上 海 教 育 信 息 化 规 范

编号：SJX/T 004-2020

上海教育数据安全管理规范

（本发布版最后修订日期： 2021-7-23）

上海市教育委员会信息中心

目 录

第一章 总则

第一条 为规范上海教育数据安全管理工作，推动数据及其应用过程的安全管理，提升数据安全管理水平和能力，特制定本管理规范。

第二条 本规范依据《中华人民共和国网络安全法》（中华人民共和国主席令（第五十三号））、《中华人民共和国数据安全法》（中华人民共和国主席令（第八十四号））、《儿童个人信息网络保护规定》、《教育部机关及直属事业单位教育数据管理办法》（教发厅〔2018〕1号）、《关于加强教育系统数据安全的指导意见》、《教育部机关和直属事业单位数据安全管理办法》、《上海市公共数据和一网通办管理办法》（上海市人民政府令第9号）、《上海教育数据管理办法（试行）》等文件制定，参照《GBT 35274-2017 信息安全技术 大数据服务安全能力要求》、《GBT 37973-2019 信息安全技术 大数据安全管理指南》等标准，旨在明确数据安全管理的角色和职责，防止数据在未经授权和许可的情况下被泄露、误用和滥用，规范对数据的操作行为。

第三条 本规范所指的上海教育数据包括上海市教育委员会（以下简称“市教委”）、各区教育局及其辖区内的公办中小学和幼儿园、各市属公办高等学校（以下简称“各高等学校”）和各市属公办中等职业学校（以下简称“各中职校”）等教育单位（部门）（以下简称“各级各类教育单位”）在履行职责过程中产生、采集和使用的各类非涉密数据。涉密数据管理按照国家和本市有关法律、法规进行。

第四条 本规范围绕上海教育数据生命周期各个环节的安全和数据安全专项提出管理要求。数据生命周期安全涉及数据采集及归集安全、传输安全、存储安全、处理安全、共享及交换安全和销毁安全，并参照《上海教育数据分级分类规范》实施分级安全管控，数据分级安全管控实施细则参见附件一。数据安全专项管理主要包含人员安全管理和数据安全事件管理。

第五条 数据安全应满足保密性、完整性和可用性的基本原则：

（一）保密性：数据不提供或泄露给非授权的个人、过程或其他实体；

（二）完整性：信息及信息系统不被非授权更改或破坏，包括数据完整性和系统完整性；

（三）可用性：被授权实体按要求能访问和使用数据。

第二章 角色和职责

第六条 根据《上海教育数据管理办法》（试行），数据管理组织架构包括数据提供部门、数据使用部门、数据管理协调部门和数据技术管理部门。职责和权利由《上海教育数据管理办法》（试行）确定。

第七条 数据管理协调部门负责数据安全管理的决策、协调和组织工作，主要内容包括：

（一）负责数据安全管理体系、数据安全管理组织架构的规划和建设；

（二）制定数据安全管理相关的制度；

（三）负责数据安全管理的监督工作。

第八条 数据技术管理部门负责数据安全管理相关工作，内容包括：

（一）数据安全事件的应急处置；

（二）制定数据安全应急预案，组织定期演练；

（三）组织开展数据安全自查和风险评估工作；

（四）组织安全管理制度、技术和意识培训。

第九条 数据提供部门和数据使用部门负责其部门内部的数据安全管理工作，内容包括：

（一）提出数据安全管理需求，配合数据安全管理相关工作；

（二）跟踪部门内发现的数据安全问题并给出解决建议；

（三）对部门内出现的数据安全事件及时上报并采取适当的处理措施；

（四）评估数据采集场景的安全风险并制定对策。

第十条 各级各类教育单位应遵循合法、正当、必要的原则加强个人信息保护，编制本级数据安全规划，建立教育数据安全体系，制定并督促落实教育数据安全管理制度，加强安全保障，落实承担数据安全管理职责各角色的人员，并明确培训技能、考核内容与考核指标，定期对数据安全管理人员进行审查和能力考核。定期开展第三方安全审计工作，对审计过程发现的不符合项进行整改。

第十一条 各级各类教育单位宜设置数据安全管理组组长、数据安全管理员、数据获取员、数据需求协调员、数据介质管理员、系统管理员等安全管理岗位，具体职责建议参见附件二。

第三章 数据采集及归集安全

第十二条 数据提供部门应定义采集数据的目的和用途，明确数据采集源和采集数据范围;遵循合规原则，确保数据采集的合法性、正当性和必要性;遵循数据最小化原则，只采集满足业务所需的最少数

据;遵循质量保障原则，制定数据质量保障的策略、规程和要求;明确数据收集和获取过程中个人信息和重要数据的知悉范围和安全管控措施，确保采集数据的合规性、完整性和真实性。

第十三条 数据提供部门采集数据应严格按照业务需求和职能边界确定数据采集使用范围，优先通过共享获取数据，原则上不得重复采集数据。利用第三方平台和教育 App 采集数据应签订数据使用和保密协议。

第十四条 采集使用个人信息应以通俗易懂、简单明了的方式展示采集使用规则，并经个人信息主体同意后方可实施。采集教职工、师生、家长的数据时，应公开采集使用规则，明示采集使用数据的目的、方式和范围。采集使用未成年人个人信息应以显著、清晰的方式告知未成年人监护人，并征得监护人的同意。不得以默认、捆绑、停止安装使用等手段变相强迫授权，不得违反法律法规和超越约定来收集使用个人信息。

