Idaho Technology Authority (ITA)

ENTERPRISE STANDARDS – S6000 SECURITY

Category: S6030 – IDENTITY AND AUTHENTICATION

CONTENTS:

I. DEFINITIONS

See ITA Guideline G105 (ITA Glossary of Terms) for definitions.

II. RATIONALE

A vital element for the proper protection of an enterprise and its assets is a strong identity management and authentication program. The objective of this standard is to provide basic authentication requirements, based on published industry best practices, that form a solid foundation for current and future identity and access management (IAM) strategies.

This standardizes addresses and outlines mandatory risk and privilege-based authentication management including password complexity, length, acceptable use, augmentation of multi-factor authentication (MFA), and verifier minimum requirements.

III. APPROVED STANDARD(S)

1. All accounts, devices, and services must be protected from unauthorized access and use with, at a minimum, a username and password that meets the mandatory length and complexity requirements described herein.
2. All passwords must:
    a. Be eight (8) characters or longer
    b. Contain at least one (1) uppercase letter
    c. Contain at least one (1) lowercase letter
    d. Contain at least one (1) numeric or symbol character
    e. Not be the same as any of the last 24 passwords
3. All passwords for user accounts with elevated privileges must meet complexity requirements and contain at least 15 characters.

4. Service accounts and built-in accounts (e.g. local administrator, super administrator, etc.) must meet complexity requirements and contain at least 20 characters.
5. Passwords on legacy systems, such as mainframes or other antiquated systems incompatible with requirements 2-4, must be the maximum allowable length and contain as many complexity elements as possible. These passwords on legacy systems should also be considered for more frequent changes as a compensating control for their weak authentication capabilities.
6. User accounts and passwords must uniquely identify an individual and are only for this assigned individual's use. Sharing of user account credentials and passwords is prohibited.
7. All users are responsible for the protection of their user accounts and must take all reasonable measures to protect them from disclosure or misuse.
8. Upon the separation of any user, for voluntary or involuntary reasons, all accounts the user had access to must be disabled and undergo an immediate authenticator reset to maintain account integrity.
9. All user accounts with elevated privilege must be protected with multi-factor authentication (MFA). Per CIS Critical Security Controls v7, control 16.3, all accounts must be protected with MFA. While other CIS controls specify MFA, control 16.3 is the most comprehensive.
10. User accounts must lock out after a maximum of five (5) failed authentication attempts within 15 minutes. Locked user accounts must be manually re-enabled by an approved IT technician, by way of a self-service solution, or automatically unlock after 15 minutes. Locked privileged accounts must not automatically unlock and are only to be unlocked by an approved IT technician or self-service solution.
11. Agencies may implement a self-service solution for non-privileged accounts to unlock or reset their account, or to manage their multi-factor authenticators. Self-service authentication solutions should use multi-factor authentication wherever possible.
12. Except service accounts and privileged accounts, all accounts will have mandatory password changes performed every 90 days or if suspected compromised, whichever is soonest. Service accounts will have passwords changes performed every 24 months or if suspected compromised, whichever is soonest. Privileged accounts will have password changes performed every 60 days or if suspected compromised, whichever is soonest.
13. Certificate-based authenticators must be reissued at least every 24 months.
14. All sensitive network devices and servers to include switches, routers, and particularly domain controllers will be protected with MFA.
15. Password management solutions will be used to contain and manage all enterprise sensitive passwords when feasible.
16. Verifiers must permit a password at least 64 characters in length.
17. Verifiers must permit use of ASCII and Unicode characters, including space characters.
18. Verifiers must only handle passwords in hashed or encrypted form using approved security functions, per FIPS 140-2 Annex A.

IV. PROCEDURE REFERENCE

- ITA Policy P4503 (Identity and Access Management)
- ITA Policy P4130 (Information Systems Classification Policy)
- IRS Publication 1075 (Tax Information Security Guidelines for Federal, State, and Local Agencies)
- NIST Special Publication 800-63-3 (Digital Identity Guidelines)
- NIST Internal Report 7298r2 (Glossary of Key Information Security Terms)
- NIST FIPS Publication 140-2 (Security Requirements for Cryptographic Modules)
- CIS Critical Security Controls v7

V. REVIEW CYCLE

Twelve (12) Months

VI. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

REVISION HISTORY

Effective Date: 12/14/2021