George Mason University	*University Standard* **Password Complexity Standard**
Version 1.0	*Date of last revision: 02/26/16*

The purpose of this standard is to define the user password requirements for electronic access to George Mason University's workstations and systems. This standard applies to every faculty member, staff member, student, temporary employee, contractor, outside vendor, and visitor to campus (AKA User) who authenticates to University-owned computing systems or devices. This standard is designed to minimize the potential exposure to George Mason University from damages which may result from unauthorized use of George Mason University resources. Damages include the loss of highly sensitive or university confidential data, intellectual property, damage to public image, and damage to critical George Mason University internal systems.

George Mason University's Password Complexity Standard Requirement is as follows:

Your password:

- Cannot be your first, middle, or last name
- Cannot be your username/netID
- Must not include repeated characters, such as AAA or 555
- Must not include alphabetic sequences, such as abc or CBA
- Must not include numeric sequences, such as 123 or 321
- Must not use common keyboard sequences, such as QWERTY or password
- Must be at least 10 and no more than 30 characters long.

Only the characters specified below may be used and the password must include 3 out of 4 of the following character classifications.

- Upper case: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
- Lower case: **abcdefghijklmnopqrstuvwxyz**
- Numbers: **1234567890**
- Special characters: **_**

The password must not use dictionary words.
The password must not be easily guessed.
The password cannot be reused.
The password selected will be tested against a pro-active password checker library, which tests passwords for effectiveness (e.g. cracklib).

Change your password as requested. An e-mail reminder will be sent to the account owner about 30 days before the password expires. For increased security, change your password frequently.

If you authenticate directly to systems, devices or workstations that are in scope for Payment Card Industry Data Security Standard compliance you must also:

- Change your password at least every 90 Days
- Include both letters and numbers in the password / passphrase