第十五条 采集 100 万人以上个人信息的信息系统计划应报教育部网信领导小组审核同意后方可实施，且网络安全等级保护应定为三级以上。采集使用教职工、学生、家长的人脸、指纹、虹膜、声纹、DNA、步态、签名等可识别自然人的生理特性与行为特征的个人生物识别信息，信息系统网络安全等级应在三级以上。

第十六条 数据提供部门应参照《上海教育数据分级分类规范》对采集的数据进行分级分类标识，对不同类型和级别的数据实施相应的安全管理策略和保障措施，对数据采集环境、设施和技术采取必要的安全管控措施，对操作、变更过程进行评审、记录，为数据分级分类管理奠定基础。

第十七条 教育数据的采集及归集应进行数据溯源管理，实现数据源的鉴别以确保数据来自于已认证的数据源；保留数据链路上每次变化情况的日志记录；保证操作可追溯，实现数据的版本管理、恢复和回退。

第十八条 数据提供部门应建立数据采集的风险评估机制，针对采集的数据源、范围、频度、渠道、程序、数据类型等进行风险评估。如涉及采集个人信息和重要数据的业务场景，应进一步依据相应的合规要求进行风险评估，防范采集过程中可能存在的数据泄漏风险。

第四章 数据传输安全

第十九条 数据传输是指依照适当的标准或要求，数据经过一条或多条链路，在数据源和数据宿之

间传送。

第二十条 数据传输安全主要包括物理传输安全和通信传输安全。

第二十一条 物理传输过程中应确保移动介质安全和传输人员操作安全，传输过程中应记录获取数据的所有操作及具体人员信息。

第二十二条 通信传输过程中应确保传输设备安全和网络安全，防止数据通过各类网络应用泄露。

第二十三条 涉及到国家重要信息、单位敏感信息和个人隐私信息的数据传输场景，应在数据分级分类的基础上进行加密传输或专线，数据传输过程中应防止被传输或路由到境外。

第五章 数据存储安全

第二十四条 数据存储指数据以某种格式记录在计算机内部或外部存储介质上。

第二十五条 各级各类教育单位应在数据分级分类的基础上建立数据存储策略，选择合适的数据存储介质，确定相应的保存期限，将不同类别和级别的数据分开存储，并采取物理或逻辑隔离机制。各级各类教育单位可采用密码技术保证存储安全，密码技术和产品使用应符合国家密码管理部门要求。

第二十六条 各级各类教育单位应建立数据存储冗余策略和管理制度，以及数据备份与恢复操作过程规范。确保分布式存储的数据及其副本的完整性，并定期备份在线数据；确保发生突发情况时能对数据进行备份恢复，以降低数据丢失的风险。数据存储应遵循“最短周期”原则，数据在信息系统上的存储期限不得超过业务有效期，超过存储期限的数据应进行归档或销毁。个人生物识别信息原则上应存储于用户终端，教育部直属机关不进行集中存储。各级各类教育单位应负责定期进行数据归档，保证历史数据的完整性和有效性，确保归档数据查找和使用的便利性，同时减少备份系统的负担。归档系统应与互联网隔离，仅提供查看功能，保障数据安全。

第二十七条 各级各类教育单位应确保在人为破坏、软硬件故障、灾难灾害或突发公共安全事件等情况下，避免数据的丢失和损坏，保证数据完整、可用，保障业务连续性。

第二十八条 各级各类教育单位应明确数据迁移的范围、目标位置、迁移频率及迁移方式等。

第二十九条 各级各类教育单位应对数据库日志动态监控，主要包括访问日志、应用日志、数据存储日志、数据获取日志等，尤其应关注个人隐私信息的相关日志。

第三十条 在境内运营采集和产生的非公开数据原则上应在境内存储。因业务需要，确需向境外提

供的，应按国家规定开展数据出境安全评估。

第三十一条 个人信息应采用加密存储设施，存储最高安全级别数据或100万人以上个人信息的单位应明确个人信息保护岗位和负责人，统筹单位内部的个人信息安全工作，采取存储加密的方式保障数据安全，信息系统（网站）应向市教委备案，网络安全等级保护应定为三级以上。教育行政部门和学校开发的存储100万以上个人信息的应报市教委审核同意方可实施。

第六章 数据处理安全

第三十二条 数据处理是指对数据进行计算、分析、挖掘、可视化等多种活动的集合，是体现数据价值的核心环节。

第三十三条 各级各类教育单位应依据个人信息和重要数据保护的法律法规要求，明确数据处理的目的和范围；建立数据处理的内部责任制度，保证分析处理和使用数据不超出声明的数据使用目的和范围；遵循最小授权原则，提供数据细粒度访问控制机制；遵循可审计原则，记录和管理数据处理活动中的操作。

第三十四条 各级各类教育单位应规范个人信息安全使用，如建立用户画像不得侵害公民和法人的合法权益。严格限制未成年人信息访问和管理权限，开展数据活动应征得数据主管单位同意，并采取技术措施，记录访问情况。使用数据画像和自动化决策分析技术处理未成年人信息应报市教委审核，不得将未成年人的数字画像用于商业用途。

