Appendix 5: CARSI Identity 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 Home Organization, Federation Member MUST ensure that the deployment of each of its Identity Providers complies with all the rules defined in this CARSI Identity Federation Identity Provider Management Standard.

3. Rules for Identity Provider

a. The Home Organization MUST collect or generate in its Identity Provider the Core Attributes as defined by the Federation.
b. The Home Organization MAY ONLY release Attributes from its Identity Provider to a Service Provider, or another Identity Provider, with the permission of the End User.
c. The Home Organization MUST ensure that accurate information is provided about End Users in its Identity Provider. In particular:
   - Credentials of End Users who are no longer permitted by the Home Organization to access the Federation MUST be revoked promptly, or at least no Attributes must be asserted for such End Users from its Identity Provider to other Service Providers;
   - Where unique persistent Attributes are associated with an End User, the Home Organization MUST ensure that these Attribute values are not re-issued to another End User for at least 24 months after the last possible use by the previous End User; and
   - Where an End User's status, or any other information described by Attributes, changes, the relevant Attributes MUST be also changed within one month starting from such change happened.
d. The Home Organization MUST use reasonable endeavors to provide those End Users in respect of to whom it provides the Attributes, with appropriate information on how to use their credentials safely and securely.
e. The Home Organization MUST ensure that sufficient logging information in its Identity Provider is retained for the period specified by the Federation (6 months) to be able to associate a particular End User with a given session that it has authenticated.
f. The Home Organization MUST make anonymized usage and log information of its Identity Provider available to the Federation Operator Team for the purposes of assisting the troubleshooting of access issues and developing aggregated /anonymized usage statistics.
g. The End User will be responsible for their acts or omissions, including abiding by any licenses or other agreements, and complying with the policies set by the Home Organization and /or the Service Provider Organization.

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 CARSI Identity Federation Steering Committee. The amended IdP Managemtn Standard will become binding upon the Federation members. The latest version of the CARSI IdP Managemtn Standard is made available on the CARSI Identity Federation website at https://www.carsi.edu.cn/docs/idp_management_standard_en.pdf.