Minimum Password Standard

TYPE:	Technology
TITLE:	Minimum Password Standard
ACCOUNTABILITY:	Administrative Services/Technology Services/Chief Information Officer (CIO)
RESPONSIBILITY:	Technology Services/Chief Information Security Officer (CISO)
EFFECTIVE:	07/15/2015
NUMBER:	S-IT-002
VERSION:	1.1

PURPOSE:

The password is a critical security control that the College uses to prevent unauthorized access to College IT resources. IT systems rely heavily on user/password credentials to ensure authorized access to services and functions, including highly confidential information. Adherence to this standard will help ensure that passwords protecting access to College network and information systems are complex and, therefore, not easily guessed by any intruder.

STATEMENT OF STANDARD:

Devices and systems connected to the Madison College network must require passwords meeting the minimum standards set by the Chief Information Officer and, if possible, technically enforce them. Faculty, staff and students must adhere to the Minimum Passwords Standard for all systems and applications that are used to access College resources.

The minimum standard is:

Length: Password must be 10 characters long.
Password complexity: Password must contain at least one (1) character from three (3) of the following categories:

- Uppercase letter (A-Z)
- Lowercase letter (a-z)
- Digit (0-9)
- Special characters (~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /)

Password history: Cannot reuse the last 4 passwords.
Lockout threshold: Account is locked out after 10 invalid attempts.
Lockout duration: Account is unlocked after 30 minutes. User can attempt another 10 times before lockout.
Change frequency: Once per year.
Exclusion: Must not contain the user's entire UserID or the user's first, last or middle name as part of the password.

Minimum Password Standard

DEFINITIONS:

- **Authentication** is the process of determining whether someone or something is, in fact, who or what it is declared to be.

SHORT-TERM LIMITATIONS:

As of 07/15/2015, complexity requirements for all new users and those users resetting their passwords will be technically enforced for Madison College's primary credential, the UserID. Current users will be encouraged to change passwords, but a password change will not be required at this time.

The development and implementation of this standard should be seen as a "minimum" requirement.

Stronger authentication methods will be the longer term focus of our authentication strategy, particularly for higher risk users (e.g. those with access to other's sensitive information) and higher risk activities (e.g. changing direct deposit information).

CONSEQUENCES OF NON-COMPLIANCE:

All faculty, staff and students are expected to follow this standard. Non-compliance with this standard puts the College at risk of unauthorized access. Violation of this standard may result in disciplinary action – up to and including termination of employment.

REFERENCES:

The Madison College Information Security Standard provides additional information on security control measures that all employees of the College are expected to follow. Adherence to these standards helps to ensure that the College adequately protects the information we have been entrusted to use.

MODIFICATION:

This standard may be modified at any time with appropriate communication. It must be reviewed every three years to ensure the standard is applicable to the existing technology environment.

REVISION HISTORY:

Version	Date	Description of Changes	Author/ Editor	Approved By
1.0	05/08/2015	Initial Standard Definition	Linda Pruss , CISO	Cabinet-05/18/15
1.1	06/04/2015	Changed Effective Date to 07/15/2015	Linda Pruss , CISO	