161 – Password Standard

Purpose

The Password Standard is intended to facilitate the attainment of the following policies and associated Information Technology (IT) Security Policy objectives:

- Access Control Policy (AC-01)
- Audit and Accountability Policy (AU-01)
- Identification and Authentication Policy (IA-01)
- Physical and Environment Protection Policy (PE-01)

Standard

This standard uses the NIST SP 800-53 Rev. 5 framework as the guideline to establish control objectives to address a diverse set of security and privacy requirements. Not all controls within NIST SP 800-53 Rev. 5 may be selected for the Statewide baseline policies and standards. Agencies must categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately. This standard uses Table 3-1 and Table 3-7 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. At a minimum, all low controls are selected, and certain moderate controls are selected. Agencies are to reflect their controls through the quarterly reporting process to DOA-DET.

Executive Branch Agencies are to develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. Some agencies will have specific regulatory requirements that they must adhere to that go beyond what other agencies would need to adhere to. Implementation of the standard controls within this document can be (1) a common (inheritable) control, (2) a system-specific control, or (3) a hybrid control. The control implementation defines the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and authorization.

This standard includes the minimum baseline controls that Executive Branch agencies are to adhere to. Agencies may have additional controls they must adhere to that are not listed here.

BASELINE CONTROLS

Note: The following password settings are the minimum for use with Active Directory. There are multiple systems and applications in use by the executive branch agencies. It is not possible to have one password standard that covers all possible password settings for different systems and applications. Agencies should have documented procedures for each type of system or application that details the password setting requirements.

Authenticator Management | Password-Based Authentication (IA-5(1)):

- For password-based authentication:
  - Maintain a list of commonly used, expected, or compromised passwords and update the list annually and when passwords are suspected to have been compromised directly or indirectly;
  - Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords;
  - Transmit passwords only over cryptographically protected channels;
  - Store passwords using an approved salted key derivation function, preferably using a keyed hash;
  - Require immediate selection of a new password upon account recovery;
  - Allow user selection of long passwords and passphrases, including spaces and all printable characters, where applicable;
  - Enforce the following settings when an agency-defined password policy is not configured to their own composition and complexity rules based on their regulatory directives:
    - Password length must be a minimum of eight (8) characters for individual account access and a minimum of sixteen (16) characters for privileged administrative account access. The mainframe password length is limited to (8) characters for both privilege administrative and individual account access.
    - Passwords must include three (3) of the following: uppercase letters, lowercase letters, numbers, special characters (e.g., !, @, #, $, etc.)
  - Passwords should not contain: your name, User ID, or simple patterns.
- Passwords are set to expire on an agency-defined frequency;
- Passwords may not be re-used within 24 iterations;
- Access to accounts will be locked after an agency-defined number of consecutive unsuccessful login attempts within an agency-defined time period;
- Temporary passwords provided for newly created or changed logons require an immediate change to a permanent password;
- Account holders must maintain the confidentiality of passwords and any associated security questions/answers or other authentication information; and
- Report any password abuse to the Enterprise Security via the ESD at (608) 264-9383 or ESDhelp@wisconsin.gov or Agency help desk.

Note: More restrictive password parameters may be implemented depending on the system/information being accessed. Those procedures should be documented accordingly. Exceptions at a lower requirement to this

standard must be requested via the Enterprise Exception Procedure and must not be implemented without documented approval of the exception request.

Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
State information - Any information that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.
DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by the agency.

Exception Process

Exceptions to any Executive Branch Agency's Security Policies or Standards must follow the Executive Branch Risk Exception Procedure.

Document History/Owner

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to the DET Bureau of Security. As such, the DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	10/29/19	Reviewed with Agency Security Officers and feedback collected. Planning for making revisions.	Bureau of Security	10/29/19
2.0	11/03/20	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	11/11/20
3.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	06/24/22
4.0	7/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/Enterprise IT Author: DOA/DET/BOS	08/01/23
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and Approved by:

Trina Zanow, CIO

DocuSigned by:
Trina Zanow
A11B57ECEC77402...

8/1/2023 | 1:49 PM CDT

Print/Type
Title

Signature

Date