2022 WEST LAKE CYBERSECURITY CONFERENCE
西湖论剑·网络安全大会

数据分类分级的实践与挑战

陈兴蜀
Chen Xingshu

四川大学网络空间安全学院 院长、教授

2022 WEST LAKE CYBERSECURITY CONFERENCE

CONTENTS 目录

2022 WEST LAKE CYBERSECURITY CONFERENCE

01

数据安全的相关法律法规

01.法律法规构建了数据安全治理体系

➢ 数据安全治理体系

01.数据安全的法律法规要求

《网络安全法》

安全防护要求

明确职责权限，完善安全监管体制

将现行有效的网络安全**监管体制法制化**，**明确**网信部门与其他相关网络**监管部门的职责分工**。

条例：第八条

完善义务和责任，加大惩处力度

对**网络运营者等主体的法律义务和责任**做了全面规定，同时**承担社会责任**等。

条例：第三章、第四章、第五章

重点保护关键信息基础设施

明确关键信息基础设施的运营者负有更多的**安全保护义务**，并配以国家安全审查、重要数据强制本地存储等法律措施，**确保关键信息基础设施的运行安全**。

条例：第三章

完善监测预警与应急处置措施

建立统一高效的网络安全**风险报告机制、情报共享机制、研判处置机制**提供了法律依据，为深化网络安全防护体系,实现全天候全方位感知网络安全态势提供了法律保障。

条例：第五章

01.数据安全的法律法规要求

➢ 《数据安全法》

安全防护要求

数据安全制度

第三章：

1、分类分级：

国家建立数据分类分级保护制度，制定重要数据目录，加强对**重要数据**的保护。关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家**核心数据**，实行更加严格的管理制度。

2、风险评估：

建立数据安全**风险评估、报告、信息共享、监测预警**机制

3、应急处理：

建立数据安全**应急处置**机制。

4、安全审查：

建立数据安全**审查制度**。

5、出口管制

可以**根据实际情况**对该国家或者地区对等采取措施。**明确**了国家**对中国数据的主权**。

数据安全保护义务

第四章：

1、管理制度：

建立健全全流程**数据安全管理制度**，**明确**重要数据处理**数据安全负责人和管理机构**。

2、风险监测：

对缺陷、漏洞等，**采取补救措施**；对数据安全事件，立即**采取处置措施**，并按规定**上报**。

3、风险评估：

定期**开展风险评估**并**上报风评报告**。

4、数据收集：

采取**合法、正当**的方式，不得窃取或者以其他非法方式获取

01.数据安全的法律法规要求

《数据安全法》

安全防护要求

数据安全保护义务

第四章：

5、数据交易

提供并**说明数据来源证据**，要**审核相关人员身份并留存记录**。

6、经营备案

数据服务**经营者**应当**取得行政许可**，**服务提供者**应当**依法取得许可**。

7、配合调查

要求依法**配合公安、安全等部门**进行犯罪调查。**境外执法机构要调取存储在中国的数据，未经批准，不得提供**。

政务数据安全与开放

第五章：

1、管理制度：

建立健全全流程**数据安全管理制度**，落实数据安全保护责任。

2、存储加工：

委托他人存储、加工或提供政务数据，当经过**严格审批，并做好监督。受托方不得擅自留存、使用、泄露或向他人提供**政务数据。

3、数据开放：

构建统一政务数据开放平台，发布数据开放目录，推动政务数据开放利用。

4、适用主体：

法律、法规授权的具有管理公共事务职能的组织。

01.数据安全的法律法规要求

《个人信息保护法》

安全防护要求

1

个人信息处理规则

1、具有**明确、合理的目的**，限于实现处理目的的**最小范围**，公开处理规则，保证信息准确，采取安全保护措施等。（第五条至九条）
2、确立以**“告知-同意”**为核心的个人信息处理一系列规则。(第十三条至十九条)

2

个人信息跨境提供规则

1、达到**规定数量**的处理者，应通过国家网信部门组织**安全评估**。(第三十八条、第四十条)
2、对 **“告知-同意” 更严格**。（第十九条）
3、经中华人民共和国主管机关**批准**。（第四十一条)

3

个人信息处理活动中
个人的权利和处理者义务

1、明确个人信息处理者的**合规管理和保障个人信息安全**等义务。(第五十一条至五十六条)
2、明确提供**基础性互联网平台服务、用户数量巨大、业务类型复杂**的个人信息处理者的义务(第五十七条)

4

个人信息保护职责的部门

1、个人信息保护**职责部门**的定义。（第六十条）

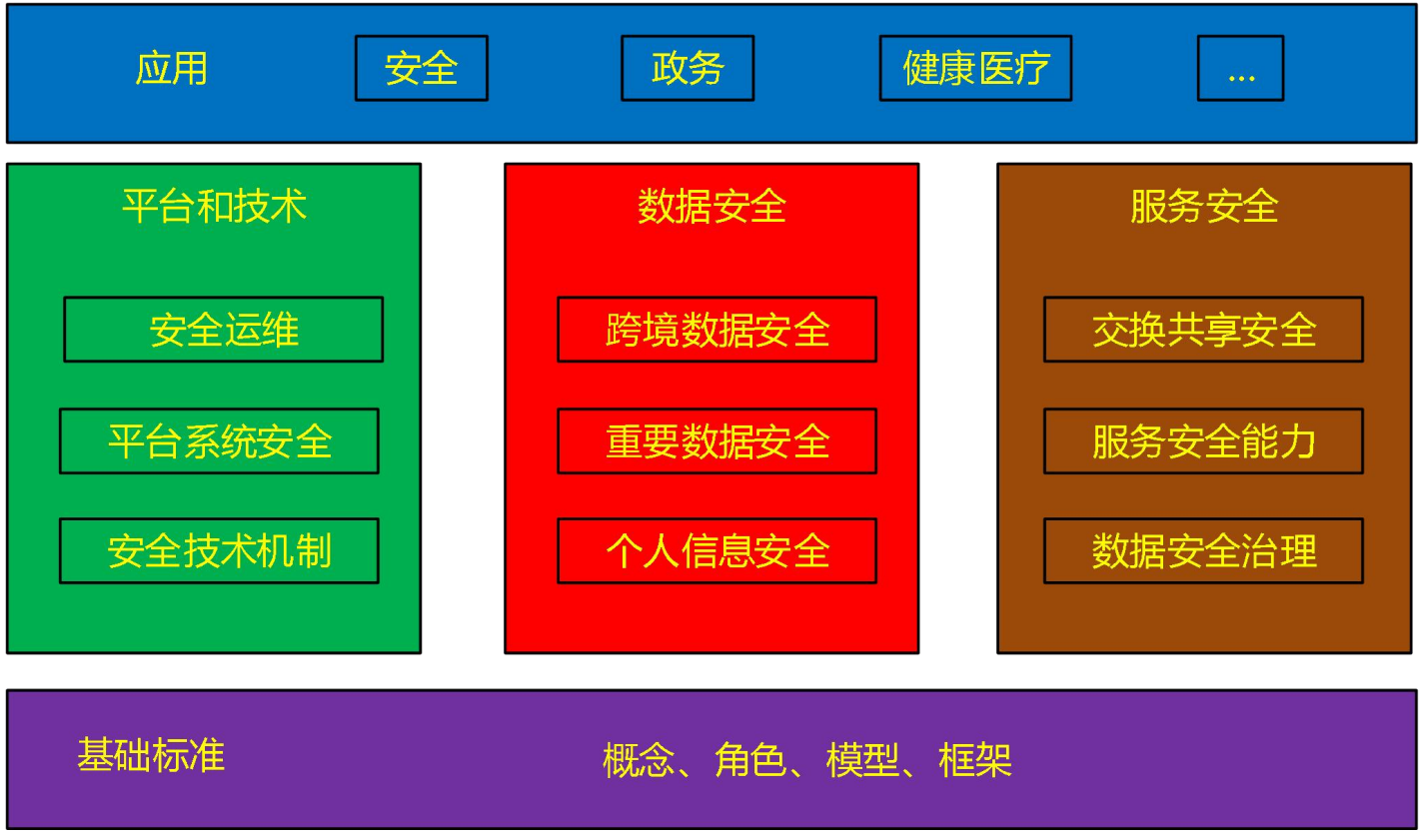
2、明确个人信息保护**部门的职责**。(第六十一条、第六十二条)

