上海科技大学智能决策系统
资源访问权限设置暂行办法

综合办公室、图书信息中心

2023 年 2 月 8 日

目录

学校智能决策系统是在智能化校园已建立的各类业务系统基础上，从学校和院所部门的决策需求为出发点，围绕学校教学、科研、学生培养、管理等活动，全面汇聚各个业务系统的多维度数据，通过综合仪表盘和多层关联深钻的方式，以问题为驱动、用数据作为支撑，提供对学校各方面情况的深度数据融汇、智能关联、多维分析、可视化展示，辅助支持学校在教学、科研、管理效能等方面的决策。

系统从 2018 年开始建设，截止到 2022 年底，经历了四期建设，目前内容覆盖十三大主题——综合校情、科研活动、本科生招生、本科生培养、研究生招生、研究生培养、学生行为、资产、人事、信息化、院所画像、教授个人画像、学生个人画像，2529 个分场景。未来将建立交互式个性化融汇化分析功能和灵活配置扩展功能，全面支持校情感知、行为分析、智能决策。

智能决策系统涉及学校各业务环节的细节数据，为保护学校数据资产安全、保护学校内部数据和个人隐私数据不被泄漏和违规使用，应建立合理的资源访问权限控制架构。因此，根据促进工作、便利使用、安全可溯、保护隐私的原则，对学校行为分析与智能决策系统的

各类资源做出以下划分，对各类资源访问权限做出设置。

一、可访问内容

主题：指针对学校各业务板块划分的分析场景的合集，以主题页面形式呈现，包括目前已有的综合校情、科研活动、本科生招生、本科生培养、研究生招生、研究生培养、学生行为、资产、人事、信息化、院所画像、教授个人画像、学生个人画像以及未来的其他业务主题和融汇主题。

主场景：指默认体现在主题页面中的针对该主题中特定业务环节的分析模块（分析图表）。

关联场景：指通过主场景关联延展出的其他场景，默认不显示在主题页面中，通过点击关联按钮展现。

下钻分析场景：指通过主场景或关联场景点击进入、跟该场景相关的更明细的分析场景。下钻分析场景从分析内容的专门程度上分为公共下钻分析场景和专门下钻分析场景。

数据：指为各类分析场景提供分析支撑的各类业务数据。

功能：指系统专门管理人员进行数据抽取、数据同步、数据清洗、系统设置、参数配置、权限控制等后台的操作。

二、访问角色权限

“角色”指根据工作需要和管理职责，对不同业务条线或其中针对具体业务环节具有相应业务职责或关注要求的一类用户的集合，具有访问与这类用户关联的资源的能力。系统中角色及其资源访问权限根据“工作必要则看、非工作必要则关”，充分保护个人隐私数据的原则，按以下规则设置：

校领导：所有主题、主场景、关联场景、下钻场景、下钻明细场景以及所有数据。

部处领导：（1）学校综合校情主题及其主场景、关联场景、下钻场景、下钻明细场景及明细数据（不包含个人画像数据）；（2）自己部处相关主题的主场景、关联场景、下钻场景、下钻明细场景及该主题内所有数据（不包含个人画像数据）；（3）其他经学校专门授权的主题、主场景、关联场景、下钻场景、下钻明细场景及相关数据。

院所领导：（1）学校综合校情主题及其主场景、关联场景、下钻场景、下钻明细场景及所有数据（不包含个人画像数据）；（2）学校科研活动、本科生招生、本科生培养、研究生招生、研究生培养、学生行为、资产、人事、信息化九个主题及其主场景；（3）有院所主题的——本院所主题及其主场景、关联场景、下钻场景、下钻明细场景及所有数据（不包含个人画像数据）；（4）没有院所主题的可以在（2）所包含的主题中查看本院所的关联场景、下钻场景、下钻明细场景及所有数据（不包含个人画像数据）；（5）其他经学校专门授权的主题、主场景、关联场景、下钻场景、下钻明细场景及所有数据。

