

附录 4：CARSI 资源共享服务提供者 SP 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）的联盟政策要求，如果联盟成员是服务提供者 SP，在提供资源或者确定服务访问权限时都必须保证遵守本服务提供者 SP 管理标准中定义的所有规则。

3. 服务提供者 SP 规则

- 1) **【授权责任】** 服务提供者 SP 负责用户授权，CARSI 联盟运行团队和用户身份所属机构 IdP 不对此负责。
- 2) **【数据保护】** 服务提供机构的每个服务提供者 SP 均需遵守“附录 3：CARSI 资源共享服务数据保护要求”中要求的所有属性处理原则。
- 3) **【面向用户的责任】** 服务提供机构应该至少在用户第一次访问该服务时，以简单、直接、永久可查询的方式提示保密政策，至少包括以下信息：
 - 服务提供机构的名称和地址；
 - 使用用户身份属性信息的目的；
 - 对被处理属性的描述；
 - 有可能和哪些第三方或者哪一类第三方共享这些信息；
 - 对用户信息所拥有的使用、校正、删除的权利；
 - 用户身份信息保存多长时间。
- 4) **【用户属性信息的用途】** 服务提供机构仅将用户属性信息用于以下用途：
 - 根据属性信息控制用户的资源访问权限；
 - 为了方便向身份提供者追溯用户，记录用户访问并保留访问记录；
 - 定制用户界面；
 - 提供用户支持；
 - 向用户详细规定的其他用途；
- 5) **【用户属性信息的管理及保护】** 服务提供机构必须对取得的用户属性信息进行严格的管理及保护，防止信息丢失、被盗用或遭篡改；
- 6) **【安全违规】** 服务提供机构应该第一时间向用户数据相关的身份所属机构报告所有涉嫌隐私和安全违规（包括未经授权的泄露或者损害，实际或者可能发生的数据、文档或者相关设备丢失，等）；
- 7) **【元文件数据的准确】** 服务提供机构必须向联盟提交关于服务提供者的准确的元文件数据，并且，当元文件中的数据发现变化时，承诺尽快通知联盟进行更新。
- 8) **【优先权】** 当本标准条款和服务提供机构与用户身份所属机构的其他协议条款发生冲突时，服务提供机构应当首先遵守与用户身份所属机构的单独协议。

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/sp_management_standard_zh.pdf。