**University of Alabama at Birmingham**

**PASSWORD RULE**

Approved and Implemented: January 1, 2014

Reviewed/Updated: February 12, 2021

**Related Policies, Procedures, and Resources**

[Data Protection and Security Policy](https://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000038.aspx)

[Data Classification Rule](https://www.uab.edu/it/home/component/k2/item/801-data-classification-rule)

[Data Protection Rule](https://www.uab.edu/it/home/component/k2/item/818-data-protection-rule)

**1.0 Introduction**

The purpose of this standard is to define password requirements for users, servers, and applications at UAB.

**2.0 Scope and Applicability**

This standard applies to all users and systems at UAB which utilize BlazerIDs.

**3.0 Password Standard**

1. Length: All account passwords on systems leveraging BlazerIDs will be a minimum of 15 characters and a maximum of 32 characters. Other account passwords not using BlazerIDs shall be required to request an exception.
   1. System Accounts will be complex, 32 characters and have no expiration.
   2. Vendor supplied, pre-configured, default passwords are forbidden.
2. Lockout: After 6 failed login attempts, accounts should be disabled and locked out for at least 30 minutes where feasible.
3. Expiration: All user account passwords shall expire annually unless authentication is protected by University provided two-factor authentication or approved biometrics. All privileged user account or administrator passwords shall expire at intervals as required by regulation (e.g., HIPAA, GLBA, etc.).
4. Password Reset after Compromise or Disclosure: Password resets will be required in situations where continued use of a password creates risk of unauthorized access to the computing account or resource.
5. History: Password / passphrase history shall be kept to prevent the previous (1) password from re-use.

6) Caching: Applications or Systems that utilize BlazerIDs shall not cache BlazerID passwords / passphrases, even if hashed or otherwise encrypted, without an approved exception. Individual devices such as smartphone, tablets, etc. are not included.

7) Complexity: Passwords shall contain at least one character from three of the following ASCII character sets: lowercase alphabetic, uppercase alphabetic, and numbers.

8) Logging: Systems shall log successful and failed logon attempts and retain such logs for a minimum of 90 calendar days.

9) Encryption: A one-way hash function wherever possible is required for storing passwords.

10) Unused Accounts: Student accounts unused for more than 180 days shall be disabled. All other accounts unused for more than 90 days shall be disabled.

11) Registration: Applications that leverage BlazerID authentication through a central mechanism/system must be registered with UAB IT.

12) Password Strength: Passwords will be checked against known bad passwords and common passwords to determine strength of the password.

4**.0 Enforcement**

The Office of the Vice President for Information Technology is responsible for this standard and will programmatically enforce it through the UAB IT Enterprise Identity Management (IDM) organization.

**Change History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Description** | **Approval** | **Date** |
| 1.0 | Initial document | Dr. Douglas Rigney | 1/1/2014 |
| 2.0 | Changed password expiration to annual | Dr. Curt Carver | 9/15/2015 |
|  | Reviewed - no changes/updates |  | 10/12/2017 |
|  | Reviewed - no changes/updates |  | 6/4/2018 |
|  | Reviewed - no changes/updates |  | 6/3/2019 |
| 3.0 | 3.3 Removed password expiration If 2FA is used  3.4 Added Password reset after compromise or disclosure  3.12 Added password checking against known bad and common passwords | Dr. Curt Carver | 3/9/2020 |
|  | Reviewed - no changes/updates |  | 2/12/2021 |