Idaho Technology Authority (ITA)

ENTERPRISE POLICY – P4500 SECURITY-COMPUTER OPERATIONS MANAGEMENT POLICIES

Category: P4502 – PRIVILEGE ACCESS MANAGEMENT

CONTENTS:

I. AUTHORITY

Authority: Idaho Code § 67-5745 (A)(B)(C)

II. ABSTRACT

This policy is designed to reduce the risk of compromise to agency's information and information assets by mandating the use of multifactor authentication for all privileged accounts. Privileged accounts are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged accounts include, for example, key management, account management, network and system administration, database administration, and web administration.

Agencies may implement multifactor authentication to secure "non-privileged" user accounts to enhance security as an alternative of single factor authentication using strong passwords (ITA Guideline G560 – Passwords).

III. DEFINITIONS

Authenticator - Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity.

Multifactor Authentication - A characteristic of an authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multi-factor authentication can be performed using a single authenticator

that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Privileged Account - An information system account with authorizations of a privileged user.

Privileged User – A user or service that is trusted to perform security-relevant functions that ordinary users are not authorized to perform.

User – Individual or (application) process acting on behalf of an individual authorized to access an information system.

IV. POLICY

Agencies shall implement multifactor authentication for all privileged user accounts (IA-2).

Privileged user accounts shall be monitored with automated tools to alert when the accounts are modified.

V. EXEMPTION PROCESS

Refer to ITA Enterprise Policy P1010 (Information Technology Policies, Standards, and Guidelines Framework).

VI. PROCEDURE REFERENCE

NIST Special Publication 800-53 Rev 4 (IA-2)
ITA Enterprise Guideline G560 (Passwords)

VII. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876 or security@cio.idaho.gov.

VIII. ADDITIONAL RESOURCES

None.

REVISION HISTORY

Effective Date: 12/6/2016