Appendix 3: CARSI Identity Federation - Data Protection Profile

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 follows all the attribute processing principles defined in this CARSI Identity Federation Data Protection Profile for providing access to the protected resources or services.

This requirement is also included in the CARSI Identity Federation Service Provider Management Standard.

3. Attribute Processing Principles

The Service Provider Organization agrees and warrants for all of its Service Providers:

a. [Legal compliance] to only process the Attributes in accordance with the relevant provisions of the Personal Data protection laws of the People's Republic of China;

b. [Data minimization] to minimize the Attributes requested from a Home Organization to those that are adequate, relevant and not excessive for enabling access to the service and, where a number of Attributes could be used to provide access to the service, use the least intrusive Attributes possible;

c. [Purpose limitation] to only process Attributes of the End User for the following purposes, under the precondition of having got permission from the end user or the Home Organization:
   - Authorizing access to the service of the Service Provider;
   - Recording End User access, and retention of records, in order to facilitate traceability of End Users via their Home Organizations;
   - Personalization of a user interface;
   - Providing End User support; and
   - Generating aggregated anonymized usage statistics for service development and /or for other purposes agreed by the Home Organization;

d. [Deviating purposes] not to process the Attributes of the End User for any other purposes (e.g. selling the Attributes or selling the personalization such as search history, commercial communications, profiling). Members that wish to use Attributes supplied to their Service Providers in other ways MUST arrange this either by obtaining positive informed consent from each individual End User, or by contract with the Home Organizations, who are then responsible for informing their End Users;

e. [Data retention] to delete or anonymize all Attributes as soon as they are no longer necessary for the purposes of providing the service;

f. [Third parties] not to transfer Attributes to any third party (such as a collaboration partner) except
   - if mandated by the Member for enabling access to its service on its behalf, or
   - if prior consent has been given by the End User;

g. [Security measures] to take appropriate technical and organizational measures to safeguard Attributes against accidental or unlawful destruction or accidental loss, alteration, unauthorized

disclosure or access. These measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

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 Data Protection Profile will become binding upon the Federation members. The Federation Members MUST follow the latest version of this document which is made available on the CARSI Identity Federation website at https://www.carsi.edu.cn/docs/data_protection_profile_en.pdf.