第三十五条 各级各类教育单位应严格规范个人生物识别信息应用，将个人生物识别信息用于识别个人身份的，应经单位领导班子集体决策同意后方可实施；将个人生物识别信息用于分析个人行为的，应对科学性进行论证，广泛征求用户意见，并报省级以上教育行政部门审核同意后方可实施。其中：部属单位报教育部审核，其他单位报市教委审核。鼓励通过共享权威个人生物识别信息库的方式开展个人身份验核，在提供服务过程中，不使用人脸作为身份验证的唯一手段。

第三十六条 数据技术部门应建立统一的数据清理、转换和加载流程，明确人员权限、操作和执行步骤，保证清洗、转换与加载过程中对数据的保护。针对个人信息和重要数据，建立数据清洗、转换与加载过程中的数据还原和恢复机制。

第三十七条 各级各类教育单位应建立数据脱敏规范和流程，通过脱敏技术和方法，对个人信息、

组织敏感数据、国家重要数据等进行脱敏、变形等处理，保障数据在开发、测试和其它非生产环境以及外包环境中的应用安全。

第三十八条 各级各类教育单位应制定数据分析结果风险评估机制，确保衍生数据不超过原始数据的授权范围和安全使用要求，避免分析结果输出中包含可恢复的个人信息、重要数据等数据及其结构标识，防止敏感信息的泄漏。

第三十九条 各类各级教育单位的数据处理类平台应具备权限管理、日志管理、安全策略控制、安全审计等能力，实现数据管理、使用和安全审计的权限分离，并保留相关日志不少于六个月。

第七章 数据共享及开放安全

第四十条 各级教育数据资源管理技术平台应具备敏感数据保护、日志审核、风险控制等能力。

第四十一条 数据共享及开放应参照《上海市公共数据开放暂行办法》（沪府令 21 号）、《上海教育数据分级分类规范》等要求，针对不同安全级别的数据实施相应安全管理措施，重点保护个人信息，特别是未成年人个人信息，需公开展示的个人信息应采取去标识化处理。

第四十二条 数据共享及开放应通过数据库表、文件或接口的形式进行，并通过相应安全策略保障共享及开放过程安全。

第四十三条 共享 100 万以上个人信息的应报市教委审核同意方可实施。

第四十四条 共享未成年人信息应严格按照数据共享责任清单的范围，原则上不得向第三方共享未成年人数据，确需共享时应进行数据安全评估并签订安全责任书。除法律、行政法规规定和监护人的约定外， 不得披露未成年人信息。

第八章 数据销毁安全

第四十五条 数据销毁是指将符合销毁标准的数据彻底删除，并无法复原，以免造成信息泄露。

第四十六条 在介质销毁前应对介质中的数据进行销毁处理，确保存储在介质中的数据无法恢复。

第四十七条 数据销毁应根据数据的分级分类采用不同的数据销毁方式，销毁过程至少保证有双人在现场，并记录数据销毁的操作时间、操作人、操作方式、数据内容等相关信息。

第四十八条 各级各类教育单位应建立数据销毁效果评估机制，对已经完成数据销毁的存储介质进

行抽样的销毁效果认定，以保证对数据销毁工具的持续改进和销毁方案的整体优化；同时，建立已共享或已被其他用户使用数据的销毁管控措施。

第九章 人员安全管理

第四十九条 各级各类教育单位应制定人员安全管理制度，明确不同岗位人员在数据生命周期各阶段的工作范畴和安全管控措施。对接触数据的人员进行授权、审批和登记,并签署保密协议,定期对人员行为进行安全审查。在重要岗位人员调离或终止劳动合同时，回收其因职务需要所持有或保管的数据及介质。

第五十条 各级各类教育单位应明确关键岗位人员安全能力要求,并确定其培训技能考核指标与考核内容,定期对关键岗位人员进行审查和能力考核。

第五十一条 各级各类教育单位应制定安全教育计划，按计划对相关人员开展安全教育,包括政策、法律、法规和标准等，并对教育结果进行记录和归档。

第十章 数据安全事件管理

第五十二条 数据安全事件包括数据篡改事件、数据假冒事件、数据泄漏事件、数据窃取事件、数据丢失事件、其它数据破坏事件等。

（一）数据篡改事件:是指未经授权将信息系统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，例如系统数据在没有获得授权的情况下被改变；

（二）数据假冒事件：是指通过假冒他人收发数据而导致的数据安全事件；

（三）数据泄漏事件：是指因误操作、软硬件缺陷等因素导致信息系统中的敏感、个人隐私等数据暴露于未经授权者而导致的数据安全事件；

（四）数据窃取事件:是指未经授权而利用可能的技术手段恶意主动获取信息系统中数据而导致的数据安全事件；

（五）数据丢失事件：是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的数据删除、丢失而导致的数据安全事件；

（六）其它数据破坏事件：是指不能被包含在以上 5 个类别之中的数据破坏事件。

第五十三条 根据数据安全事件对个人、组织、客体造成的损害和影响程度不同，数据安全事件分为特别重大事件、重大事件、较大事件、一般事件。

（一）特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况:

