

Appendix 4: CARSI Service Provider Management Standard

1. Definitions and Terminology

Section 1 - 'Definitions and Terminology' of the latest CARSI Identity Federation Policy published on the CARSI Identity Federation website at https://www.carsi.edu.cn/docs/federation_policy_en.pdf applies to this document.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119, see <http://tools.ietf.org/html/rfc2119>.

2. Introduction

The CARSI Identity Federation Policy requires that, when acting as a Service Provider Organization, Federation Member MUST ensure that the deployment of each of its Service Providers complies with all the rules defined in this CARSI Identity Federation Service Provider Management Standard.

3. Rules for Service Provider

- a. [Responsibility of authorization] The Service Provider Organization acknowledges that it is responsible for the management of Authorization to the services and resources of its Service Providers for the End Users, and that CARSI, the Federation Operator Team and the Home Organizations will have no liability in respect thereof.
- b. [Data protection] The Service Provider Organization SHALL comply with all the attribute processing principles defined in the CARSI Identity Federation Data Protection Profile on each of its Service Providers.
- c. [Information duty towards End User] The Service Provider Organization SHALL provide to the End User, at least at first contact, in an easily, directly and permanently accessible way a Privacy Policy, containing at least the following information:
 - the name and address of the Service Provider Organization;
 - the purpose or purposes of the processing of the Attributes;
 - a description of the Attributes being processed;
 - the third party recipients or categories of third party recipient to whom the Attributes might be disclosed;
 - the existence of the rights to access, rectify and delete the Attributes held about the End User;
 - the retention period of the Attributes;
- d. [User Attributes Using] The Service Provider Organization May only use the user attribute information for the following purposes:
 - Authorizing access to the service for which the attributes have been provided.
 - Recording end user access, and retention of records, in order to facilitate traceability of end users via an Identity Provider;
 - Personalization of a user interface;
 - Providing end user support;
 - Any other uses required, to the extent they are specifically disclosed.
- e. [User Attribute Information Management and Protection] The Service Provider Organization MUST strictly manage and protect users' attribute information, and prevent the information from being lost, stolen or tampered with.
- f. [Security Breaches] The Service Provider Organization SHALL, without undue delay, report all suspected privacy or security breaches (including unauthorized disclosure or compromise, actual or

possible loss of data, documents or any device, etc.) concerning the Attributes to the Home Organization(s) or its Agent(s).

- g. [Metadata Accuracy] The Service Provider Organization MUST provide accurate metadata to CARS Identity Federation and agree to notify CARS Identity Federation as soon as possible when the metadata changes.
- h. [Precedence] The Service Provider Organization SHALL comply with the stipulation that in the event of a conflict between a provision contained in this Standard and a provision of the agreement concluded between the Service Provider Organization and the Home Organization, the provision of the agreement concluded between the Service Provider Organization and the Home Organization takes precedence over the provision of this Standard.

4. Amendment

The Federation Operator Team has the right to amend this document from time to time. Any such amendments need to be approved by the CARS Identity Federation Steering Committee. The amended CARS Service Provider Management Standard will become binding upon the Federation Members. The Federation Members MUST follow the latest version of this document that is made available on the CARS Identity Federation website at https://www.carsi.edu.cn/docs/sp_management_standard_en.pdf.