附录 5：CARSI 资源共享服务身份提供者 IdP 管理标准

1. 定义和术语

https://www.carsi.edu.cn 网站上公布的最新版本“CARSI 资源共享服务政策”的第一部分“定义和术语”适用于本文件。

2. 介绍

CARSI 资源共享服务（即 CARSI 身份联盟）政策要求，如果联盟成员是用户身份所属机构，它必须保证每一个部署的 IdP 遵守本身份提供者 IdP 管理标准中定义的所有规则。

3. 身份提供者 IdP 规则

1) 身份所属机构必须在它的 IdP 中收集或者生成联盟指定的核心属性；
2) 在获得用户许可的前提下，身份所属机构可以只从 IdP 向 SP 提供用户身份属性信息；
3) 身份所属机构必须保证 IdP 所提供用户信息的准确性。特别是：
   - 身份所属机构必须及时撤销不再具有联盟资源访问权限的用户信息，或者至少 IdP 不再向其他 SP 发送关于该用户的属性信息；
   - 身份所属机构必须保证唯一的、永久的用户属性不会被在放弃使用的 24 个月之内分配给其他用户重复使用；
   - 当用户状态或者其他以属性形式描述的用户信息发生改变时，相关属性必须在一个月之内进行修改。
4) 身份所属机构必须保证用户数据安全。
5) 身份所属机构应该告诉用户他们的身份属性将提供给谁以及如何安全可靠地管理他们的身份信息；
6) 身份所属机构必须确保 IdP 按照联盟要求保留至少 6 个月日志信息，主要包括每个用户和每个认证会话的关联信息。
7) 身份所属机构在帮助联盟运行团队或其他联盟成员排查故障时应将 IdP 的使用和日志信息预先进行匿名化处理，提供的统计数据是聚合过的或者匿名化处理过的。
8) 用户为他们的行为或者疏忽负责，包括遵守任何许可或者协议，遵守身份所属机构或者服务提供机构的制定的政策。

4. 修订

CARSI 资源共享服务运行团队有权不定期修订此文件。任何此类修订需要获得 CARSI 指导委员会的认可，对所有联盟成员具有约束力。CARSI 资源共享服务运行团队将本文件最新版本发布在 CARSI 资源共享服务官方网站
https://www.carsi.edu.cn/docs/idp_management_standard_zh.pdf。