STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2024

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

Based on NIST SP 800-53 Rev. 5, DET's Standards address a diverse set of security and privacy requirements. As a currently established baseline for implementation, DOA utilizes all low level, and selected moderate level controls in support of its security posture initiatives. Agencies shall categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately as defined by Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. Agencies shall update DET on the status of their baseline control implementation through the reporting and monitoring process.

Executive Branch Agencies shall develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. **Note:** Some agencies have specific regulatory requirements to follow that go above and beyond the requirements for other agencies. 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 contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Note: The following password requirements are currently established for use with Active Directory. As a result of there being multiple systems and applications in use by the Executive Branch Agencies, specific requirements for those systems and applications exceed the scope of this standard. Therefore, it is the responsibility of the branch agencies to develop and implement sufficient procedures that support every type of system or application requiring password requirements they manage.

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 shall 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 shall include three (3) of the following: uppercase letters, lowercase letters, numbers, special characters (e.g. !, @, #, $, etc.).
    - Passwords shall not contain: your name, User ID, or simple patterns.
- Passwords are set to expire on an agency-defined frequency.
- Passwords shall not be re-used within 24 iterations.
- Access to accounts shall 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 shall maintain the confidentiality of passwords and any associated security questions/answers or other authentication information.
- 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 shall be requested via the Enterprise Exception Procedure and shall 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. Agency or State Agency may be used interchangeably with Executive Branch Agency.

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 shall 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 Wis. Stat. § 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
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 and Enterprise IT Author: DOA/DET/BOS	08/01/23
5.0	7/2/24	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	7/30/24
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:

Troy Stairwalt, State of Wisconsin Chief Information Security Officer

DocuSigned by:
Troy Stairwalt
DFEB606EC2524A8...

7/31/2024 | 4:05 PM CDT

Print/Type Title

Signature

Date