

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

**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 passwords 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**

Password Selection and Protection Guide  
Policy on Naming and Certificates

**5.0 Policy**

**5.1 Use of Passwords.** Passwords shall be used to protect all company digital assets from unauthorized access and use with two exceptions. (1) Passwords are not required when another authentication mechanism is used and that mechanism can be shown to be at least as strong as password authentication. (2) Password authentication is not required of digital assets that have specifically been designated as “publicly accessible” by their custodian.

**5.2 Protection of Passwords.** Employees who are issued passwords are responsible for protecting them from intentional or accidental disclosure. Passwords must not be shared with anyone. Procedures for user support shall be designed such that it is never necessary for anyone to know someone else’s password after initial assignment. Passwords are often embedded in applications. Designers and operators of those systems should take precautions consistent with best practices to protect those passwords from disclosure.

**5.3 Password Reset.** Password reset functions must be implemented to require authentication of the individual during the reset operation to the same level that the password system itself maintains.

**5.4 Password Aging.** Password aging is {required | not allowed} on Example Company, Inc. systems unless specifically authorized by the Office of the CIO.

**5.5 Format of Passwords.** Passwords must be at least eight characters long and include two characters that are not alphabetic. Dictionary words are not acceptable as passwords. Password reset systems shall be designed to enforce these format requirements.

**5.6 Storing and Transmitting Passwords.** Passwords shall be stored only in approved repositories. The Chief Security Office is responsible for approving password storage repositories. Passwords shall not be stored or transmitted in plaintext without express permission of the Office of the CIO.

**5.7 Passwords for Each Identifier.** Each identifier used for authentication shall have its own password.

**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.