指标访问权限控制功能开发说明

相关实体

数据安全级别（security_level）

安全级别代码使用数字编码，码值越大表示安全级别越高。目前定义为：

- 00 - 公开
- 01 - 内部
- 02 - 保密
- 03 - 绝密

业务部门（busi_department）

定义机构（及用户）所在的业务部门。其中的“是否负责系统维护”（is_admin_dept）属性定义了该部门是否是指标系统维护部门。

用户角色（user_role）

定义了用户所拥有的角色。其中的安全级别代码（sec_level_cd）属性决定了该角色能够访问的指标的最高安全级别。

指标（metric）

定义了指标的属性。其中的默认安全级别（default_sec_level）属性定义了该指标的安全级别。

指标及指标目录的访问控制

非指标系统维护部门用户的指标访问

指标及目录的可见性

用户对指标及目录的可见性由两个方面决定，

1. 用户所具备的安全级别
   - 用户所具备的安全级别由用户所拥有的所有角色中，安全级别最高的角色所决定。
   - 用户能够访问（可见）的指标的安全级别，必须低于或等于用户通过角色所获得的安全级别。
2. 用户所在的部门
   - 指标和指标目录具备部门属性，表示该指标或指标目录所属的部门。
   - 如果部门属性为空（Null），表示该指标或指标目录对所有用户开放，即属于“公共”指标体系。
   - 对用户可见的指标及指标目录范围包括：
     a. 指标或指标目录的部门属性为空值
     b. 指标或指标目录的部门属性与该用户所属机构的部门属性相同

指标维护和审核

非指标系统维护部门的用户，只能维护和审批本部门的指标及指标目录，即指标和指标目录的部门属性与用户所在机构的部门属性相同。

指标系统维护部门用户的指标访问

指标及目录的可见性

参见非指标系统维护部门用户的指标可见性说明。

指标维护和审核

指标系统维护部门的用户，既可以维护和审核“公共”指标及目录，也可以维护本部门私有的指标和目录。

指标数据访问控制

根据对指标不同维度和粒度定义的数据安全级别，实现对同一指标不同部分数据的安全访问控制。待补充。

Last updated 2020-08-27 15:11:02 +0800