门关于加强教育系统数据安全工作的通知》中，要求建立教育系统数据分类分级制度，全面加强数据安全保护能力。同年《中华人民共和国数据安全法》正式实行，明确规定“建立数据分类分级保护制度”；《中华人民共和国个人信息保护法》规定“建立健全个人信息保护合规制度体系”，并要求采取严格保护措施来处理敏感个人信息。由此可见，对数据安全要求越来越严格与

收稿日期：2024–10–22
通信作者：刘淑梅，smliu@mail.buct.edu.cn
基金项目：北京高等教育学会2023年度面上课题基金资助项目（No.MS2023110）；北京化工大学十五五规划课题基金资助项目（No.GH2024-09）
Foundation Items: The 2023 General Program of Beijing Association of Higher Education (No.MS2023110), The Research Project of 15th five-year plan of Beijing University of Chemical Technology (No.GH2024-09)

全面，进行数据分类分级保护迫在眉睫[2-3]。但在探索和实践过程中还存在缺乏数据安全治理制度和流程、缺乏数据分类分级技术与方法这两大难题[4]。

本文在国家数据安全相关法规的指导下，依据数据安全能力成熟度模型（DSMM, data security capability maturity model），从制度流程和技术工具2个维度开展研究，并依托学校数据平台实践，构建了学校的数据分类分级保护体系，为学校数据安全管理与共享提供了坚实保障。

1　基于DSMM的数据分类分级

1.1　DSMM模型

如图1所示，数据安全能力成熟度模型是我国首个数据安全标准认证，2019年正式成为国标对外发布，以DSMM为数据安全治理思路方案选型，可以更好地实现数据安全治理的制度合规。

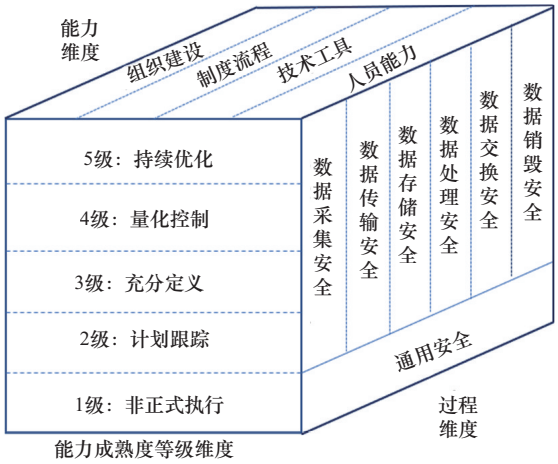

图1　数据安全能力成熟度模型

DSMM以数据为中心，围绕组织建设、制度流程、技术工具、人员能力4个安全能力维度，从数据采集、传输、存储、处理、交换到销毁进行全生命周期的能力等级评估。数据能力成熟度等级被划分为5个级别。1级：非正式执行，代表随机、无序、被动地执行安全过程，依赖于个人经验，无法复制。2级：计划跟踪，代表在业务系统级别主动地实现了安全过程的计划和执行，但没形成体系化。3级：充分定义，代表在组织级别实现了安全过程的规范执行。4级：量化控制，代表建立量化目标，安全过程可度量。5级：持续优化，代表根据组织的整体目标，不断改进和优化安全过程。

在此基础上，将6个生命周期细分，划分出30个过程域（PA），每个过程域围绕4个安全能力制定不同集合的实践指标（BP）。数据分类分级是第一个过程域，对数据全生命周期的安全影响至关重要。本文以DSMM为指导，从数据分类分级入手开展实践，研究强化学校的数据安全能力。