业务主管：（1）学校综合校情主题的主场景；（2）所在责任部门主题的主场景；（3）所在责任部门自己所负责的主场景、关联场景、下钻场景、下钻明细场景及所有数据（不包含个人画像数据）；（4）所在责任部门的经专门授权的其他主场景；（5）其他经学校专

门授权的主题、主场景、关联场景、下钻场景、下钻明细场景及相关数据。

教师和导师：（1）学校综合校情主题的主场景；（2）所在院所主题的综合院情主场景；（3）本人的教授个人画像主题，包括主场景、关联场景、下钻场景、下钻明细场景及所有数据；（4）自己作为导师（包括作为本科生导师组成员）所负责学生的学生个人画像主题，包括主场景、关联场景、下钻场景、下钻明细场景及所有数据，一般不包含其他学生的数据。

学生：本人的学生个人画像主题，包括主场景、关联场景、下钻场景、下钻明细场景及所有数据。

三、数据下载权限

系统为方便决策应用设置了多种类别的数据下载功能，但需要对数据下载严格管理：

（1）学校有权根据需要封闭特定数据的下载权限；

（2）在前述条件下，所有用户只能下载自己授权范围的数据；

（3）所有数据下载行为（包括校领导的下载行为）将计入系统日志（谁、什么时间、什么场景、什么形式、下载什么数据）；

（4）系统区分全局数据（有关场景的全部年份、范围、项目或人员的数据，例如学校大型仪器总表、全体特聘教授表等）、局部数据（有关场景的部分年份、范围、项目或人员的数据，例如物质学院大型仪器表、信息学院全体学生表等）、具体数据（有关场景的个别年份、具体细分范围、具体细分项目或人员的数据，例如生命学院2021年入学学生表、创管学院2021年科研项目表等）；

（5）所有下载全局数据的请求将接受再次权限检查，提示下载行为将记录到系统日志，并在当日以系统警示方式提醒系统管理员；所有下载局部数据和具体数据的请求将提示下载行为会被记录到系统日志；如果同一用户在24小时内连续下载不同的局部数据三次及

以上，系统在当日以系统警示方式提醒系统管理员。

四、权限设置流程

角色分配：采用前置机制，所有用户事先被分配具体角色；属于同一类型的用户被分配相同角色；如果一个用户具有多种角色，采用访问权限更高的角色；有并列访问需求的用户可分配并列的多种角色。未分配角色的用户不能访问系统中的任何资源。

角色检验：系统通过 Egate 或域名(bi.shanghaitech.edu.cn）进入智能决策系统，用户通过统一身份认证登录后自动转换为系统用户角色；用户进入相应场景（例如关联场景、下钻场景和数据展示）时将动态进行角色检验；如果不具备权限，友好提示后引导用户返回上层场景；在数据下载时，如果下载全局数据，系统将再次检查用户权限。

角色设置流程：

（1）系统建立用户角色匹配表，优先通过统一身份认证平台本身的角色类别进行常规的角色匹配，然后由智能决策系统管理员按照下面流程进行角色匹配。

（2）通过角色配置批准单及其审批流程进行进一步的角色配置，角色配置批准单说明具体用户的角色类别，如果是责任中层干部和责任主管，还需要说明其分管业务类别。

（3）校领导角色和中层干部角色配置单由综合办公室主任和图书信息中心主任审批后生效，责任中层干部、责任主管和其他主管的角色配置批准单由所在院所部门负责人和图书信息中心主任共同签署后生效。

（4）任何用户的角色变化时，由（3）所规定的部门负责人以书面“用户角色变更单”通知图书信息中心责任管理人进行调整。

（5）校领导角色和中层干部角色配置批准单每年核实一次，责任中层干部、主管和责任主管角色配置批准单每半年核实一次，未经

核实的用户将暂停使用权限。

（6）角色配置属于系统最高权限，仅限系统根管理员。