1.会使特别重要的信息系统遭受特别严重的系统损失;

2.产生特别重大的社会影响。

（二）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.会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失;

2.产生的重大的社会影响。

（三）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.会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失;

2.一般信息信息系统遭受特别严重的系统损失;

3.产生较大的社会影响。

（四）一般事件是指不满足以上条件的信息安全事件，包括以下情况:

1.会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失;

2.一般信息系统遭受严重或严重以下级别的系统损失;

3.产生一般的社会影响。

第五十四条 数据安全事件，遵循“谁主管、谁负责，谁使用、谁负责”的原则，对各类数据安全事件和可能引发数据安全事件的有关信息进行收集、评估和持续监测，各级各类教育单位应协同市教委，加强与网络安全职能部门、专业机构、行业协会和企业的合作，建立数据安全监测预警机制，通过远程监测等方式，及时发现数据安全威胁，并将数据安全事件上报管理协调部门，管理协调部门组织技术管理部门评估安全事件影响范围，协调相应单位处理安全事件。事件响应时限与流程参见附件三和附件四。

第五十五条 各级各类教育单位的全体员工及第三方服务商人员有义务对发现的安全弱点及时上报。相关部门对发现的安全弱点应及时进行整改处理，避免数据安全事件的发生。

第五十六条 数据安全事件应急处理完毕，业务流程恢复正常后，单位内负责数据安全管理的组织或相关负责人应开展事件总结工作，审查所有应急记录和文件等资料，分析事件发生的原因、对应的弱点和威胁，总结和评价导致应急响应工作的突发事件情况和在应急响应期间采取的主要行动，指出当前

需要增强或增加的控制措施，并完善应急预案。

第五十七条 为预防同样数据安全事件再次发生，各级各类教育单位应不定期进行安全抽查，对各项制度、计划、方案、人员和物资等方面进行验证。对发现的安全弱点应及时上报数据管理协调部门。对未有效落实预防措施、事件处理方案和有关规定的内部人员进行通报批评。对第三方服务商产生的安全弱点，应通报其项目负责人，并督促其限时整改，逾期未整改完成的将按照相关规定对其所在公司进行问责、处罚直至终止合同。

第五十八条 数据管理协调部门应将数据安全事件的应急处理和工作流程等作为数据安全风险培训的内容，增强数据安全事件处置工作中的组织能力。

第五十九条 数据管理协调部门负责数据安全事件应急预案的制定和演练实施方案的制定，并不断完善应急方案内容，定期对应急预案进行评估和修订；根据国家法律法规和行业监管要求等变化，及时对应急预案进行修改和完善。数据技术管理部门组织安排数据安全突发事件应急演习。

第六十条 市教委将协同各级各类教育单位，全面掌握数据安全动态，并将数据安全，特别是个人信息保护工作纳入对各级各类教育单位履行教育职责督导评估，形成投诉联动机制，及时受理投诉举报，主动回应社会关切。

第十一章 附则

第六十一条 本规范由上海市教育委员会信息中心负责解释。

第六十二条 本规范自发布之日起施行。

第六十三条 部属高等学校、行业主管的中等职业学校、各类民办学校和中外合作办学学校参照执行。

附件一：数据分级安全管控实施细则

数据分级安全管控依据“谁主管、谁负责，谁使用、谁负责”的原则实施管理。数据定级定类依据《上海教育数据分级分类规范》实施，数据在生命周期管理中实施分级安全管控的总体要求如附表 1 所示。

附表 1 内部分级管控总体要求

级别	分级管控要求
第 4 级	实施最严格的内部安全管理措施、审批制度及应急处置措施。并将相关的安全责任落实到接触数据个人，签订个人安全承诺； 实施最严格的数据全生命周期安全管理；采用严格的技术措施保障数据安全；建立实时安全预警机制。
第 3 级	实施严格的内部安全管理措施、审批制度及应急处置措施。并将相关的安全责任落实到接触数据个人，签订个人安全承诺； 实施严格的数据全生命周期安全管理；采用严格的技术措施保障数据安全；建立准实时安全预警机制。
第 2 级	实施必要的内部安全管理措施、审批制度及应急处置措施。并将相关的安全责任落实到项目负责人，签订负责人安全承诺； 实施必要的数据全生命周期安全管理；采用必要的技术措施保障数据安全；建立准实时安全预警机制。
第 1 级	实施基本的内部安全管理措施； 实施基本的数据全生命周期安全管理。

（一）数据采集及归集环节

数据采集及归集环节对各级数据管控要求包括物理监控、物理防护、人员访问管理、待采集/归集数据管理、账号权限管理、采集设备接入管理、采集监控告警、数据线下交互过程管控等方面，具体要求如附表 2 所示。