02

数据安全的实践探索

02. 数据安全标准体系

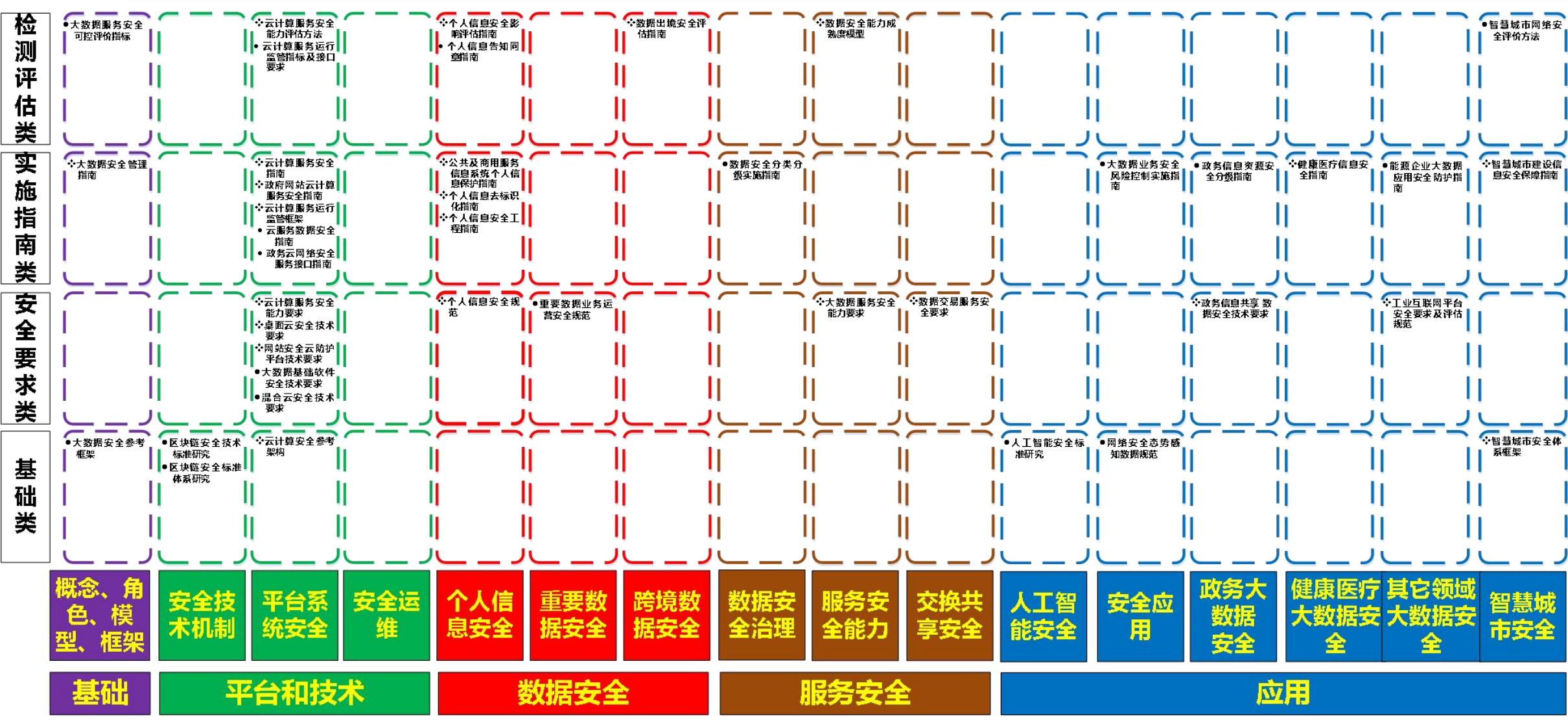
大数据安全标准体系



标准类型

- 基础类
- 安全要求类
- 实施指南类
- 检测评估类

02.大数据安全标准地图



02. GB/T 37973-2019《信息安全技术 大数据安全管理指南》

大数据安全管理要素

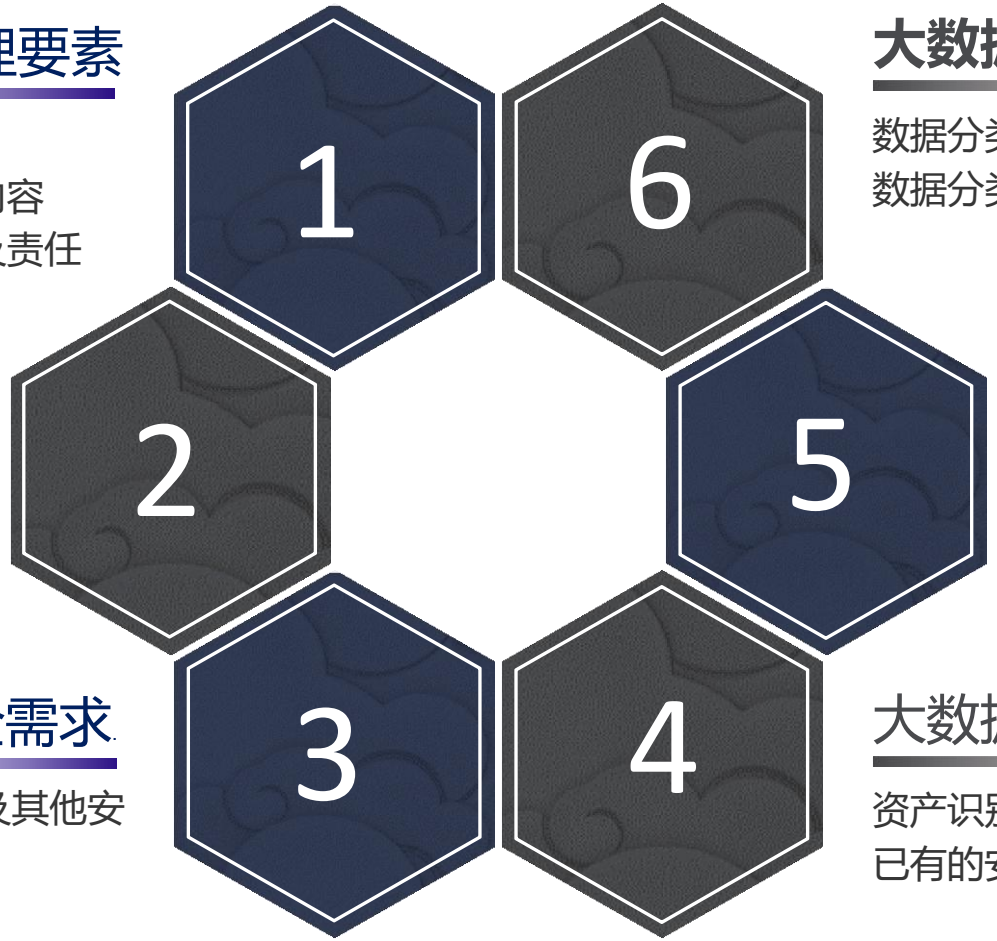
- 目标
- 主要内容
- 角色及责任

大数据安全管理原则

职责明确、安全合规、质量保障、数据最小化、任不随数据转移、最小授权、确保安全及可审计

大数据安全需求

保密性、完整性、可用性，及其他安全需求



大数据分类分级

数据分类分级流程
数据分类分级方法

大数据活动安全要求

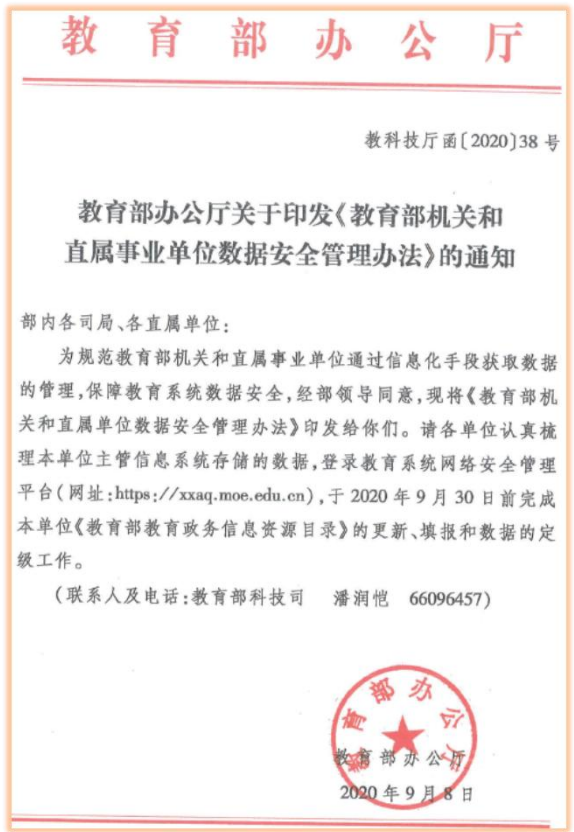
数据采集、存储、处理、分发等环节的技术和管理措施。

大数据安全风险评估

资产识别；威胁识别；脆弱性识别；已有的安全措施确认；风险分析

➢ 教育行业数据安全实践

2020年发布《教育部机关和直属事业单位数据安全管理办法》



教 育 部 办 公 厅

教科技厅函〔2020〕38号

教育部办公厅关于印发《教育部机关和直属事业单位数据安全管理办法》的通知

部内各司局、各直属单位：

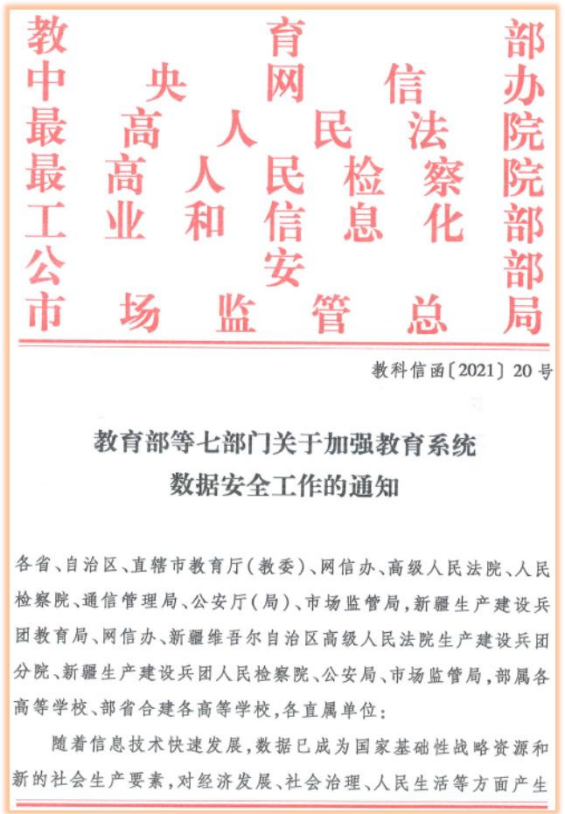
为规范教育部机关和直属事业单位通过信息化手段获取数据的管理，保障教育系统数据安全，经部领导同意，现将《教育部机关和直属单位数据安全管理办法》印发给你们。请各单位认真梳理本单位主管信息系统存储的数据，登录教育系统网络安全管理平台（网址：https://xxaq.moe.edu.cn），于2020年9月30日前完成本单位《教育部教育政务信息资源目录》的更新、填报和数据的定级工作。

（联系人及电话：教育部科技司　潘润恺　66096457）

教育部办公厅

2020年9月8日

2021年七部委联合发布《关于加强教育系统数据安全工作的通知》



部办院院部部局
信法察化总
民检息管
人民信安
高人和
央高业场
育网
教中最最工公市

教科信函〔2021〕20号

教育部等七部门关于加强教育系统数据安全工作的通知

各省、自治区、直辖市教育厅（教委）、网信办、高级人民法院、人民检察院、通信管理局、公安厅（局）、市场监管局，新疆生产建设兵团教育局、网信办、新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局、市场监管局，部属各高等学校、部省合建各高等学校，各直属单位：

