智慧校园建设背景下高校数据安全管理平台建设中面临的问题及应对方案①

刘白秋　李艳婷
（集美大学诚毅学院信息中心，福建厦门，361021）

摘　要　［目的］本文以集美大学诚毅学院为范例，通过剖析集美大学诚毅学院在智慧校园建设背景下数据管理平台中面临的四个主要问题并提出解决方法。［方法］以“数据资产梳理”、“数据管理平台技术体系建设”、“数据安全管理制度建设”、“数据安全管理组织建设”和“人员能力建设”五个方法着手，解决集美大学诚毅学院在智慧校园背景下数据安全管理平台建设所面临的问题。［结果］本文形成了适合集美大学诚毅学院实际情况的数据管理平台建设方案。［局限］由于数据安全管理平台建设涉及面较广，项目暂未落地完成，笔者只能从建设规划设计的角度进行总结和探索。［结论］通过对高校数据安全管理平台建设中面临的问题及应对方案进行梳理和总结，以期为学院数据安全管理平台建设提供有益参考。

关键词　智慧校园；数据安全；数据安全管理平台

Problems and Solutions in the Construction of Data Security Management Platform in Higher Education under the Background of Smart Campus

Liu Baiqiu　Li Yanting
(Information Center of Chengyi College of Jimei University, Xiamen, Fujian, 361021, China)

Abstract　［**Objective**］This paper takes Jimei University Chengyi College as an example, and analyzes the

①本文系福建省中青年教师教育科研项目“高校智能数据管理平台”（项目编号：JAT191924）的研究成果之一。

four main problems faced by the data management platform of Jimei University Chengyi College in the context of smart campus construction, and proposes solutions. ［**Methods**］Based on the five methods of "data asset sorting", "data management platform technology system construction", "data security management system construction", "data security management organization construction" and "personnel capacity building", this paper solves the problems faced by the data security management platform construction of Jimei University Chengyi College in the context of smart campus. ［**Results**］A data management platform construction plan suitable for the actual situation of Jimei University Chengyi College was formed. ［**Limitation**］Due to the wide coverage of data security management platform construction, the project has not been completed yet, and the author can only summarize and explore from the perspective of construction planning and design. ［**Conclusion**］By sorting out and summarizing the problems and solutions in the data security management platform construction of colleges and universities, this paper aims to provide useful reference for the data security management platform construction of the college.

Keywords Smart Campus；Data Security；Data Security Management Platform

1 引言

随着教育信息化的不断推进和发展，高校数据中心在日常业务管理、系统稳定运行中发挥着重要的作用。高校通过建设数据中心，逐步解决了数字校园建设中“数据孤岛”这一难题，通过全面的数据开发、整理与利用，向高校师生提供了更多的数据服务，使数据价值得到充分的发挥。

集美大学诚毅学院（以下简称“学院”）创办于 2003 年，是经教育部批准、由福建省重点建设高校集美大学与福建集美大学教育发展基金会联合创办的独立学院。学院于 2017 年完成了信息安全等级保护相关建设工作，并从 2019 年开始规划建设“智慧诚毅”项目。利用前沿信息技术手段，将学院里分散的信息化系统和资源整合为一个具有协同能力、服务能力和感知能力的有机整体，为教学、科研、管理和公众服务提供强有力的智能支撑。经过几年的建设，“智慧诚毅”逐步完善，其中智能化信息业务系统发挥了明显的作用。但是，随着数据存储量的日益增加，很多数据对于学院来说绝对不能外流，更不允许丢失，一旦数据发生泄露或遭到篡改，将影响到全院的信息化系统的正常运转和全体教职员工及师生的利益，所以，大家也开始意识到高校数据安全的重要性。只有意识到数据安全的重要性，才能实现数据的流通和共享，从而挖掘出数据的价值，为学院的日常管理和决策做出贡献，推进学院的数字化转型。

2 高校数据安全管理研究现状

目前在国外对于数据安全等相关方面关注的时间较早，也相应地出台了系列的法律法规和政策。德国在 1970 年颁布了世界上第一部《数据保护法》，瑞典于 1973 年颁布《瑞典数据保护法》，欧盟也分别在 1995 年、2016 年颁布了《数据保护指令》和《通用数据保护条例》。英国则是在立法保障的同时不断地加强国际间合作，大力培养网络人才，积极发展最新技术，紧跟国际互联网前沿水平。在数据保护方面，美国推行行业自律模式，即“由公司或者产业实体制定行业的行为规章或行为指引，为行业的网络隐私保护提供示范的行为模