附表 2 采集及归集环节分级管控要求

类别	第 1 级	第 2 级	第 3 级	第 4 级
物理监控			针对数据采集/归集重要区域，部署全天候视频监控记录手段。	
物理防护			对重要系统实施机柜上锁等物理防护手段，必要时可实施机房内分区隔离措施。	
待采集/归集数据保护	采取必要的技术手段或管控措施，对收集和获取到的数据进行完整性和一致性校验。		待采集/归集数据采取数据加密保护；保证个人信息和重要数据不被泄露。	
人员访问管理	针对机房内实施或第三方参与的操作，安排内部人员现场监督，做好操作步骤记录和事后审计。			
账号权限管理	依据权限最小化原则分配采集/归集账号权限，并通过 4A 管控（认证 Authentication、授权 Authorization、账号 Account、审计 Audit）实现账号认证和权限分配，不得采集/归集提供服务所必需以外数据。			
采集设备接入管理	对采集设备 IP 地址，Console、USB 端口访问进行限制，对采集设备接入进行认证鉴权。			
采集监控告警	跟踪和记录数据收集和获取过程，支持对数据收集和取操作过程的可追溯性；记录采集日志，对重复采集、采集异常、传输量超过设定阀值情况进行告警。			
数据线下交互过程管控	加强数据线下交互的过程管控，对数据线下交互建立审批机制及操作流程，要求对线下交互数据采取加密脱敏、物理封装等防护手段，防止数据被违规复制、传播、破坏等。			

（二）数据传输环节

数据传输环节对各级数据管控要求包括网络边界安全防护、接口安全、数据传输保护、物理传输等方面，具体要求如附表 3 所示。

附表 3 传输环节管控要求

<table>
<tr><th>类别</th><th>第 1 级</th><th>第 2 级</th><th>第 3 级</th><th>第 4 级</th></tr>
<tr><td>网络边界安全防护</td><td colspan="4">1、区分安全域内、安全域间等不同的数据传输场景，建立相应的数据传输安全策略和规程；
2、在网络边界上针对数据流向做好隔离封堵的限制。</td></tr>
<tr><td>接口安全</td><td colspan="2">建立数据传输接口安全管理工作规范，包括安全域内、安全域间等数据传输接口规范。</td><td colspan="2">当发现被保护主机上的数据通过接口被违规转移出主机时，对其主机的数据泄露行为采取拦截或报警设置。</td></tr>
<tr><td>数据传输保护</td><td>1、对传输通道采取合理的加密技术手段，具备在构建传输通道前对两端主体身份进行鉴别和认证的能力，对数据报文实施来源正确性的鉴别处理；
2、能够检测重要数据在传输过程中完整性是否受到破坏。</td><td>除满足第 1 级数据传输保护要求外，应符合如下要求:
1、对于跨安全域的数据传输，应采用加密或其他有效措施实现传输保密性；
2、提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统高可用性。</td><td colspan="2">除满足第 2 级数据传输保护要求外，应符合如下要求:
1、在检测到传输过程中数据完整性错误时采取必要的恢复控制措施；
2、应采用加密或其他有效措施实现传输保密性；
3、建立机制对数据传输安全策略的变更进行审核和监控，包括对通道安全配置、密码算法配置、密钥管理等保护措施的审核及监控。</td></tr>
<tr><td>物理传输</td><td colspan="2">1、从可信渠道购买或获得存储介质，采取有效的介质净化技术和规程对存储介质进行净化；
2、对存储介质进行标记，明确介质存储的数据对象，并对介质访问和使用行为进行记录和审计；
3、进行常规和随机检查，确保存储介质的使用遵守单位制定的关于介质的使用规范；
4、根据不同的安全管理需要将移动介质设置为通用和专用两类，通用介质在单位内部和外部都能使用，专用介质只能在单位内部使用，在单位外部不能使用；
5、邮寄数据移动介质应使用中国邮政 EMS。</td><td colspan="2">维修、销毁前应清除介质中的敏感数据，并对维修、销毁等处理活动进行登记，由专门的技术人员负责对介质维修、销毁。</td></tr>
</table>

（三）数据存储环节

数据存储环节对各级数据管控要求包括存储架构、逻辑存储、数据存储隔离、访问控制、数据可用性和完整性保护、数据副本、数据归档和数据时效性等，具体要求如附表 4 所示。

附表 4 存储环节管控要求

类别	第 1 级	第 2 级	第 3 级	第 4 级
存储架构	1、建立开放可伸缩数据存储架构，以满足数据量持续增长、数据分级分类存储等需求； 2、确保存储架构具备数据存储跨机柜或跨机房容错部署能力。	通过相关的管理规范和安全规则制定、技术和管控措施保障等，确保访问控制、存储转移安全、存储完整性和多副本一致性。	具备对个人信息、重要数据等加密存储能力。	
逻辑存储	1、满足不同数据类型、不同数据容量和不同业务需求的逻辑存储安全管理要求； 2、建立数据分片和分布式存储安全规范和规则，满足分布式存储下分片数据完整性、一致性和保密性保护要求。			
数据存储隔离	对不同安全等级的数据进行隔离存储，并在各自存储区域之间做好严格的访问控制限制。			
访问控制	建立存储系统安全管理员的身份标识与鉴别策略、权限分配策略及相关操作规程。	除满足第 1 级要求外，需符合如下要求： 实施用户身份标识与鉴别策略、数据访问控制策略、数据扩容及复制策略等，并实现相关安全控制措施。	除满足第 2 级要求外，需符合如下要求： 1、具备访问控制时效的管理和验证，以及应用接入数据存储的合法性和安全性取证机制； 2、具备数据分布式存储访问安全审计能力，建立受保护的审计信息存储机制和管控措施。	除满足第 3 级要求外，需符合如下要求： 建立数据存储安全主动防御机制或措施，如基于用户行为或设备行为安全控制机制。
数据可用性和完整性保护		硬件冗余，保证系统高可用性	除满足第 2 级要求外，需符合如下要求： 1、应能够检测重要数据在存储过程中完整性是否受到破坏，并在检测到完整性错误时采取必要的恢复	除满足第 3 级数据传输保护要求外，需符合如下要求: 应进行异地灾难备份、异地实时备份，提供业务应用的实时无缝切换。