随着信息技术快速发展，数据已成为国家基础性战略资源和新的社会生产要素，对经济发展、社会治理、人民生活等方面产生

➢ 《管理办法》--总体架构

总体框架
共9章38条。目录如下：
第一章 总则
第二章 工作职责
第三章 数据等级划分
第四章 数据收集的安全保障
第五章 数据存储传输的安全保障
第六章 数据处理使用的安全保障
第七章数据共享公开的安全保障
第八章 数据安全监督管理
第九章 附则

《管理办法》--六大亮点

01 明确范围

- 保护对象：个人信息和重要数据
- 数据范围：教育部直属机关在履行行政职能时，通过信息化手段获取的法定统计数据和行政记录数据

02 树立原则

- 一溯一源
- 最小够用
- 分级保护
- 安全合规

03 确定数据等级

- 公开数据
- 内部数据
- 敏感数据

04 覆盖主要的数据活动

- 数据收集
- 存储传输
- 处理使用
- 共享开放

05 突出强调100万人以上个人信息

06 提出“权限分离”

- 数据管理者
- 数据处理者
- 安全审计者

《管理办法》--三个特点

具有针对性

管理办法从教育部直属机关面临的数据安全问题出发，参考《网络安全法》等法律法规，建立保障数据安全的各项措施，重在管用，重在解决实际问题

具有全面性

管理办法比较全面和系统地确立了各个主体包括科技司、规划司、信息中心、教育部直属机关各单位的义务和责任，它确立了保障个人信息和重要数据安全的基本管理制度和技术手段

具有协调性

管理办法鼓励安全与发展并重，协调推进数据安全和使用流动，注重保护广大师生的合法权益，保障数据依法、有序、自由的流动，最终实现数据安全和数据价值最大化

《数据安全通知》--总体要求

依据

- 《中华人民共和国民法典》《中华人民共和国未成年人保护法》《中华人民共和国网络安全法》等法律法规和政策文件要求

目标

- 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。

《数据安全通知》--四个能力

- 制度建设
  1、加强数据安全统筹领导
  2、落实数据安全责任制
  3、数据等级保护制度
  4、数据安全监测通报
  5、数据主管单位和网信职能部门监督检查
- 监测预警
  1、远程检测
  2、信息共享
- 安全保障
  1、脱敏处理
  2、在线接口
  3、安全认证
  4、权限管理
- 应急处置
  1、备份恢复
  2、密码技术