式”。美国与个人信息保护相关的行业自律模式主要有建议性的行业指引、网络隐私认证计划和技术保护模式。在俄罗斯则更加强调个人对数据的自主保护能力，着力推进数据存储本地化。同时，俄罗斯政府还颁布了《个人数据保护法》，该法规表明任何收集俄罗斯公民个人信息的本国或者外国公司在处理与个人信息相关的数据，包括采集、积累和存储时，都必须使用俄罗斯境内的服务器，禁止数据外流[1]。

在国内，2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过《中华人民共和国网络安全法》，并于 2017 年 6 月 1 日就开始正式实施了。其中，《中华人民共和国网络安全法》第二十一条写明国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。《信息安全技术—网络安全等级保护定级指南（GB/T 22240-2020）》是目前我国等级保护标准体系的核心标准之一，该指南于 2020 年 4 月 28 日发布，并于 2020 年 11 月 1 日正式实施。数据安全建设是等级保护 2.0 建设的核心内容之一，在等保 1.0 对数据安全的要求基本不变的情况下，新增了根据新计算环境和业务场景，对数据安全保护能力做出了更贴合实际情况的明确要求。2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》。主要内容包括：确立数据分级分类管理以及风险评估、监测预警以及应急处置等数据安全管理各项基本制度；明确开展数据活动的组织、个人数据安全保护义务，落实数据安全保护责任；坚持安全与发展并重，规定支持促进数据安全与发展的措施；建立保障政务数据安全和推动政务数据开放的制度措施。数据安全法的发布，标志着数据安全上升到国家安全层面，事关国家安全与经济社会发展[2]。

学院为贯彻落实《中华人民共和国数据安全法》和《教育部关于加强新时代教育管理信息化工作的通知》的文件精神，切实加强网络安全防护和保障能力，以及校园数据安全、网络个人信息安全，落实教育系统数据安全指导意见，结合学院实际，于 2021 年颁布了《集美大学诚毅学院数据安全管理办法（试行）》制度，注意到了保护学生隐私利益的重要性，如数据传递过程中严格要求程序合规，明确数据禁止使用的地方，目的是在使用数据的同时，严格保护数据隐私等。

由此可见，在互联网不断对人们生活渗透的今天，数据安全是当今信息化建设中最重要的内容之一。随着高校信息化建设的发展，高校对信息化的依赖程度也日益增高，数据信息安全也是目前学院信息化建设的重中之重。

3 校园数据安全管理面临的问题

数据已成为国家基础性战略资源和新的社会生产要素之一。学院的信息化发展到目前阶段，已经解决了数据生产的问题，但是在数据的汇总、数据算法分析、数据的利用，数据价值深度挖掘，以及利用数据来驱动学院数字化转型等还做得远远不够。我们结合学院的信息化建设情况，从实际出发，发现目前校园的数据安全存在以下几点问题：

3.1 资产底数不清

目前学院数据分布在各个信息业务系统、个人电脑、档案文件等多处地方，因此需要开展数据资产摸底调查与分级分类，厘清学院的数据资产是首要任务。

3.2 管理缺位

内部的数据管理机制不够完善，数据所属职能部门管理人员对数据的安全性意识不够强烈，存在数据被意外丢失和随意散布的风险；另外，学院与第三方机构合作的越来越多，包括教育科技企业、在线教育平台等，但是这些合作机构的信息安全管理水平不一，在合作过程中需要谨慎选择合作伙伴，加强对其信息安全的监督和管理。以及，学院内部的人员流动性大，员工离职后未及时删除其账号权限，也会给数据安全带来隐患。

3.3 意识不够

目前学院大部分师生对于个人信息数据保护意识缺乏，要增强法律意识的培养，严格按照法律法规行事。对新业务、新应用的上线使用需要评估数据安全风险，避免过度的数据采集和滥用，要重视个人隐私保护。定期面向师生开展网络安全意识教育，形成重视数据安全保护的校园氛围。

3.4 使用混乱

缺乏系统化的信息数据采集、数据可共享目录、使用申请审批授权等安全有效的数据流转监管机制。对于数据采集使用情况不了解，对于数据用途和使用场景不明确，这可能会给个人隐私和权益带来损害，引起社会的广泛关注。

