

Example Company, Inc.
Identity Management Architecture
Policy on Privacy

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

Date: 01APR04

1.0 Purpose

The purpose of this policy is to provide guidance concerning information privacy at Example Company, Inc..

2.0 Scope

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

3.0 Definitions

3.1 Personally Identifying Information. Personally identifying information is any collection of identity attributes that, when taken together, can be used to identify a single individual.

3.2 Aggregate Identity Information. Aggregate Identity Information is statistical information about the identity of groups. To not also me personally identifying, it must be impossible to infer personal identity information from the aggregate.

4.0 References

Office of the CIO, General Data Confidentiality Agreement, version 1.3

Example Company, Inc. Guiding Principles on Privacy, version 1.1

5.0 Policy

5.1 Chief Privacy Officer (CPO). An individual at the Vice President level or above will be designate as Chief Privacy Officer for Example Company, Inc. The CPO will be responsible for enforcing this policy and establishing other rules regarding privacy as needed and in keeping with this policy and Example Company, Inc. Guiding Principles on Privacy.

5.2 Protecting Personally Identifying Information. Personally identifying information will be protected from accidental disclosure and theft. Personally identifying information should only be disclosed with the individual's explicit permission or when required by law.

5.3 Posting Privacy Statement. Any online service that requests or requires personally identifying information shall post a user readable privacy statements that states why personal information is being collected, how it will be used, and if it will be disclosed to any third party.

5.4 Privacy Reviews. Any online service that collects personally identifying information shall conduct an initial study of the information being collected and the need to collect it. The study shall further review the plans for protecting the information. After the service has gone live, the review will be repeated annually.

5.5 Using Best Practices. System designers and operations personnel shall ensure that adequate steps are taken to protect personally identifying information consistent with best practice.

5.6 Applicable Law. Personally identifying information shall only be collected and stored in a manner consistent with applicable laws.

5.7 Data Custodian Requirements. Each repository of personally identifying information shall have a formally appointed custodian who will be responsible for ensuring that this policy is adhered to for that repository.

5.8 Data Confidentiality. Any person with access to repositories containing personally identifying information shall sign a statement that gives specific guidelines about what they may and may not do with the data. The Office of the CIO is responsible for maintaining a generic agreement. Data custodians may, with the help of the Office of the CIO tailor the generic agreement to their specific requirements as needed.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Services that fail to meet the standards outlined in this policy can be shutdown by the Office of the CIO until they are brought into compliance.

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.