《数据安全通知》--五项任务

- 一 加强数据安全统筹协调
- 二 规范数据生命周期管理
- 三 重点保障个人信息安全
- 四 加大数据安全监管力度
- 五 健全数据安全保障体系

1 明确责任主体，建立数据管理制度

2 规范数据收集、存储、使用、分发、删除等过程。

3 明确保护大规模个人信息、儿童信息、敏感个人信息。

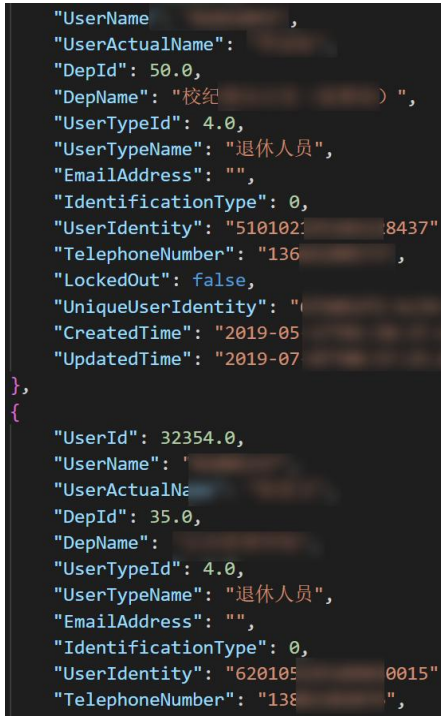
4 加强对教育市场监管，对监督部门考核，对数据安全监测。

5 完善数据安全制度，加强数据安全宣传。

→ 教育系统数据安全治理体系

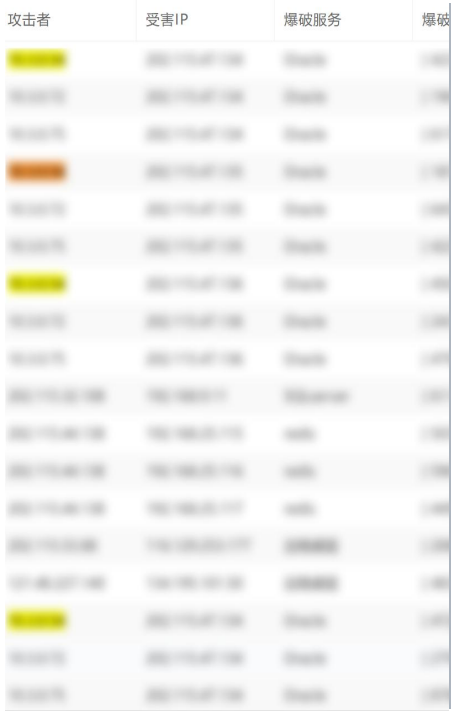
02.数据安全防护能力积累

精准定位个人信息



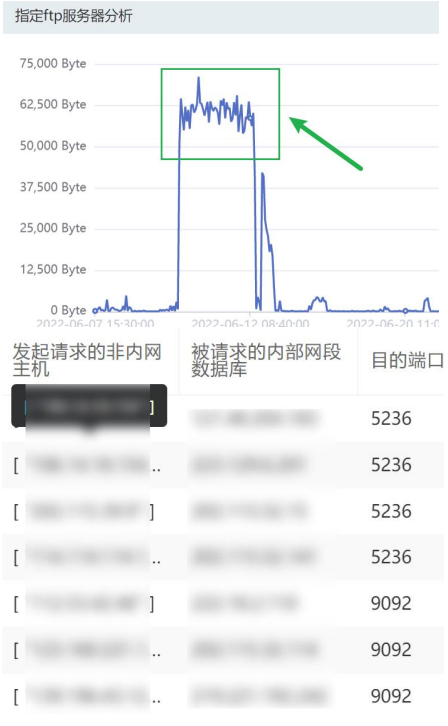
- 敏感信息明文传输的一种
- 其特点为：单个接口即暴露多个维度的个人信息，可精准定位到个人，情节更加严重。

密码爆破风险



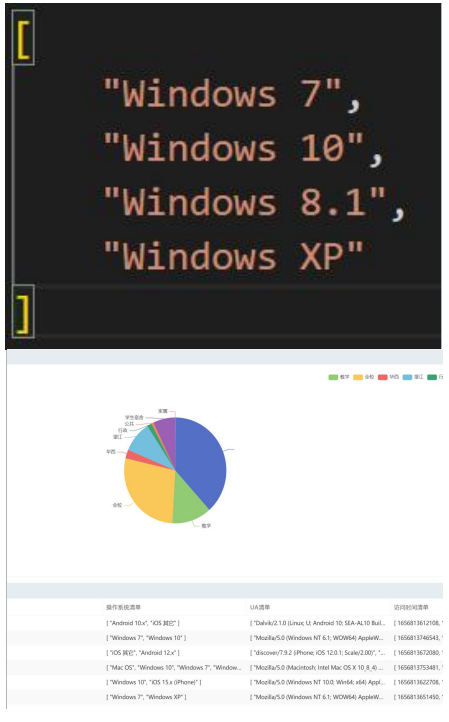
- 相比扫描行为，数据安全监测平台更关注爆破“成功”的事件。

关键服务器行为监测



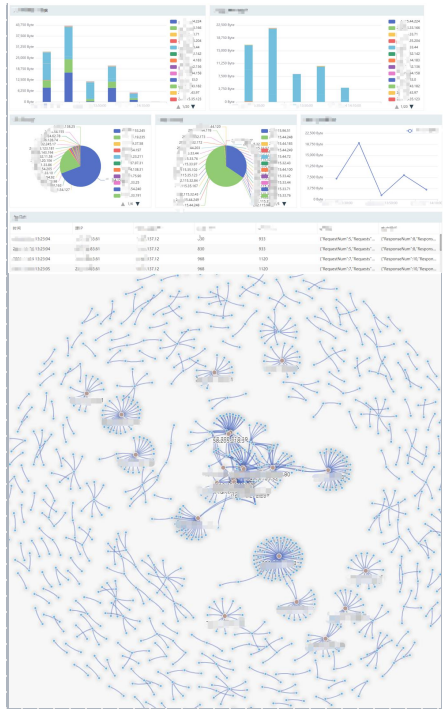
- 监测网络环境中服务器行为，自动关注流量大、波动大的服务器。
- 对内部数据库暴露到公网的情况进行重点监测。

用户违规接入



- 判断每个IP地址下某一时间段内的设备种类。
- 结合各个操作系统的使用人数，判断是否存在用户私设WiFi供他人接入内网的情况。

跨境邮件监控



- 监测邮件服务器行为，重点关注有频率有节奏的跨境邮件。

02.数据安全防护能力积累

■前期支撑工信部网安局研究形成行业数据安全管理总体技术方案，通过**建设部-省-企业三级联动**的数据安全监管技术平台，**统筹整合企业内外部**网络数据安全技术能力，实现行业数据安全风险**实时监测、溯源核查、态势感知、精准定位、快速响应、高效管理**能力