4 学院数据安全管理平台建设方案

针对上述问题，学院数据安全管理平台建设将分为以下几个部分开展：梳理数据资产分类分级建设、建设数据安全管理技术体系、建设数据安全管理制度、数据安全管理组织建设和数据安全人员能力建设五个部分。开展数据安全管理体系建设工作前，需要通过咨询调研的形式摸清学院数据安全管理现状、业务、合规和风险需求，然后再设计或优化数据安全管理组织架构，编制和完善数据安全管理制度，通过培训宣传的方式提升师生数据安全意识和技能。

4.1 学院数据资产梳理及分类分级建设

数据资产梳理盘点主要解决数据资产不清楚、不清晰、不可知等问题。其主要内容为深入组织业务，分析敏感数据及使用场景（包含但不限于开发测试、数据运维、数据分析、应用访问、特权访问、数据共享交换等场景），对资产、数据、用户、权限、流程等过程进行梳理并形成数据资产清单、数据流向清单、管控策略清单等文件，帮助组织精确梳理数据资产分布及使用状况。具体流程如图 1 所示。

图 1 数据资产梳理流程图

数据资产的梳理和分类分级起着承上启下的作用。对上，从运维管理制度、安全保障措施、岗位职责等管理制度体系都需依托数据分类分级进行具有针对性和有效性的编排和制定。对下，根据不同数据级别，实现不同安全防护，如高等级数据需要实现细粒度规则管控和数据加密，低级别数据实现单向审计即可。所以，数据分类分级是管理体系合理规划、数据安全合理管控、人员精力及力度合理利用的基础，是迈向数据安全精细化管理的重要一步。

4.2 学院数据安全管理平台技术体系建设

学院数据安全管理平台技术体系建设主要包括了数据审计、数据访问控制、数据脱敏、数据加密传输四个方面，如图 2 所示。

数据审计需要细粒度的双向审计，更精准多种资产发现方式的组合应用，能够最大程度地提高资产发现能力。流量动态监测，可持续发现新的资产，应对资产的动态变化，避免资产遗漏。资产扫描的即时或预约任务，可以灵活应对不同的发现场景。集群发现能力，能够避免重复任务，保证资产数据源的准确性。系统内置多样化的敏感数据识别规则，支持多种匹配方式下的规则自定义扩展，如正则表达式、自定义函数、混合类型等。同时可自定义分类分级标准，根据所需进行管理，满足各行业下对数据灵活识别的需求，使敏感数据识别和分类分级方案更贴合实际业务，实现对敏感数据的有效识别和分析，提高对敏感数据安全监控的准确性。

数据访问控制，需要穿透学院原有应用，完全针对学院的数据实施保护控制，避免数据因某个应用遭受入侵而失控；多重保障，在学院原有的应用系统安全的基础上，再次对数据安全进行了巩固，形成双重安全壁垒，同时又互不冲突，使数据安全如虎添翼；同时提供黑名单、白名单的双向认证，实现更加灵活、便捷的组合控制；兼容大数据平台的多种组件，性能高效；控制授权，可基于角色、组、用户不同集合进行灵活授权。

数据脱敏是针对每种敏感数据类型均提供了高度仿真的脱敏算法，保证脱敏后的数据不可逆，保持原有的特征、语义，保证不同表之间相同字段的数据关联性，保证数据的长度不超过表结构，能够顺利入库。当数据进入后，系统能自动运行数据扫描任务，先从数据源中获取少量的样本数据，再与系统内置的敏感数据指纹特征进行比对，快速识别敏感数据类型，并记录敏感数据的存放位置。从便利性和可持续性上看，脱敏规则需要灵活丰富，根据实际需要提供数据遮蔽、数据仿真、关键部分替换、随机字符串、重置固定值等多种多样的敏感数据处理方式，从而实现隐蔽或模糊处理真实敏感数据信息的目的，提高生产数据在应用开发、测试以及第三方工具做数据分析等使用场景中的安全性。通过数据脱敏系统的使用，可以有效防止单位内部的敏感数据随意导出，防止敏感数据在未经处理的情况下从开放的环境中被复制、流出、泄露等。