			措施； 2、应采用加密或其他保护措施实现数据存储保密性； 3、应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放； 4、应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。	
数据副本	1、建立数据存储冗余策略和管理制度，以满足大数据服务可靠性、可用性等数据安全保护目标； 2、建立数据复制、备份与恢复操作过程规范，包括复制、备份和恢复的日志记录规范。		1、建立数据冗余强一致性、弱一致性等控制策略与规范，以满足不同一致性水平需求的数据副本多样性和多变性存储管理要求； 2、建立数据复制、数据备份与恢复的定期检查和更新工作程序，包括数据副本更新频率、保存期限等，确保数据副本或备份数据的有效性； 3、具备数据副本或数据备份存储的多种压缩策略和实现机制，并确保压缩数据副本或数据备份的完整性和可用性。	
数据归档	1、依据数据生命周期和业务规范建立不同阶段数据归档存储相关的操作规程； 2、建立在线/离线的多级数据归档架构，支持海量数据的有效归档、恢复和使用； 3、建立归档数据的安全策略和管控措施，确保非授权用户不能访问归档数据； 4、建立归档数据的压缩或加密策略，确保归档数据存储空间的有效利用和安全访问； 5、定期地采取必要的技术手段和管控措施查验归档数据完整性和可用性； 6、建立归档数据安全审计与恢复制度，并指定专人负责。			
数据时效性	1、明确数据分享、存储、使用和清除的有效期，具备数据存储时效性授权与控制能力； 2、建立过期存储数据及其备份数据彻底删除方法和机制，能够验证数据已被完全消除或使其无法恢复。		1、建立过期存储数据的安全保护机制，对超出有效期的存储数据应具备再次获取数据控制者授权的能力； 2、具备数据时效性自动检测能力，包括但不限于告警、自动清除以及拒绝访问。	

（四）数据处理环节

数据处理环节对各级数据管控要求包括账号权限管理、数据清洗、转换与加载、数据质量监控、数据分析挖掘、数据查询展现等方面要求，具体要求如附表五所示。

附表 5 数据处理环节管控要求

类别	第 1 级	第 2 级	第 3 级	第 4 级
账号权限管理	依据权限最小化原则分配账号权限，通过 4A 管控技术手段统一实现账号认证和权限分配；各级数据资源管理技术平台对不同等级的数据设置不同的访问权限，用户只能访问与本人工作职责相对应的数据；及时回收过期的数据访问权限。			
数据清洗、转换与加载	1、制定数据清洗、转换和加载操作相关的安全管理规范，确保清洗和转换前后数据间映射关系； 2、采取必要的技术手段和管理措施，确保在数据清洗、转换和加载过程中对数据进行保护。		1、记录并保存数据清洗、转换和加载过程中个人信息、重要数据等数据的处理过程，保证 ETL 过程中产生问题时能有效的还原和恢复数据； 2、具备数据清洗、转换和加载数据一致性检测及故障处理能力。	
数据质量监控	1、建立质量监控规则，明确数据质量监控范围及监控方式； 2、明确数据质量评价要素，建立异常事件处理流程和操作规范，指定处理对应质量监控项的责任部门或人员； 3、定期对数据质量进行分析、预判和盘点，明确数据质量问题定位和修复时间要求。			
数据分析挖掘要求	1、各级数据资源管理技术平台统一提供分析用数据及数据分析功能，进行业务模型训练、业务数据分析，分析结果以群体数据形式提供共享开放； 2、防止数据被恶意删除、随意篡改、无约束的滥用，应对原始数据和挖掘结果进行签识。		1、建立多源数据派生、聚合、关联分析等数据分析过程中的数据资源操作规范和实施指南； 2、对数据分析结果共享的风险进行合规性评估，避免分析结果输出中包含可恢复的个人信息、重要数据等数据和结构标识，如用户鉴别信息的重要标识和数据结构； 3、对数据分析过程个人信息、重要数据等敏感数据操作进行记录，以备对分析结果质量和真实性进行数据溯源； 4、应具备基于机器学习的重要数据自动识别、数据安全分析算法设计等数据分析算法及其安全性分析能力。	
数据查询展现要求	对敏感信息进行对外查询、展现、统计等操作时，必须经过模糊化处理。			

特定要求			1、对敏感数据访问应进行模糊化或脱敏处理； 2、不同应用之间应进行数据关联性隔离，防止因数据关联分析产生数据泄露； 3、供开发人员使用的测试数据必须经过模糊化处理； 4、移动介质中的数据必须进行加密保护。	除满足第 3 级要求外，应满足如下要求： 高风险操作应遵循多人操作管理，确保单人无法拥有重要数据的完整操作权限。