首批试点：新疆、湖南、山东、上海

其它省份会陆续扩展，各省运营商强化内部数据安全管理和上层链接，已非常必要。

建设必要性

本次专项工作所涉及的系统，**可部分满足**数据安全合规所要求的技术能力。

华数安可有效避免后期专项工作实施与数据安全合规要求两者不兼容问题。

建设内容

◆ **国家级平台**

实现全国或重点地区数据安全监测追溯、行业综合管理和全局研判分析

◆ **属地侧平台**

在省通信管理局建设国家级平台属地化支撑模块，实现属地数据安全综合管理、监测预警、追踪溯源和应急响应

◆ **企业级平台**

对上与国家级平台属地化支撑模块对接，对下分别采集IDC出口流量、城域网出口流量和企业内部大数据平台及对外业务相关系统的流量和日志数据

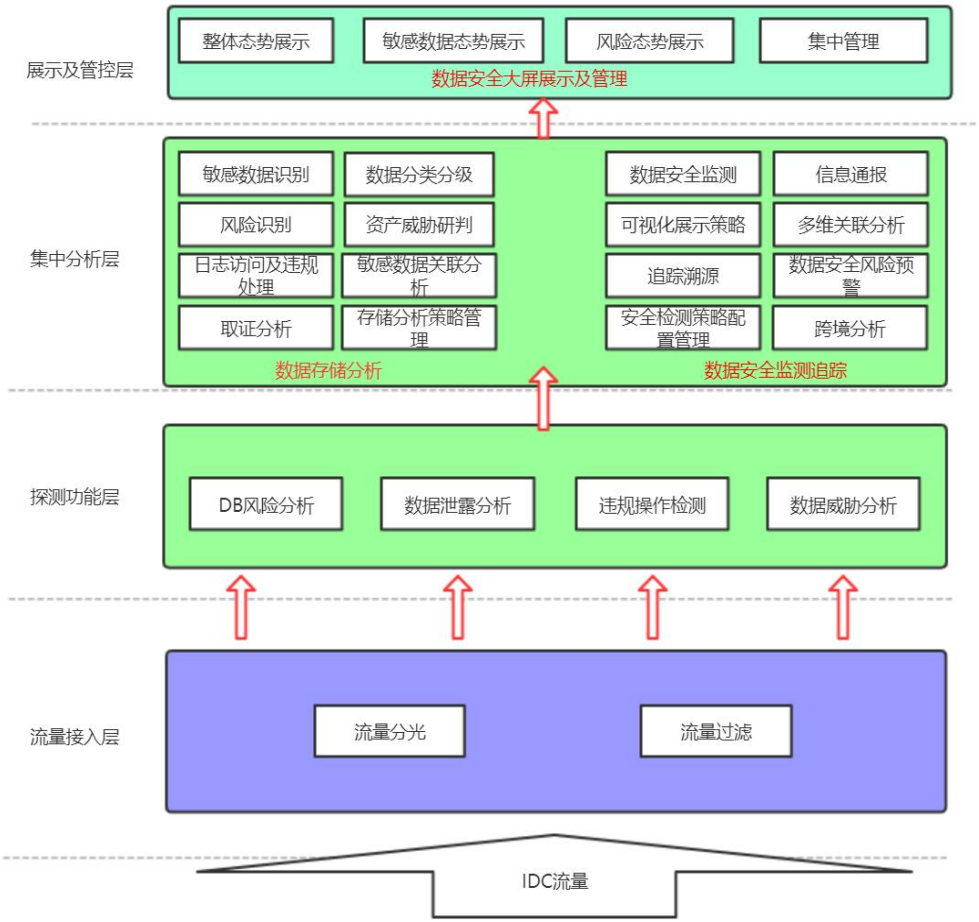
企业外部为获取企业IDC流量和城域网流量，将数据上报至属地侧平台中。

企业内部为**对企业各业务系统数据资产进行资产管理、分级分类管理、对外开放管理、安全预警、安全风险追溯、风险上报管理，以及大数据分析等。**

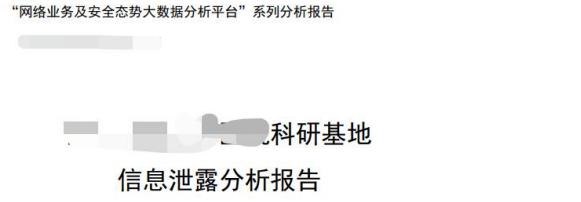
2020年工业互联网创新发展工程项目《数据安全风险监测追溯与综合管理平台》

02.数据安全防护能力积累-某省试点案例

- 通过信安系统升级方式实现前端流量采集后，通过**新建数据安全管理系统**实现后端数据安全管理；
- 验证后端分析系统的功能完善性，在数据安全**监测巡查**、**关联分析**、**追踪溯源**、**风险预警**、**信息通报**、与属地其他**系统联动**等方面形成技术能力，支撑数据安全监管工作实现“技管结合”。



02.数据安全防护能力积累-典型案例



发现某**内部测试环境公网暴露**，且该平台账号密码明文传输，可以使用暴露的账号密码登录正式系统。

通过对接口的行为分析，无异常行为，可知目前该接口尚未被恶意利用，未产生巨大损失。

2021 年 10 月 17 日起，通过“四川大学数据安全管理平台”对于校园网 API 接口敏感访问日志进行分析，检测到 有敏感数据明文传输的现象，经查定位到该域名隶属与 该二级域名隶属于 以下简称科研管理基地。

序号	请求时间	请求URI	域名	服务端IP	请求方IP	敏感标签	敏感字段
1	2021-10-18...					["密码"]	查询条件
2	2021-10-18...					["身份证","密码","电话号...	查询条件
3	2021-10-18...					["身份证","密码","电话号...	查询条件
4	2021-10-18...					["身份证","密码","电话号...	查询条件
5	2021-10-18...					["身份证","密码","电话号...	查询条件
6	2021-10-18...					["身份证","密码","电话号...	查询条件
7	2021-10-18...					["身份证","密码","电话号...	查询条件
8	2021-10-18...					["密码","电话号码"]	查询条件
9	2021-10-18...					["密码","电话号码"]	查询条件
10	2021-10-18...					["密码","电话号码"]	查询条件
11	2021-10-18...					["密码","电话号码"]	查询条件
12	2021-10-18...					["密码","电话号码"]	查询条件
13	2021-10-15...					["密码"]	查询条件
14	2021-10-14...					["密码"]	查询条件
15	2021-10-12...					["密码"]	查询条件
16	2021-10-12...					["密码","电话号码"]	查询条件
17	2021-10-11...					["密码"]	查询条件