数据加密传输需要在学院的核心服务器上部署加密软件，主要通过对文档的加密保护，防止内部教职工、学生泄密和外来人员非法盗取并使用学院的核心重要数据资产。保护范围涵盖终端电脑（Windows、Linux 系统平台）、智能终端（Android、IOS）及各类应用系统（OA、知识管理、文档管理、项目管理、PDM 等），根据用户需求可以对表空间结构、电子文档进行自动加密、手动加密、智能加密和文档细粒度权限控制，对文档的全生命周期进行安全管控，做到事前防御、事中控制、事后审计，帮助学院搭建一套完善的文档防泄密体系。

图 2　加密软件部署示意图

4.3　学院数据安全管理制度建设

数据安全管理制度流程会从组织层面整体考虑和设计，从业务、风险和合规的角度出发，构建包含四级的数据安全管理制度体系框架，为组织提供数据安全规范，为日常工作流程提供标准依据，为组织业务合规和规避风险提供有力保障。数据安全管理制度体系如图 3 所示。

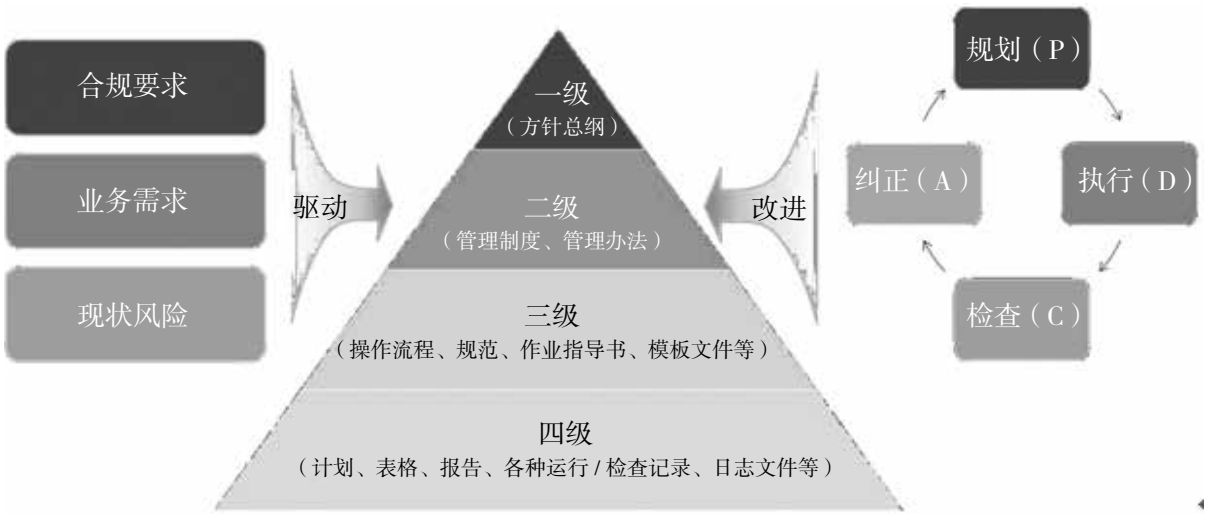

图 3　数据安全管理制度体系

另外，制定应急预案并不断改进完善应急预案体系，结合实际情况，定时进行安全演练，提高应急响应速度，健全应急预案体系。

4.4　学院数据安全管理组织建设

通过前期的咨询调研，针对学院的信息安全管理现状、业务流程、合规和风险需求设计出了数据安全管理组织架构，大体上分为以下几种。

决策层即数据安全管理工作的决策机构，是数据安全组织机构的第二层。建议由数据安全官及其他高层管理人员组成，数据安全官是组织内数据安全的最终负责人。数据安全官应能参与到组织的业务发展决策中，因为业务的发展和数据安全是密不可分的。除数据安全官外，其他高层管理人员对于数据安全的重视和决策是非常重要的，决策层也需要其他业务、法务、研发等高管共同组成，形成定期的沟通运作机制。

管理层是数据安全组织机构的第二层，基于决策层给出的策略和要求，对数据安全实际

工作制定详细的实施方案，做好业务发展与数据安全之间的平衡。在组织中起到承上启下的作用。

执行层与管理层有着紧密配合的关系，其职责主要聚焦每一个数据安全场景，对设定的流程逐个实现，参与人员包括执行层主要数据安全管理人员以及各业务部门的数据安全管理人员和数据所有者等。

教职工和合作伙伴，范围包括学院教职工和有合作的第三方人员，须遵守并执行学院内对数据安全的要求，尤其是共享数据的第三方，必须从保密协议、数据使用环境、办公环境和技术工具等方面做好约束和管理。

