# National Identity Exchange Federation

# Privacy Policy

## Version 1.0

## August 18, 2014

# Table of Contents

# 1. Target Audience and Purpose

This document specifies technical privacy requirements for participants in the National Identity Exchange Federation (NIEF). The target audience includes technical representatives of organizations that intend to participate in NIEF as Identity Provider Organizations (IDPOs), Service Provider Organizations (SPOs), Service Consumer Organizations (SCOs), Attribute Provider Organizations (APOs), or some combination of these roles.[1] This document focuses only on issues of end-user privacy. It does not cover governance, policy, or other technical and nontechnical interoperability requirements. For more information about those topics, see the documents listed in Table 1.

# 2. NIEF Identity Trust Framework and Terminology

This document is one component of the NIEF Identity Trust Framework. See [NIEF OPP] for more information about the full NIEF Identity Trust Framework. This document contains language that uses technical terms related to federations, identity management, Web services, and other related technologies. To minimize confusion for readers, it is important that each technical term have a precise definition. Accordingly, all technical terms in this document are to be interpreted as described in [NIEF Terms].

# 3. References

Table 1 contains a list of references used within this document.

| References | |
|---|---|
| **Document ID** | **Document Name and URL if Applicable** |
| NIEF Terms | NIEF Terminology Reference |
| NIEF OPP | NIEF Center Operational Policies and Procedures |
| RFC 2119 | Key words for use in RFCs to Indicate Requirement Levels |

**Table 1: References**

# 4. Notation for Normative Content

This document contains both normative and non-normative content. Sections containing normative content are marked appropriately. In those sections, the key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in [RFC 2119].

# 5. NIEF Privacy Policy Rules

NIEF participants are subject to the following rules regarding the protection of end-users’ privacy.

[1] See [NIEF Terms] for terminology related to various organizational and technical roles in NIEF.

1. **Opt-In** – When participating in a transaction using the NIEF Web Browser User-to-System Profile, a Federal Identity, Credentialing, and Access Management (FICAM) Level of Assurance (LOA) 2 Identity Provider Organization (IDPO) or FICAM LOA 3 IDPO MUST obtain positive confirmation from the End User before any End User information is transmitted to any NIEF Service Provider Organization (SPO) or Federal relying party systems. Confirmation MUST be obtained at "run-time" (just before the information is transmitted) and MUST enable the End-User to see each attribute that is to be transmitted to the SPO or Federal relying party system as part of the opt-in process. Also, the IDPO SHOULD allow the End User to opt out of individual attributes for each transaction.

2. **Minimal Attribute Release** – A FICAM LOA 2 or FICAM LOA 3 IDPO MUST transmit only those attributes that were explicitly requested by the NIEF Service Provider Organization (SPO) or Federal relying party. A NIEF Attribute Provider Organization (APO) MUST transmit only those attributes that were explicitly requested by the NIEF attribute requester. When acting as an attribute requester, a FICAM LOA 2 IDPO, FICAM LOA 3 IDPO, or APO MUST only request attributes that are in accordance with the set of attributes that were explicitly requested by the NIEF SPO for which the attributes are requested.

3. **Activity Tracking** – A FICAM LOA 2 IDPO, FICAM LOA 3 IDPO, or APO MUST NOT disclose information on its End Users' activities to any party, or use the information for any purpose other than federated authentication, audit, and privilege management.

4. **Adequate Notice** – A FICAM LOA 2 IDPO or FICAM LOA 3 IDPO MUST provide the End User with adequate notice regarding federated authentication. "Adequate Notice" includes a general description of the authentication event, any transaction(s) with the NIEF SPO or Federal relying party, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice SHOULD be incorporated into the IDPO's Opt-In process.

5. **Termination** – In the event that a FICAM LOA 2 IDPO, FICAM LOA 3 IDPO, or APO ceases to provide its services to, or on behalf of, an End User, the IDPO or APO MUST continue to protect any sensitive data, including PII, about the End User.

6. **Appropriate Attribute Request and Usage** – A NIEF member MUST request only those attributes that it requires for the purposes of making authorization decisions, dynamically provisioning accounts, performing audit logging, or forwarding the attributes to another NIEF member for these purposes. In addition, a NIEF member MUST use requested attributes only for the purposes of making authorization decisions, dynamically provisioning accounts, performing audit logging or forwarding the attributes to another NIEF member for these purposes.