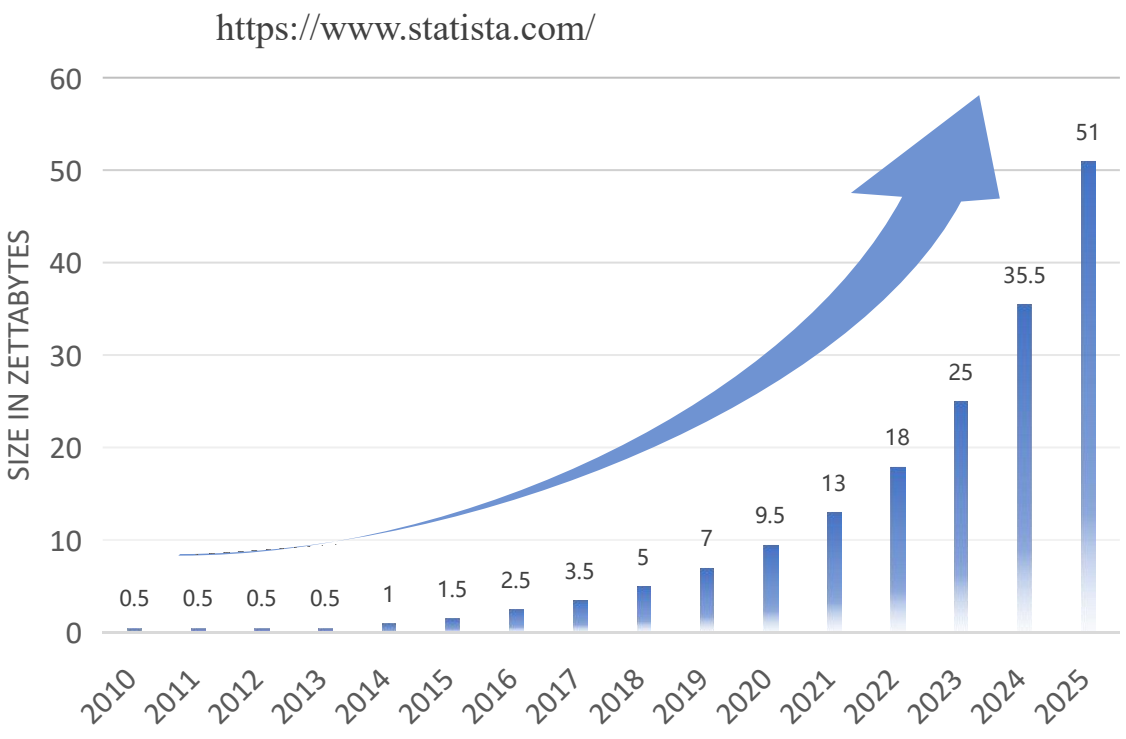
图表 1 四川大学数据安全综合管理平台-敏感接口访问日志

图表 3 注册接口日志和对应界面

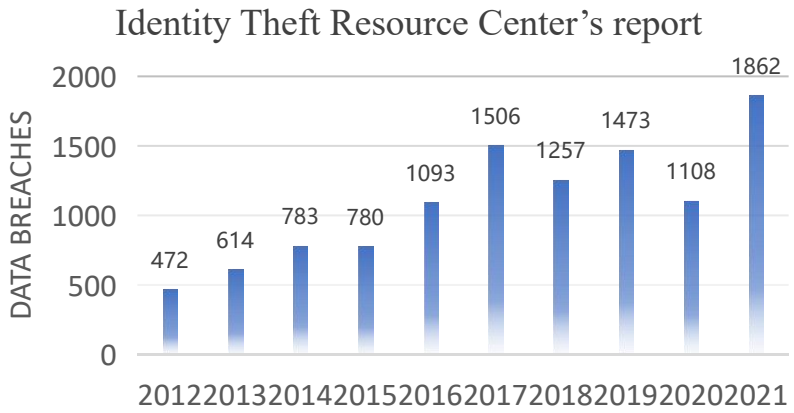
03

数据分类分级的实践与挑战

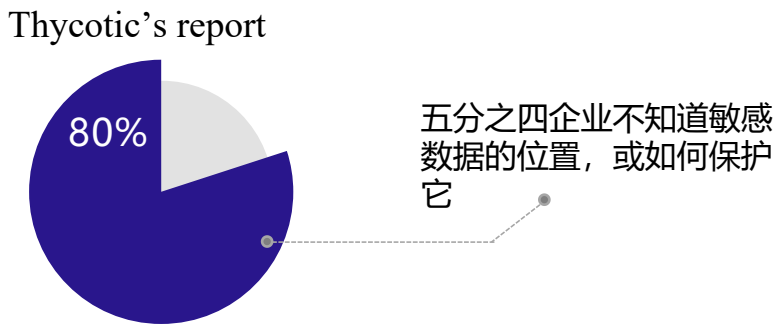
03.数据分类分级的必要性



全球数据量飞速增长



数据泄露事件频发



- 组织有哪些数据类型，数据如何分布？
- 什么是敏感数据，敏感数据在哪里？
- 数据处理是否满足法律法规要求？

03.数据分类分级的重要性

安全策略制定

- 数据安全策略
- 用户安全策略
- 安全分析策略

数据查询管理

- 明确数据位置
- 明确数据责任主体
- 安全地更改和销毁数据
- 数据权限管理

数据安全合规

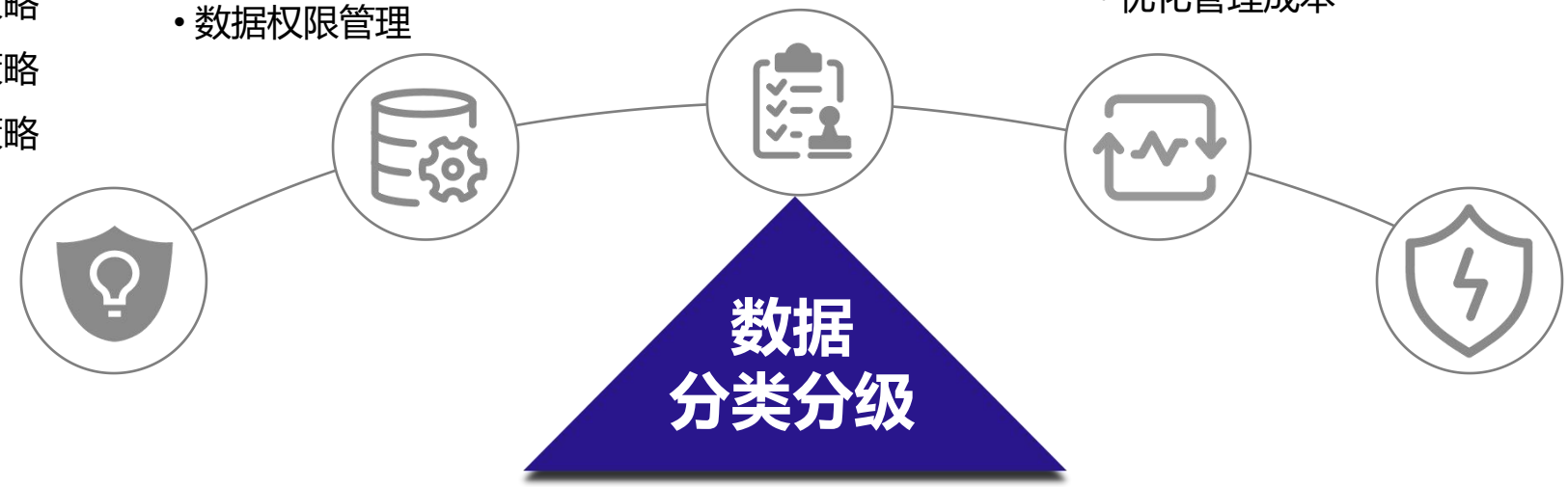
- 不同的数据类型、数据级别采取不同的措施
- 识别法规管控的数据

高效利用数据

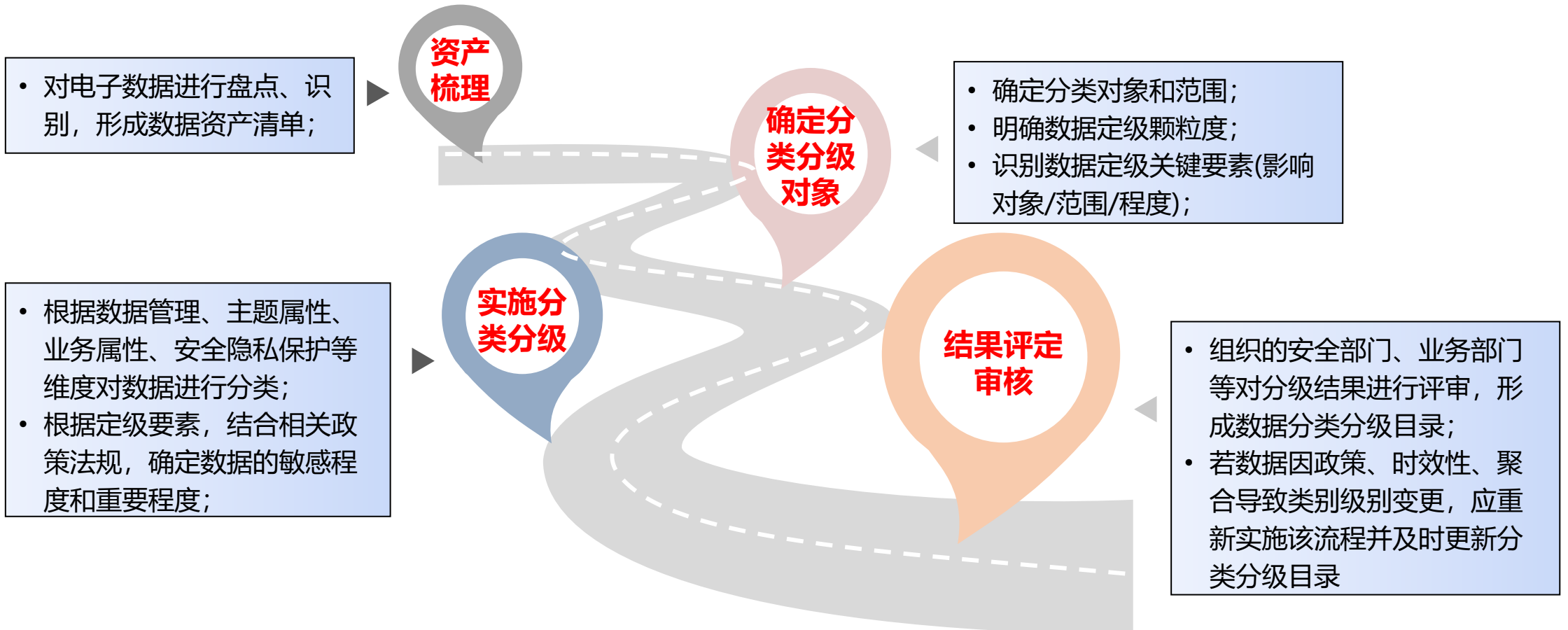
- 最大化共享数据
- 有效访问受保护的数据
- 优化管理成本

降低数据风险

- 限制敏感数据访问
- 减少敏感数据攻击面



03.数据分类分级流程


资产梳理
• 对电子数据进行盘点、识别，形成数据资产清单；
确定分类分级对象
• 确定分类对象和范围；
• 明确数据定级颗粒度；
• 识别数据定级关键要素(影响对象/范围/程度)；
实施分类分级
• 根据数据管理、主题属性、业务属性、安全隐私保护等维度对数据进行分类；
• 根据定级要素，结合相关政策法规，确定数据的敏感程度和重要程度；
结果评定审核
• 组织的安全部门、业务部门等对分级结果进行评审，形成数据分类分级目录；
• 若数据因政策、时效性、聚合导致类别级别变更，应重新实施该流程并及时更新分类分级目录

