

**Example Company, Inc.**  
**Identity Management Architecture**  
**Policy on Access Control**

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

**Date:** 01APR04

**1.0 Purpose**

The purpose of this policy is to provide guidance concerning access control for resources on information systems at Example Company, Inc..

**2.0 Scope**

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

**3.0 Definitions**

Owner – the person responsible for control of a resource. The owner is accountable for access control and disposition of a resource. A resource will typically have one owner.

Custodian – anyone who has control of a resource. Resources may have multiple custodians. Custodians manage resources day-to-day for the owner.

User – anyone who wants access to a resource.

Access – any action taken on a resource including creating, modifying, destroying, disseminating, or sharing.

**4.0 References**

Policy on Naming and Certificates

Policy on Directories

Policy on Authentication

**5.0 Policy**

**5.1 Access Control Levels.** Information resources shall be classified as one of “uncontrolled,” “audited,” or “controlled.” Uncontrolled resources are freely available to anyone without restriction. Audited resources will be made available so that access can be reliably tracked. Controlled resources can only be accessed according to an access policy set by the owner or custodian of the resource.

**5.2 Use of Authentication Levels.** Uncontrolled resources require no authentication. Audited resources may use any of the authentication levels specified on the Policy on Authentication. Controlled resources may not use Casual authentication. The resource owner may specify minimum authentication levels for any audited or controlled resource.

**5.3 Owner Responsibilities.** Owners are responsible for correctly classifying their resources and for tracking the actions of custodians and users as well as monitoring the design and operations of systems to ensure that the policy is followed. Owners are responsible for ensuring that access privileges to their resource are removed for users or custodians who routinely disregard their policies.

**5.4 Custodian Responsibilities.** Custodians are responsible for following the policies and guidelines set by the owner of the resource and for informing the owner whenever such policies are not being followed, may be ineffective, or should be reviewed. Custodians are responsible for ensuring technical solutions to access control policies set by the owner are effective.

**5.5 User Responsibilities.** Users are responsible for following the policies of the resource owner and instructions from the owner or custodian regarding proper access to a resource.

**5.6 Access Control Audits.** The Chief Security Office is responsible for auditing access control systems, access control policies, and classification levels for all Example Company, Inc. resources. Audited resources will be reviewed on a spot basis (statistically meaningful sample) monthly. Controlled resources will be audited once per year. Information systems will be audited in the design phase, as part of the pre-launch quality assurance process, and after any major system upgrades.

**5.7 Unintended Disclosure.** Owners and custodians shall take necessary steps to protect controlled resources from unintended disclosure.

### **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.