1.2　数据分类分级要求

在DSMM中，关于数据分类分级围绕4个安全能力维度，对应5个成熟等级，提出了15个实践指标，分布如表1所示。表1中各指标解释如下[5-6]。

BP.01.01: 组织未在任何业务建立成熟稳定的数据分类分级，仅根据临时需求或基于个人经验，对部分数据进行了分类或分级。

BP.01.02: 应由业务团队相关人员负责相关业务的数据分类分级。

BP.01.03: 应根据业务特性和外部合规要求，对核心业务的关键数据进行分类分级管理。

BP.01.04: 应设立负责数据安全分类分级工作的管理岗位和人员，主要负责定义组织整体的数据分类分级的安全原则。

BP.01.05: 应明确数据分类分级原则、方法和操作指南。

BP.01.06: 应对组织的数据进行分类分级标识和管理。

BP.01.07: 应对不同类别和级别的数据建立相应的访问控制、数据加解密、数据脱敏等安全管理和控制措施。

表1　数据分类分级实践指标

能力维度	1级	2级	3级	4级	5级
组织建设	—	BP.01.02	BP.01.04	—	—
制度流程	BP.01.01	BP.01.03	BP.01.05 BP.01.06 BP.01.07 BP.01.08	—	BP.01.13
技术工具	—	—	BP.01.09	BP.01.11 BP.01.12	BP.01.14 BP.01.15
人员能力	—	—	BP.01.10	—	—

BP.01.08: 应明确数据分类分级变更审批流程和机制，通过该流程保证对数据分类分级的变更操作及其结果符合组织的要求。

BP.01.09: 应建立数据分类分级打标或数据资产管理工具，实现对数据的分类分级自动标识、标识结果发布、审核等功能。

BP.01.10: 负责该项工作的人员应了解数据分类分级的合规要求，能够识别哪些数据属于敏感数据。

BP.01.11: 应记录自动分类分级结果与人工审核后的分类分级结果之间的差异，定期分析改进分类分级标识工具，提升工具处理的准确度。

BP.01.12: 应对数据分类分级的操作、变更过程进行日志记录和分析，定期通过日志分析等技术手段进行变更操作审计，数据分类分级可追溯。

BP.01.13: 应定期评审数据分类分级的规范和细则，考虑其内容是否完全覆盖了当前的业务，并执行持续的改进优化工作。

BP.01.14: 应跟踪数据分类分级标识效果，持续改进数据分类分级的技术工具。

BP.01.15: 应参与国标、国家或行业相关标准的制定。在业界分享最佳实践，成为行业标杆。

经过对比分析发现，3级要求包含了全部4个安全能力，且能够实现安全过程的规范执行，对实际工作有较强的指导意义。因此本文参考第3级的指标要求，从制度流程和技术工具2个维度，探索与实践针对高校师生数据的分类分级体系建设。

2 数据分类分级体系构建

2.1 制度流程

制度流程是数据分类分级体系构建实施的根本保证，需要整体考虑和设计，流程是制度的框架和主线，制度是流程有效执行的保障。结合学校的实际情况，本文形成了以《基础数据信息化管理办法》《数据安全管理办法》为一级纲领性文件，以《基础数据编码规范》《数据分类分级工作指南》和《数据质量检测规范》为二级实施指南，以数据分类分级流程为三级操作流程的制度体系框架。

1) 《基础数据信息化管理办法》。《基础数据信息化管理办法》是学校基础数据管理的一级制度，建立学校数据管理体系，将学校各类数据资源进行有机整合，实现和谐、安全、稳定、高效运行的数据环境。

2) 《数据安全管理办法》。《数据安全管理办法》是学校数据安全管理工作的一级制度，明确了学校数据安全管理机构及职责，并按照“统一标准、业务归口、授权共享、安全管控”的原则对数据采集、存储、共享使用过程安全进行规范，并约定了数据安全监督和应急处置措施。

3) 《基础数据编码规范》。《基础数据编码规范》对学校校区、机构、人员、楼宇房屋编码负责部门、编码结构、类型、格式等进行约定，学校所有信息化系统建设和数据共享中相关的数据均需遵循本文件规定。

4) 《数据分类分级工作指南》。《数据分类分级工作指南》是对学校数据进行分类管理和分级保护的指导性文件，结合学校实际，从机构、人员和业务层面，结合业务场景，进行主题分类、专题分类、指标分类。在分类的基础上开展分级保护，根据数据重要性和敏感程度，将数据划分为4个等级，分别对应4种共享方式，保障学校重要数据的安全共享。

5) 《数据质量检测规范》。数据质量检测分为数据集成前、中、后全周期的监控检测。对标国家标准、教育部标准，结合学校基础数据标准，分别制订检测规则，对表级别和字段级别的准确性、完整性、合法性进行检测，及时发现数据异常，逐步提高数据质量。常见如空值、重复、格式、数值合法等，记录数是否符合实际情况，是否出现极端变化等。

