附录 3：CARSI 资源共享服务数据保护要求

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”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，如果联盟成员是服务提供者 SP，每一个 SP 在部署资源访问权限时都必须保证遵守本数据保护要求中定义的属性处理原则。

这一规定同时包含在 CARSI 资源共享服务服务提供者 SP 管理标准中。

3. 属性处理原则

服务提供机构同意并保证它的所有服务提供者 SP 遵守如下原则：

1) 【合法合规】根据中国相关法律法规处理属性；
2) 【数据最小化】减少从身份所属机构获得的属性，只保证服务所需足够的、相关的、必须的属性，尽可能减少属性使用；
3) 【目标限制】只在以下情况下使用用户属性，所有用户属性的使用和获得需征得用户本人或身份所属机构同意：
   - 服务提供者 SP 授权用户访问所提供的服务；
   - 为了便于身份所属机构追溯用户而记录和保留的用户访问信息；
   - 提供个性化用户接口；
   - 为用户提供支持；
   - 为了解服务部署和/或身份所属机构同意的其他目的而生成的使用统计。
4) 【其他目的】不会因为任何其他目的来处理用户属性（比如，出售属性或者出售个性化信息如检索历史、商业通信等）。若服务提供者 SP 想要以其他方式使用属性，必须征得每一个用户的同意，或者和身份所属机构签署协议，由身份所属机构负责通知他们的用户；
5) 【数据保留】每完成一次根据用户属性提供服务的过程，SP 将删除或者匿名化所有属性；
6) 【第三方】不会将属性传递给第三方（比如合作伙伴）除非
   - 联盟成员为了允许服务访问而必须要求的，或者
   - 之前，用户同意过；
7) 【安全措施】采用适当的技术措施或者管理措施来保护属性免受突发或者非法的损坏、突发丢失、篡改、未授权泄露或者访问。综合考虑目前的技术水平和实现代价，这些措施应符合所要处理的风险、符合要保护数据的性质，保证一定级别的安全。

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。联盟成员必须遵循本文档最新版本，详见 CARSI

资源共享服务官方网站
https://www.carsi.edu.cn/docs/data_protection_profile_zh.pdf。