GEORGE MASON UNIVERSITY

Password Complexity Standard

Version 1.4

STANDARD INFORMATION

This table should be completed by the responsible office(s) and IT Risk & Compliance, as it provides general information about the standard.

RESPONSIBLE OFFICES	IT Security Office (ITSO)
ADDITIONAL INFORMATION	▪ Data Stewardship (University Policy Number 1114) ▪ Responsible Use of Computing (University Policy Number 1301) ▪ Information Technology Security Program (University Policy Number 1311) ▪ Information Technology Security Standard (ITS.ITS-STD003) ▪ Payment Card Industry Data Security Standard
DOCUMENT CONTROL NUMBER	ITS.ITSO-STD008
LAST REVIEWED DATE	3/22/2024
APPLIES TO	This standard applies to every faculty member, staff member, student, temporary employee, contractor, outside vendor, and visitor to campus (i.e., user) that authenticates to university-owned computing systems or devices.

NOTE TO ALL USERS

REVISION HISTORY

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
1.0	2/26/2016	IT Security Office	Initial Release
1.1	12/11/2019	IT Security Office	Annual Review; Minor Revision (reformatting)
1.2	2/23/2021	IT Security Office	Annual Review; Minor Revision (reformatting)
1.3	03/16/23	IT Security Office	Annual Review; Minor Revision (reformatting)
1.4	3/22/2024	IT Security Office	Annual Review with minor updates to character specifications.

ABOUT THE STANDARD

PURPOSE

The purpose of this standard is to define the user password requirements or electronic access to George Mason University's workstations and systems. This standard is designed to minimize the potential exposure to George Mason University from damages that 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 Reputation, and damage to critical George Mason University internal systems.

DEFINITIONS

ACRONYM/TERM	DEFINITION
Highly Sensitive Data	Highly sensitive data is data that, if exposed, could lead to identify theft or exposure of personal health information, financial theft, or otherwise have significant adverse impact on the university.

STANDARDS

List statement(s).

Your password:

- Cannot be your first, middle, or last name
- Cannot be your username/netID
- Cannot be reused
- Must not use dictionary words
- Must not be easily guessed
- 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 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 email reminder will be sent to the account owner about 30 days before the password expires. For increased security, change your password frequently.

GEORGE MASON UNIVERSITY

For PCI Compliance
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

EXCEPTIONS

None

TIMETABLE FOR REVIEW

This standard will be reviewed every 2 years at a minimum.

APPROVALS

ROLE	NAME & ORGANIZATION	SIGNATURE	DATE
ITSO Director	Curtis McNay	DocuSigned by: Curtis McNay 6179577EE174479...	3/22/2024
(Interim) Vice President and Chief Information Officer	Charles Spann	DocuSigned by: Charles Spann 463A1FFF579B4BC...	4/15/2024