03.数据分类分级教育行业实践

系统名称	数据子集分类			相关表名		
一网通办平台	学校概况数据子集	学校基本数据类	学校基本数据子类	organizations 机构表		
			机构数据类	departments 部门表		
	教职工管理数据子集	教职工基本数据类	教职工基本数据子类	teachers 教师表		
			配偶数据子类	emergency_contacts 紧急联络人		
			家庭其他成员数据子类	family 家庭信息表		
			学习简历数据子类	trian_experience培训经历表		
			工作简历数据子类	work_experience工作经历表		
			奖励数据子类			
			惩处数据子类			
			政治面貌数据子类			
		教职工资质数据类	学历学位数据子类	edu_experience 学历信息		
			岗位证书数据子类	credentials证书信息表		
			教师资格证书数据子类	titles 职称信息表		
			特级教师数据子类			
		岗位职务数据类	行政、党派职务数据子类			
			专业技术职务数据子类			
			管理工作数据子类	OA授权项目表	OA授权项目关联表	OA授权部门关联
		特岗教师聘任数据类				
		校内异动数据类	学校内部机构调动数据子类			
			编制异动数据子类			
			离岗数据子类			
			病休数据子类			
		离职数据类	离退休数据子类			
			工作返聘数据子类			
			离职数据子类			
		工资、保险福利数据类	工资变动子类	工资单表	薪资岗位表	薪资等级表
			工资结构子类	工资单类目关联分组表	工资单类目关联表	工资单用户条目
			保险福利子类			
		教职工考核数据类	教师业务考评数据子类			
			组织考察(考核)数据子类			
			干部工作考核数据子类			
		教案数据类				

4

5

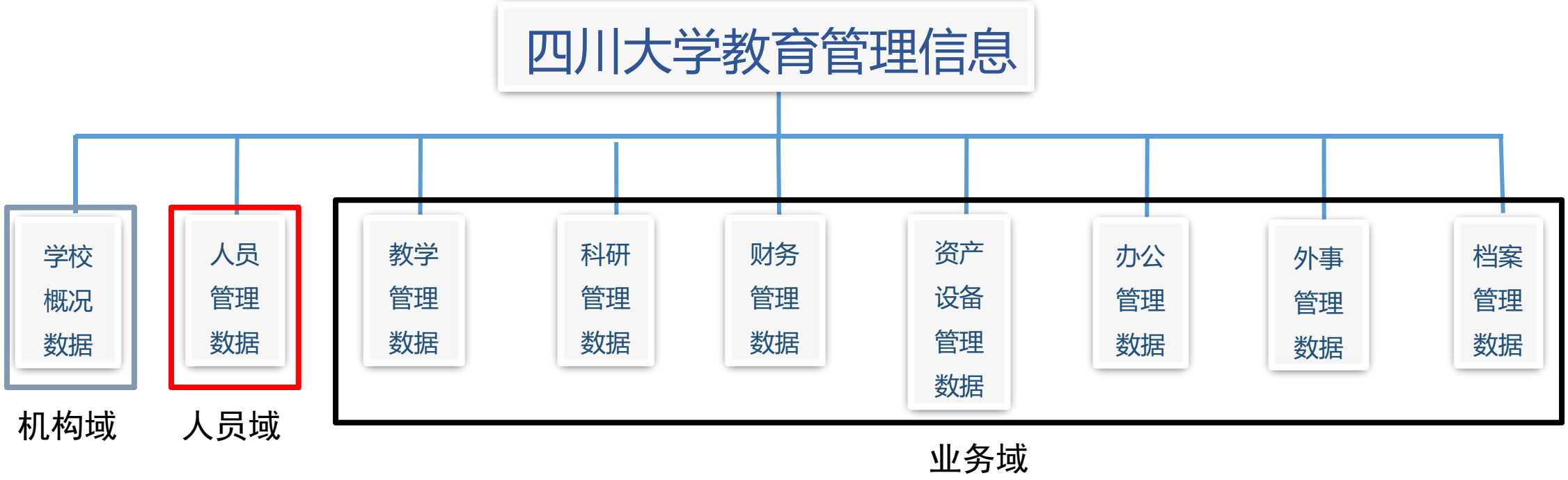
在成都两所界外国语学、四川大学谈、回收调同教育层次

03.教育数据分类方法

分类按**业务条线**分

好处：按业务条线分能够**明确不同业务的管理主体**，进而确定数据管理的基本责任主体，遵循《管理办法中》“谁主管，谁负责”的准则）

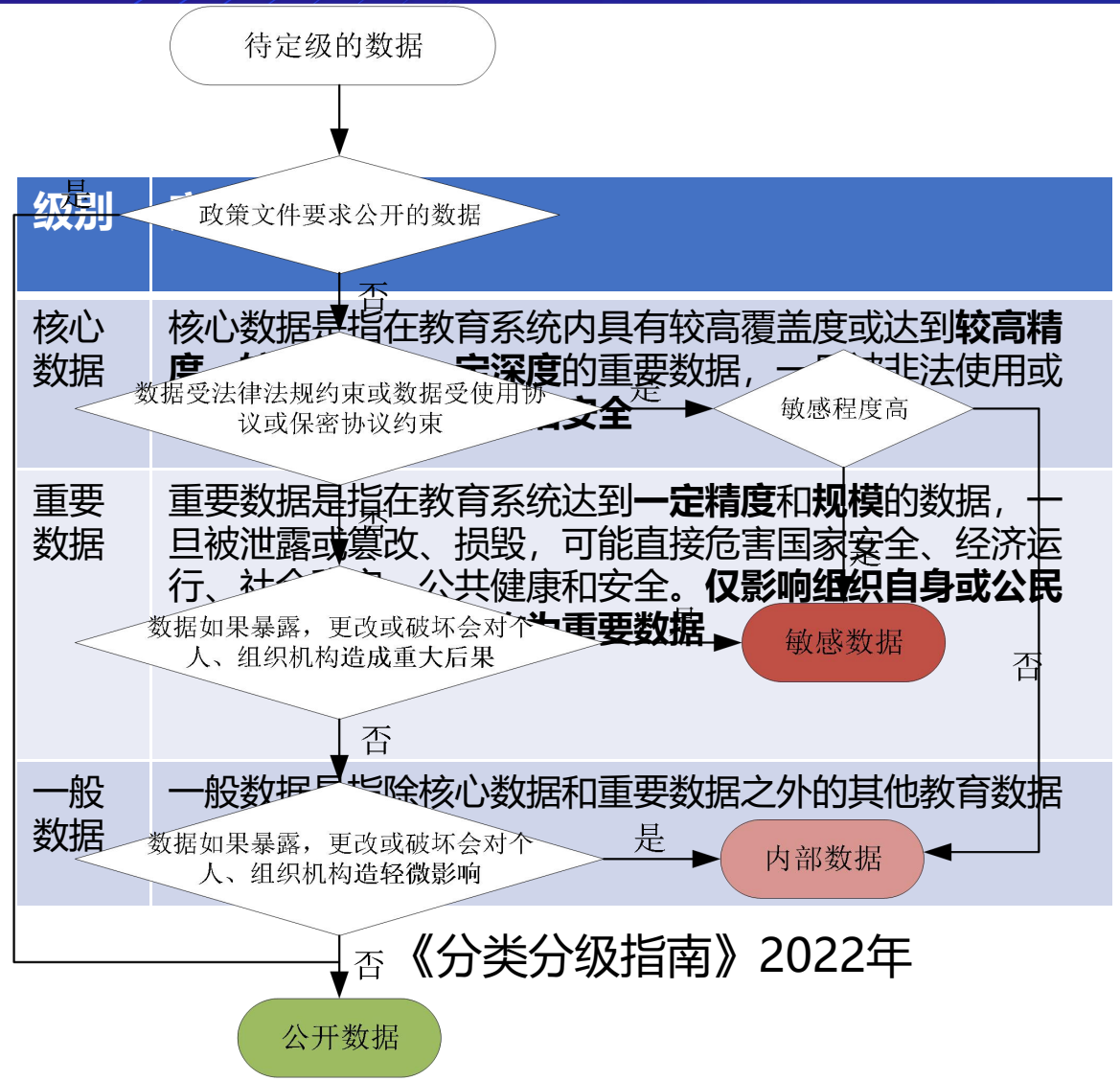
分为：**机构域数据**（单位基本数据、单位领导小组数据等）、**人员域数据**（学生信息、家长信息、教职工信息等）、**业务域数据**（财务管理、办公管理、资产管理、档案管理等）。