6) 《数据分类分级流程》。数据资产梳理是对数据进行安全定级的首要步骤，理清数据所属单位、数据分级的颗粒度、数据关键要素是进行安全定级的必要步骤，然后按照数据定级规则，综合考虑数据规模、时效性、形态等因素，对数据安全级别进行定级，形成数据安全级别评定结果及定级清单。

2.2 技术工具

技术工具是数据安全工作自动化和持续化的重要手段，能够实现对制度流程的固化执行，学校建立了数据安全共享平台，保障数据安全共享的常态长效。主要功能如下。

1) 数据资产分类管理。对学校所有数据资产进行精细化的管理，支持按组织机构、数据分类为单位进行数据资产的增加、删除、修改、统计等，并能够对每个数据资源进行字段级的确权绑定和等级分配等。

2) 数据安全等级管理。根据学校相关制度，设置数据安全等级，颗粒度可达到字段级别。基于

安全等级和管理要求，定制不同模式的审核流程。

3) 数据开放管理。以应用程序接口（API）、文本、数据库、ETL类型的数据清单对外进行数据共享开放，根据数据定级结果，对数据进行字段级脱敏、加密等，支持AES、SM3、SM4、MD5等主流加密算法，并能够根据一数一源结果自动匹配审核流程和权责审核部门。

4) 数据安全监控。管理侧对数据开放接口进行限流、限应用等访问控制的配置。用户侧对接口的申请、调用、下载情况进行记录监控，有效监控数据的动态流向，使数据共享可见可控。

2.3　分类分级实践步骤

1) 数据资产梳理，实行分类管理

数据资产梳理是实现数据分类分级的先行条件。目前我校数据中台汇聚了人事、教务、科研等17个关键业务系统的全量数据，有效数据表2 000多个。依据《教育系统核心数据和重要数据识别认定工作指南》中的数据分类指导，并根据数据来源分类为内部数据和外部数据。针对内部数据，根据业务属性将其划分为不同的主题类，每个主题类下根据业务类型再细分为多个子集，每个子集下包含若干相关的数据表和代码表。针对外部数据，根据原始来源部门细化分类。具体如表2所示。

2) 数据确权定级，实行分级保护

依据《教育系统核心数据和重要数据识别认定工作指南》的分级原则，我校已汇集的数据均属一般数据，但需要识别涉及的个人信息、敏感个人信息等。根据数据一旦遭到篡改、破坏、泄露或非法获取利用，可能会带来的危害程度，将数据分为4个级别，并按照“一数一源”的原则，确定数据权责部门，建立相应的数据共享审批流程。如表3所示。

表2　　数据分类管理

数据属性	数据来源	数据主题	数据子集
业务数据	内部数据（校内各业务系统）	教工主题	基础数据、组织干部
		学生主题	本科生、研究生、继教生
		科研主题	科研项目、论文成果、荣誉获奖
		财务主题	薪资、缴费、项目
		资产主题	固定资产
		教学主题	学生选课、学生成绩、教师授课、第二课堂
		公服主题	一卡通、楼宇门禁、图书管理、班车管理、宿舍管理
	外部数据（教育部共享接口）	公安部	
		科技部	
		工信部	

3) 数据接口发布，实行授权使用

通过数据安全管理平台实现数据的分类管理和分级保护，并根据数据定级设定相应的审批流程，目前已通过平台发布数据清单67个，关联2个审核审批流程，并实现身份证、手机号等敏感个人信息的加密/脱敏共享，安全级别及关联流程如图2所示，个人敏感信息加密/脱敏授权示例图3所示。