监督层，数据安全监督层负责定期监督审核管理小组、执行小组，员工和合作伙伴对数据安全政策和管理要求的执行情况，并且向决策层进行汇报，监督层人员必须具备独立性，不能与其他管理小组、执行小组等人员共同兼任，建议由组织内部的审计部门担任。

4.5 学院数据安全人员能力建设

数据安全的人员能力主要包括几个维度，数据安全管理能力、数据安全运营能力、数据安全技术能力和数据安全合规能力。我们将会提供四个维度的安全技能培训或安全意识宣传，从而提升全体教职员工的数据安全意识和专业能力。

其中数据安全意识培训服务包括但不限于数据安全国际及国内环境事件分析、数据安全风险分析、数据安全政策法规解读等；数据安全技术培训包括但不限于数据库安全常规技术手段、数据库安全态势感知、大数据安全常规防护手段、大数据安全全生命周期管控技术、大数据安全态势感知等。通过培训提升全校师生的数据安全使用意识。

5 结语

集美大学诚毅学院数据安全管理平台建设工作，是学院认真贯彻《中华人民共和国网络安全法》《中华人民共和国数据安全法》和高校“十四五”信息化发展规划的产物。当今数据作为重要资产在高校中已经逐渐被重视和利用。如何确保数据在流通过程中的安全是一个值得我们深入研究的问题。根据集美大学诚毅学院在数据安全管理平台建设工作中所遇到的问题及解决方法，我们总结出了以下几个方面的建议。

从顶层设计出发，制定数据安全管理平台的目标和策略。要明确数据安全管理平台要解决的问题和需求，如数据资产清晰、数据风险可控、数据价值可挖掘等。要结合自身的业务特点和发展阶段，制定合理的数据安全管理平台的架构和功能模块，如数据资产管理、数据安全防护、数据风险监测、数据安全审计等。

从技术创新入手，提升数据安全管理平台的能力和效率。要引入先进的技术工具和方法，如人工智能、区块链、差分隐私等，提升数据安全管理平台的技术水平和性能。要探索新的技术应用和场景，如数据治理、数据价值挖掘、数据资产化等，实现数据安全管理平台的创新发展。

从法律法规着眼，保障数据安全管理平台的合规性和可信度。要遵循国家和行业的相关标准和规范，如《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等，确保数据安全管理平台符合法律要求。要建立完善的数据安全管理制度和流程，如数据分类分级、数据权限分配、数据使用审批等，保证数据安全管理平台的规范运行。

从人才培养着手，增强数据安全管理平台的人力支撑。要加强对数据安全管理人员的培训和考核，提高他们的专业素养和技能水平。要建立有效的激励机制和考核机制，鼓励数据安全管理人员积极参与数据安全管理平台的建设和运维。

日后，信息安全和数据安全将成为各高校“数字化转型”的重要课题之一。

参考文献

[1] 朱方彬. 大数据时代个人信息权保护的模式选择与制度设计［C］//中国—东盟数字经济高端论坛论文集. 南宁：广西知识产权学会，2018：102-109.

[2] 全国信息安全标准化技术委员会. 信息安全技术—网络安全等级保护基本要求：GB/T 22239—2019［S］. 北京：中国标准出版社，2019.

[3] 张芳芳，贾晓纯，李丽. 高校数据共享平台的数据安全管理系统建设方案［C］//中国计算机用户协会网络应用分会2021年第二十五届网络新技术与应用年会论文集. 重庆：《计算机科学》编辑部，2021：29-35.

[4] 顾瑞，张珍义，卢加元. 高校数据中心的安全问题研究［J］. 中国教育信息化，2008(21)：59-60.

[5] 方禹. 论对《网络安全法》第67条中“个人信息”的理解［J］. 网络信息法学研究，2020 (1)：41-54.

[6] 王世新，郑艺龙，姜开达. 高校要形成数据保护的氛围［J］. 中国教育网络，2021，2：23-25.

[7] 王鹏，王玉. 构建共享数据中心安全防护体系［J］. 中国教育网络,2022,1:79-80.

[8] 大数据安全工程研究中心（贵州）有限公司. 一种基于DSMM的数据采集安全检测方法：CN202111246365.9［P］. 2022-03-01.

[9] 孔策. A银行数据安全风险分析与防范研究［D］. 北京：中国科学院大学，2020.