（五）数据共享及开放环节

按照确定后的数据安全等级，参照《上海教育数据分级分类规范》8.1、8.2 和 8.3 进行数据共享及开放。数据共享及开放环节数据分级管控要求包括数据导入导出、数据共享、数据发布、数据交换监控等方面，具体要求如附表 6 所示。

附表 6 数据共享及开放环节管控要求

类别	第 1 级	第 2 级	第 3 级	第 4 级
数据导入导出	1、综合数据量、增长速度、业务需求、性能等因素制定数据导入导出策略与规程； 2、建立数据导入导出安全评估机制和授权审批流程； 3、对导入导出终端、用户或服务组件等执行身份鉴别，验证其身份的真实性和合法性； 4、制定导入导出审计策略和审计日志管理规范，并保存导入导出过程中的出错数据处理记录。	1、依据数据分级分类要求建立授权策略、不一致处理策略和流程控制策略； 2、采取多因素鉴别技术对数据导入导出操作员进行身份鉴别。	1、采取数据加密、访问控制等技术措施，保障导入导出数据在传输中的保密性、完整性和可用性； 2、在导入导出完成后对数据导入导出通道缓存的数据进行清除且保证不能被恢复； 3、为数据导入导出通道提供冗余备份能力，确保数据安全可靠导入导出要求； 4、对导入导出接口进行流量过载监控，确保海量数据导入导出过程安全可控。	
数据共享	1、明确数据共享涉及机构或部门相关用户职责和权限，保证数据共享安全策略有效性； 2、技术支持部门审核共享数据应用场景和数据内容，确保没有超出授权使用范围； 3、审核共享数据的数据内容，确认属于满足大数据共享业务场景需求范围； 4、配置专业数据共享机制或服务组件，明确数据共享最低安全防护基线要求； 5、对于数据共享开放的所有操作和行为进行日志记录，在安全事件发生后，能通过安全日志快速进行回溯分析； 6、具备违约责任、缔约过失责任、侵权责任等数据使用风险分析和处理能力。		1、明确数据使用部门的数据保护责任，确保其具备足够或相当的安全防护能力； 2、采用数据加密、安全通道等措施保护数据共享过程中的个人信息、重要数据等敏感信息； 3、数据使用部门不直接接触原始数据，主要通过治理表的方式（定制化的数据视图）共享数据； 4、具备信息化技术手段或机制，对数据滥用行为进行有效的识别、监控和预警。	
数据开放	参照《上海市公共数据开放暂行办法》（沪府令 21 号）执行。			

数据交换监控	1、采用自动和人工审计相结合的方法或手段对高风险数据交换操作进行监控； 2、记录数据交换操作事件，并制定数据交换风险行为识别和评估规则。	1、部署必要的数据防泄漏实时监控技术手段，监控及报告个人信息、重要数据等的外发行为； 2、使用工具对被监控的数据交换服务流量数据进行数据安全分析，具备对异常或高风险数据交换操作的自动化识别和实时预警能力； 3、记录数据交换服务接口调用事件信息，监控是否存在恶意数据获取、数据盗用等风险。
数据库表专项	1、对于明文数据，按列加密处理。进行权限分配，无权限的内部人员禁止查看全部明文数据； 2、建立数据归档机制，实现数据归档和读写分离； 3、对运维侧人员的数据库运维操作进行事前审批、和事中管控，防止出现误操作。	
文件专项	1、对文件进行分级保护，严禁随意下载文件数据，下载的文件不通过即时通讯工具传输，对于涉及敏感信息的文件数据，加密不同渠道传输文件和密码； 2、确认文件可打开次数、是否可复制、是否可打印、是否可修改、是否设置过期自动销毁等。	
接口专项	1、通过 HTTPS 协议构建可进行加密传输、身份认证的网络协议，解决信任主机和通讯过程中的数据泄密和数据被篡改的问题； 2、通过公私钥签名或加密机制提供细粒度的身份认证和访问、权限控制，满足数据防篡改和数据防泄漏要求； 3、实现时间戳超时机制，过期失效，满足防接口重放要求； 4、通过接口参数过滤、限制，防止接口特殊参数注入引发的安全问题； 5、通过接口参数限制，判断接口是否已经提交，如已经提交则抛系统异常并中断后续请求。	

（六）数据销毁环节

数据销毁环节数据分级管控要求包括存储介质管理、资源回收管理、数据销毁、销毁日志记录要求等方面，具体要求如附表 7 所示。

附表 7 销毁环节管控要求

类别	第 1 级	第 2 级	第 3 级	第 4 级
存储介质管理	1、对存储介质进行物理销毁的监督管理措施，确保对销毁的存储介质有登记、审批、交接等环节的记录； 2、依据介质存储内容的重要性明确磁介质、光介质和半导体介质销毁方法和机制； 3、针对闪存、硬盘、磁带、光盘等存储数据，建立硬销毁和软销毁的数据销毁方法和技术； 4、使用国家权威机构认证的机构或设备对存储介质设备进行物理销毁。			
资源回收管理	1、数据删除后应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除； 2、对于逻辑销毁，应为不同数据的存储方式制定不同的逻辑销毁方法，并确保当数据存在多个副本时，所有副本均被安全地删除。			
数据销毁	1、建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程； 2、应采用可靠技术手段删除敏感信息，确保信息不可还原； 3、针对网络存储数据，建立硬销毁和软销毁的数据销毁方法和技术，如基于安全策略、基于分布式杂凑算法等网络数据分布式存储的销毁策略与机制； 4、确保以不可逆方式销毁数据及其副本内容。			
销毁日志记录	数据超出保存期限时，对数据进行及时销毁，对销毁操作过程进行日志记录，建立完善的审计机制并严格执行。			
数据销毁特定要求		1、删除覆写数据并格式化； 2、按照国家相关法律和标准销毁个人信息、重要数据等敏感信息。	1、删除覆写数据，并格式化、然后对磁盘进行消磁； 2、建立已共享或者已被其他用户使用的数据销毁管控措施。	

