Title:	**UAB Password / Passphrase Standard**	
Version:	1	**Related Documents:**
Approved:	September 10, 2015	Acceptable Use Policy
Effective:	September 15, 2015	Data Protection and Security Policy
		UAB IT Security Practices

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

Scope: This standard applies to all users and systems at UAB which utilize BlazerIDs or other authentication identifiers.

Standards:

1) **Length:** All account passwords / passphrases on systems leveraging BlazerIDs will be a ***minimum*** of 15 characters and a maximum of 32 characters. Other account passwords / passphrases not using BlazerIDs shall be a minimum of 8 characters.
   - **a.** Proto-BlazerID will be a minimum of 8 characters in length.
   - **b.** System Accounts will be a minimum of 32 characters in length.

2) **Lockout:** After 6 failed login attempts, accounts should be disabled and locked out for at least 30 minutes where feasible.

3) **Expiration:** Passwords / passphrases shall expire according to the table below:

Category	Interval	Category	Interval	Category	Interval
Employee	365 days	Student	365 days	Administrator	90 days
Resource	90 days	Temporary	90 days	Guest (XIAS)	365 days
Proto-BIDs	365 days	System	None	Alumni/Inactive	365 days

   - **a.** The vast majority of UAB students, faculty and staff will fall into the category of Employee or Student.
   - **b.** Information Technology personnel with elevated access or higher compliance assurance requirements will be treated as Administrator category.
   - **c.** When there is a question on which expiration interval applies, the more restrictive interval shall be used.

4) **History:** Password / passphrase history shall be kept to prevent previous passwords / passphrases from re-use to the technical extent possible.

5) **Caching:** Applications or Systems that utilize BlazerIDs shall not cache BlazerID passwords /

passphrases, even if hashed or otherwise encrypted without an approved exception.

   a. Individual devices such as smartphone, tablets, etc. are not subject to this requirement.
   b. Use of a secure, enterprise grade password vault approved by UAB is acceptable by this standard.

6) **Complexity:** Passwords / passphrases shall contain at least 1 character from three of the following ASCII character sets: lowercase alphabetic, uppercase alphabetic, numbers, and symbols.
   a. System Accounts must utilize characters from all four of the character sets mentioned.

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

8) **Screen Lock:** A computer screen locking feature is recommended to be enabled and configured to lock the computing device after a period of inactivity not longer than 15 minutes. If enabled, access to the device shall be granted only after a valid password / passphrase is entered or provided.

   a. Conference rooms may be configured to lock after 60 minutes of inactivity.
   b. Classroom podium systems will be configured to lock after the maximum time of a standard class in that space.

9) **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.

10) **Registration:** Applications that leverage BlazerID authentication through a central mechanism/system or through a federated authentication system (such as eduroam or InCommon) must be registered with UAB IT through the appropriate form available on the UAB IT website. Any systems which do not utilize BlazerID authentication must also be registered with UAB IT.

11) **Encryption:** All credential usage shall be encrypted while in transit, at rest and while in storage.

12) **Multi-factor Authentication (MFA):** The use of a multi-factor authentication (MFA) system adds an additional layer of security for information systems. Some types of regulated sensitive data access require the use of multi-factor authentication per federal guidelines. Use of multi-factor authentication may be a compensating control for exceptions to the standard.

13) **Exceptions:** Exception to or exemptions from any provision of this standard should be routed through the Dean or Vice President first and to the Vice President for Information Technology and Chief Information Officer for consideration.

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.

Approval / Revision History:

Revision	Approval	Approval Date	Effective Date
1	E. Douglas Rigney, PhD, Vice President of Information Technology	December 13, 2013	January 1, 2014
2	Curt A. Carver Jr., Ph.D., Vice President for Information Technology and Chief Information Officer		September 15, 2015

Definitions

Term	Description / Definition
Administrator Accounts	Accounts that have elevated privileges – administrator or privileged access rights.
BlazerID	A mnemonic identifier selected by authorized UAB users to provide a unique identification mechanism for access to systems and processes.
Complexity	The use of a mix of characters to construct a strong password / passphrase that is resistant to guessing and brute-force attacks.
Employee	An individual who holds an active faculty or staff assignment based on Human Resource records maintain by UAB or its affiliates. All employment categories are included in this definition.
Encryption	Process of encoding messages (or information) in such a way (unreadable ciphertext) that eavesdroppers or hackers cannot read it but authorized parties can.
Enterprise Information Security Council	A UAB authorized committee consisting of representatives from the various Colleges/School/organizations on campus focusing of IT issues and topics.
Guest (XIAS) Account	A type of account authorized by a UAB sponsor for non-employees/students to allow access to limited systems.
Lock-out	Security feature that temporarily disables an account for a specified period of time.
Passphrase	A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.
Proto-BlazerID	An identifier selected by individuals to provide a unique identification mechanism for limited access to certain UAB systems. These identifiers may be converted into fully functioning BlazerIDs at a point in time. Examples of Proto BlazerID are those used for pre-admit students, pre-hire employees or professional studies students.
Resource Accounts	Accounts specifically used for inter-process activities such as program to program communications.
Screen Lock	A protective feature that prevents access to device when not in use by authenticated user.
Service Accounts	Generally an account that does not correspond with an actual person that services use to access resources they need to perform their activities.
Standards	Established procedure to be followed in carrying out a given operation or in a given situation.
Student	A student is a person who is enrolled in a formal educational program at UAB typically to take classes, seminars, special studies, etc.
System Accounts	Servers and other high-level computers/devices which run code not normally associated with a user workstation/handheld device; e.g. file servers, application/database servers, and similar devices.
Temporary Accounts	A type of account used for non-permanent situations typically for software testing and debugging prior to being migrated to a production status.