图2　安全级别及关联流程

表3　　数据分级与管控流程

数据等级	数据级别	数据特征	共享要求	管控流程
一般数据	L4	数据一旦遭到篡改、破坏、泄露或非法获取利用，可能会对学校利益或师生个人权益造成严重危害，且可能会影响社会稳定和公共利益	不予共享	—
	L3	数据一旦遭到篡改、破坏、泄露或非法获取利用，可能会对学校利益或师生个人权益造成严重危害，但不影响社会稳定和公共利益	有条件共享（加密/脱敏授权）	1. 用户申请 2. 申请部门审核 3. 归口部门审核 4. 数据中心授权 5. 审核通过
	L2	数据一旦遭到篡改、破坏、泄露或非法获取利用，可能会对学校利益或师生个人权益造成轻微危害	有条件共享（审批授权）	
	L1	经评估后，可向社会公开或可被公众获知、使用的学校相关数据	无条件共享（授权）	1. 用户申请 2. 数据中心授权 3. 结束

安全级别	字段名称	别名	描述	部门	业务系统	关联码表	脱敏授权	加密授权
有条件共享	sfzjlxdm	身份证件类型代码	身份证件类型代码	信息化办公室（信息中心）	无	--	☐	☐
条件共享（加密）	sfzjh	身份证件号	身份证件号	信息化办公室（信息中心）	无	--	☑	☐
有条件共享	cjrq	从教日期	从教日期	信息化办公室（信息中心）	无	--	☐	☐
条件共享（加密）	zzmmdm	政治面貌代码	政治面貌代码	信息化办公室（信息中心）	无	--	☐	☑
有条件共享	hkszd	户口所在地	户口所在地	信息化办公室（信息中心）	无	--	☐	☐

图3 个人敏感信息加密/脱敏授权示例

3 结束语

本文以DSMM为数据安全治理方案为思路，分析了DSMM中第一个分类分级过程域的指标项，从数据分类分级入手进行实践，围绕制度流程和技术工具2个维度开展研究，形成了一级纲领性文件、二级实施指南、三级操作流程的制度体系框架，搭建了数据安全管理平台，实现对数据资产、数据资产分类、数据等级、数据开放、数据安全监控的规范化管理以及数据管控流程的固化执行，保障数据安全工作的常态长效。最后依托学校数据平台进行实践，建立了学校的数据分类分级保护体系，强化了学校的数据安全能力。

参考文献：

[1] 江魁. 深圳大学: 数据安全保护从数据分级做起[J]. 中国教育网络, 2021(S1): 73-75.
JIANG K. Shenzhen University: Data security protection starts with data classification [J]. China Education Network, 2021(S1): 73-75.

[2] 张聪. 高校数据分类分级策略的探讨与实践[J]. 网络安全与数据治理, 2024, 43(6): 53-57.
ZHANG C. Discussion and practice of data classification and grading strategy in colleges[J]. Cyber Security and Data Governance, 2024, 43 (6): 53-57.

[3] 李松涛, 谢宗晓. 数据分类/分级及其相关标准解析[J]. 中国质量与标准导报, 2019(4): 14-16.
LI S T, XIE Z X. Data classification/grading and related standards analysis [J]. China Quality and Standards Review, 2019(4): 14-16.

[4] 王晓震, 金培莉, 陈瑛, 等. 高校数据中心数据安全风险分析及对策研究[J]. 北京联合大学学报, 2021, 35(3): 53-59.
WANG X Z, JIN P L, CHEN Y, et al. Research on data security risk analysis and countermeasures of university data center[J]. Journal of Beijing Union University, 2021, 35(3): 53-59.

[5] 张琼丽, 陈翼. 数据分级分类方法及实践研究[J]. 技术与市场, 2022, 29(8): 150-153.
ZHANG Q L, CHEN Y. Research of data classification model and practice[J]. Technology and Market, 2022, 29(8): 150-153.

[6] 全国信息安全标准化技术委员会. 信息安全技术 数据安全能力成熟度模型: GB/T 37988—2019[s]. 北京: 中国标准出版社, 2019.
National Information Technical Standardization Committee. Information security technology, Data security capability maturity model: GB/T 37988-2019[s]. Beijing: Standards Press of China,2019.

[作者简介]

云桂桂（1986– ），女，湖北襄阳人，北京化工大学工程师，主要研究方向为信息化建议与数据治理。

杜彬（1971– ），女，河北石家庄人，博士，北京化工大学研究员，主要研究方向为教育理论与教育管理。

刘淑梅（1973– ），女，天津人，博士，北京化工大学高级工程师，主要研究方向为数据分析与数据挖掘。