Password Construction and Enforcement Guidelines

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network. This guideline provides best practices for creating secure passwords.

2. Purpose

The purpose of these guidelines is to provide best practices for the creation and enforcement of strong passwords.

3. Scope

These guidelines apply to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, and e-mail accounts.

4. Statement of Guidelines

All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters (15+ will prevent the use of less secure hashing algorithms).
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).
- Unique when compared to previously used passwords (for example, users cannot reuse any of their last 3 passwords)

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters (Windows will not allow usernames as part of complex passwords).

- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)

Passphrases

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, special characters, and spaces (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

Password Expiration

Password expiration is a source of frustration to users, who are often required to create and remember new passwords every few months for dozens of accounts, and thus tend to choose weak passwords and use the same few passwords for many accounts. Organizations should consider having different policies for password expiration for different types of users, systems, operating systems, and applications, to reflect their varying security needs and usability requirements (for example, Faculty/Staff expire annually while student passwords do not expire except in the case of a suspected breach).

Rate Limiting

Controls shall be implemented to protect against online guessing attacks. Unless otherwise specified, failed authentication attempts on a single account shall be limited to no more than 100. Upon reaching the set limit of consecutive failed authentication attempts, the account shall be locked-out until manually unlocked by an administrator or alternate acceptable means (for example, ResetMe Portal).

5. Policy Compliance

5.1 Compliance Measurement

The IT department will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the IT department in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

NIST Special Publication 800-63B

NIST Special Publication 800-118

SANS Consensus Policy Resource Community

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Separated out from the Password Policy and converted to new format.
November 2017	BLaST IU17 IT Department	Update content to reflect NIST as well as the needs of districts served within IU17.