

**Example Company, Inc.**  
**Identity Management Architecture**  
**Policy on Federating Identity**

**Status:** [Approved | Draft – RFC | Final Draft – Awaiting Approval ]

**Date:** 01APR04

**1.0 Purpose**

The purpose of this policy is to provide guidance concerning the use of federated identity technologies and services at Example Company, Inc..

**2.0 Scope**

This policy applies to all Example Company, Inc. projects, procurements, employees and affiliates.

**3.0 Definitions**

**4.0 References**

Identity Reference Framework, Section 3.9, Federation Standards  
Identity Reference Framework, Section 8.6, Federation Products  
Policy on Privacy.

**5.0 Policy**

**5.1 Use of Identity Reference Framework.** Where ever possible, federated identity project shall use the standards contained within the Identity Reference Framework. Because working with external partners may often require compromise, deviation from those standards is authorized as long as written approval from the CIO's office is obtained.

**5.2 Federation Charters.** When entering into a federated identity arrangement with either internal or external parties to Example Company, Inc. a charter for the project shall be prepared that contains:

- Description of the federation use-case and the identity problem being solved
- Roster of participants
- Definition of the technical agreements, including standards to be used and any deviations from the Identity Reference Framework
- Definition of business requirements

The charter shall be approved by the project manager and all participating organizations for internal federations. The charter must be approved by the Office of the CIO for external federations.

**5.3 Logging.** Federated identity systems shall log identity transactions. The logs may be kept by either Example Company, Inc. or a third party as long as they are available to Example Company, Inc. on demand (maximum of 4 hour delay from request to delivery). Logs shall contain sufficient detail to identify the identity of the party to the transaction, the resource being accessed, the authorization scheme used, the authentication scheme used, and time to within millisecond accuracy.

**5.4 External Auditor.** All external parties to federated identity agreements with Example Company, Inc. shall be approved by the Chief Security Officer or certified to meet the security standards of SAS70 by providing Example Company, Inc. with a SAS70 Type II report documenting an audit by a reputable external auditor.

**5.5 Legal and Technical Counsel.** Any federation agreement with an external partner shall be reviewed by corporate counsel and the CIO's office prior to being signed.

**5.6 Privacy Policy.** Federated identity agreements will meet the requirements of the Policy on Privacy unless approval of the CIO's office is obtained.

**5.7 Liability Limits.** Any federation agreement with an external party shall include language that limits Example Company Inc.'s liability in the event of fraud or error. These liability limits must be specifically reviewed and approved by corporate counsel.

**6.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**7.0 Contacts**

**7.1 Custodian**

IMA Team, Office of the CIO  
imateam@example.com  
801.555.1212 x563

**7.2 Approval Body**

Identity Management Architecture Review Board

**8.0 Revision History**

Version	Approval Date	Comments
1.0	01APR04	Initial version approved.