03.教育数据分类方法

级别	定义
敏感数据	指一旦遭泄露或篡改，可能对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成严重损害的数据
内部数据	是指不予公开，但可在一定范围内共享的数据，包括教育部直属机关间共享、教育系统间共享、政府部门间共享和特定对象间共享的数据。依职能收集并为公共服务、管理决策提供支撑的数据，如教师、学生、家长个人基本信息等，均属于内部数据
公开数据	指《教育部政府信息公开目录》中主动公开和依申请公开的政务数据和可在互联网公开的业务数据

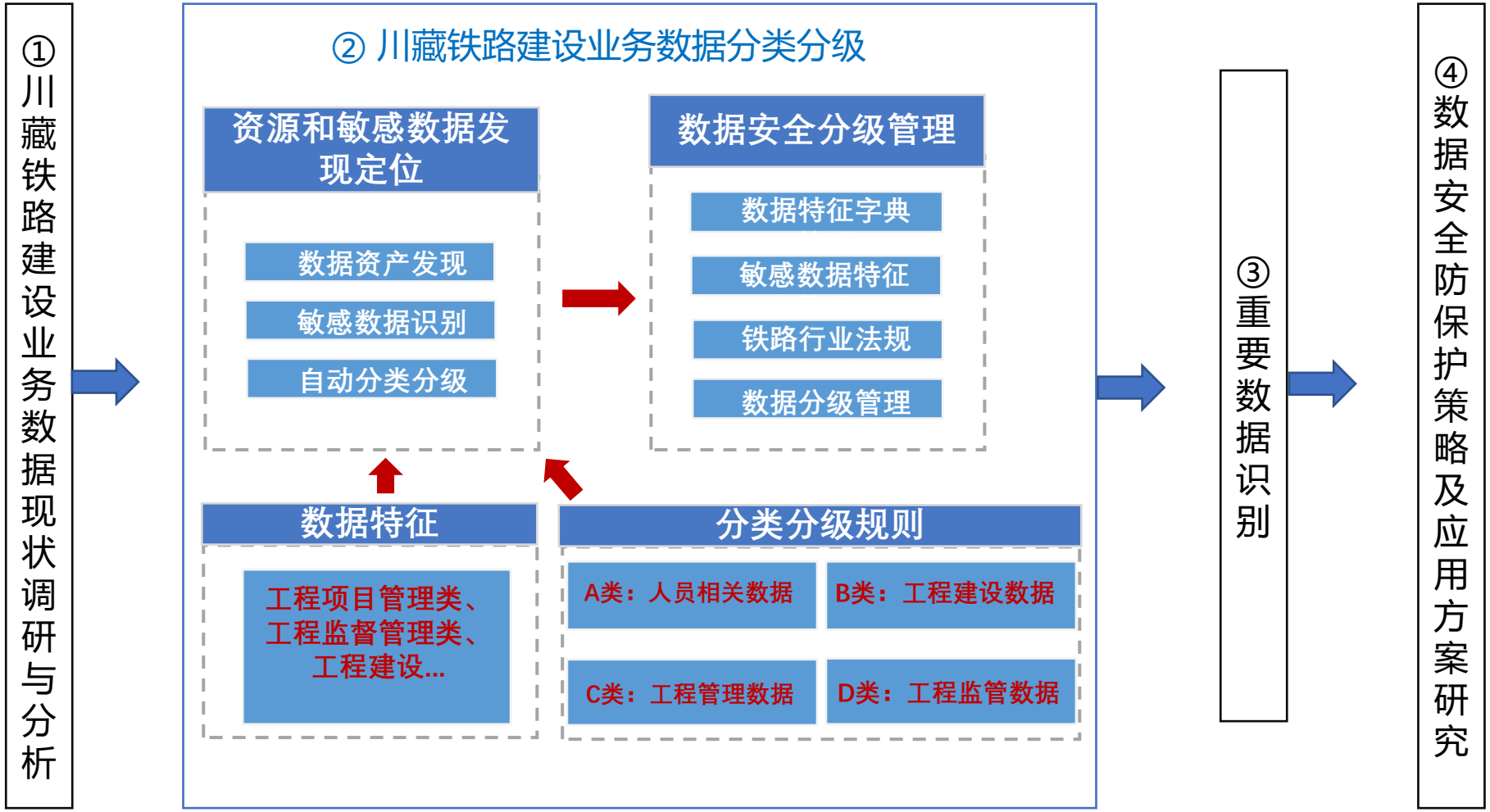
《管理办法》2020年



级别	
核心数据	核心数据是指在教育系统内具有较高覆盖度或达到**较高精度**、**较高深度**的重要数据，一旦被非法使用或**共享**，可影响**政治安全**、**国土安全**、**军事安全**、**经济安全**、**文化安全**、**科技安全**、**网络安全**以及**生物安全**
重要数据	重要数据是指在教育系统达到**一定精度**和**规模**的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。**仅影响组织自身或公民**的数据通常不作为**重要数据**
一般数据	一般数据是指除核心数据和重要数据之外的其他教育数据

《分类分级指南》2022年

03.铁路行业数据分类分级研究



03.铁路行业数据安全防护策略及应用方案研究

调研分析相关的政策法律法规、文献、案例，**为川藏铁路建设期数据安全保护提供支撑。**

调研

多方研讨

与相关单位探讨交流，**研究数据使用场景及其风险。**

以数据安全管理办法基本要素、管理制度、技术措施为支撑，**制定非涉密数据安全管理办法与实施方案。**

编写办法

制定策略

基于通用要求，结合管理要求与技术要求，**制定以全数据生命周期为主的安全防护策略。**

面临的挑战

合规性遵从

法律法规的不断发布，迫使组织分类时需考虑合规性。如：存储用户的哪些个人数据？它们分布在哪些系统中？是否满足立即响应客户的数据访问权、更新权和删除权等权利？

数据体量大

大数据技术的发展，组织积累了海量的数据资产，业务系统复杂，海量数据梳理效率差、准确率低

技术手段缺乏

现有的数据分类分级产品依赖于人工制定大量的识别规则与分类分级规则，导致成本高，更新慢等问题普遍存在

人员安全意识薄弱
制度规范缺乏

人员缺乏对数据隐私和安全的整体认知；在数据分类分级实施流程上缺乏策略文件提供清晰的具体指导

最佳实践经验不足

国标/行标有待完善、健全，各行业、各地区分类分级标准不同，处于摸索阶段，缺乏分类分级最佳实践经验

03.挑战与展望

➢ 解决方案

1

明确法律法规，确保合规性

数据分类分级与监管和合规使用相关。收集汇总组织所需遵循的内部合规性政策、标准及法律法规等信息，分析个人信息保护要点，建立个人数据关联图谱，明确个人数据的分布热图，快速响应合规要求

2

确定总体目标，规划先行，分步实施

数据分类分级不可能一蹴而就，需要遵循一定的方法论，结合组织业务，进行妥善规划并分步建设。首先在一个较小业务范围内，对分类分级方案进行验证，能力优化，发现新需求，基于验证结果规划后续能力演进阶段

3

“人工+智能”实施分类分级

正确的数据分类分级离不开人工的干预。利用数据标签技术结合预定义参数和规则，创建机器学习任务，建立知识算法，用于大规模数据自动分类分级。

4

组织建设隐私保护和数据安全文化

对数据安全管理离不开人员的组织与实施，组织体系是数据安全保护工作最重要的部分，从意识-意愿-认知-能力四个方面逐步培训固化人员的安全合规意识

2022 WEST LAKE
CYBERSECURITY
CONFERENCE

谢 谢

THANK U