附件二：数据安全管理角色职责建议

各级各类教育单位应建立教育数据安全管理组织架构，根据组织的规模、数据平台的数据量、业务发展及规划等明确不同角色及其职责，建议包含数据安全管理组组长、数据安全管理员、数据获取员、数据需求协调员、数据介质管理员和系统管理员等角色。各角色的职责具体如下：

（一）数据安全管理组组长的职责主要有：

1.设计数据安全管理体系；

2.建立数据安全管理体系的评审、发布流程，并对体系进行更新；

3.审批数据的获取范围和方式；

4.审批各类数据的存储方案；

5.审批数据备份、归档申请及方案；

6.审批各类数据的访问权限和脱敏方案；

7.审批数据的处理申请；

8.审批介质维修、转换、销毁申请；

9.审批数据安全事件处理方案和追责。

（二）数据安全管理员的职责主要有：

1.梳理数据安全风险，明确数据安全风险等级及其中可接受的等级；

2.建设完善数据安全管理制度；

3.对数据的分级分类进行审核；

4.负责审批数据分级分类变更申请；

5.设计数据存储方案并监督实施；

6.分派数据备份、归档任务；

7.设计数据访问权限和数据脱敏方案，并监督实施；

8.监督数据传输过程的合规性；

9.监督数据处理、使用过程的合规性；

10.监督数据、介质销毁操作的执行并记录；

11.保障灾难恢复预案的有效性，监督数据安全事件演练的实施；

12.数据安全事件的处理及整改。

（三）数据获取员的职责主要有：

1.使单位内外部数据合规、及时地进入内部信息系统；

2.实施数据分级分类。

（四）数据需求协调员的职责主要有：

1.制定数据获取管控措施和安全保障机制；

2.参与制定数据分级分类规范和标准；

3.提出数据分类定级的变更申请；

4.接收数据处理申请，并提交至数据安全管理组组长。

（五）数据介质管理员的职责主要有：

1.负责数据存储介质的物理环境保护；

2.负责数据存储介质的转换；

3.负责介质的管理、维护、检查工作，并记录操作信息；

4.负责提出介质维修、转换、销毁申请；

5.负责执行介质销毁操作；

6.做好介质的移交登记和报废登记。

（六）系统管理员的职责主要有：

1.负责提交备份申请，制定数据备份方案；

2.负责执行备份操作和测试备份数据有效性，并记录操作信息；

3.负责提交归档申请，制定数据归档方案；

4.负责执行归档操作和测试归档数据有效性，并记录操作信息；

5.负责定期核验存储数据有效性，并记录操作信息；

6.负责数据脱敏的实施；

7.负责介质维修、销毁流程前后数据处理。

附件三：数据安全事件级别定义及报告提交

事件级别	事件现象	响应时间	解决时间	数据安全事件报告要求
特别重大事件	1、会使特别重要信息系统遭受特别严重的系统损失； 2、产生特别重大的社会影响。	立即响应	30 分钟内	于故障解决次日提供数据安全事件报告，三个工作日内提供数据安全事件分析报告。应包括数据安全事件情况说明、起因、解决方案、避免同类事件方案等。
重大事件	1、会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失； 2、产生的重大的社会影响。	30 分钟内	1 小时内	于数据安全事件解决次日提供数据安全事件报告，一周内提供数据安全事件分析报告。应包括数据安全事件情况说明、起因、解决方案、避免同类事件方案等。
较大事件	1、会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失； 2、一般信息信息系统遭受特别严重的系统损失； 3、产生较大的社会影响。	1 小时内	4 小时内	于一周内提供数据安全事件分析报告。应包括数据安全事件情况说明、起因、解决方案等。
一般事件	1、会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失； 2、一般信息系统遭受严重或严重以下级别的系统损失； 3、产生一般的社会影响。	8 小时内	24 小时内	不需提供专门数据安全事件分析报告。

附件四：数据安全事件影响时限与升级上报流程

事件影响时限	特别重大事件	重大事件	较大事件	一般事件
30 分钟	各级各类教育单位安全负责人			
1 个小时	数据技术管理部门安全负责人	各级各类教育单位安全负责人		
4 小时	数据技术管理部门领导	数据技术管理部门安全负责人	各级各类教育单位安全负责人	
8 小时	数据管理协调部门领导	数据技术管理部门领导	数据技术管理部门安全负责人	
12 小时		数据管理协调部门领导	数据技术管理部门领导	
48 小时				各级各类教育单位安全负责人